Ruijie Networks – Innovation Beyond Networks

RG-Router Implementation Cookbook (V1.3)

Copyright Statement

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

1 Preface

This guide provides an overview and explains how to configure the various features for the RG-RSR30-44 Router, RG-RSR20-14E Router, RG-RSR10-02E Router, RG-RSR10-02 Router, and RG-RSR 77 series Router. Some information may not apply to your particular router model.

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

- Ruijie Networks Websites : http://www.ruijienetworks.com
- Ruijie Service Portal : http://caseportal.ruijienetworks.com

Welcome to report error and give advice in any Ruijie manual to Ruijie Service Portal

Related Documents

- Product Datasheet

  RG-RSR30-44 Reliable Multi-Service Router Datasheet

  RG-RSR20-14E Reliable Multi-Service Router Datasheet

  RG-RSR10-02E Reliable Multi-Service Router Datasheet

  RG-RSR10-02 Reliable Multi-Service Router Datasheet

  RG-RSR77-X Core Service distributed Router Datasheet
- Hardware Installation Guide

  RG-RSR30 Series Routers Hardware Installation and Reference Guide

  RG-RSR20-14E Series Routers Hardware Installation and Reference Guide

  RG-RSR10-02E Series Routers Hardware Installation and Reference Guide

  RG-RSR10 (20) Series Router Hardware Installation and Reference Guide

  RG-RSR77 Series Router Hardware Installation and Reference Guide
- RGOS Configuration guide

  RG-RSR30 Series Router RGOS Configuration Guide

  RG-RSR20-14E Series Router RGOS Configuration Guide

  RG-RSR10-02E Series Router RGOS Configuration Guide

RG-RSR10 (20) Series Router RGOS Configuration Guide

RG-RSR77 Series Router RGOS Configuration Guide

- RGOS Command Reference

RG-RSR30 Series Router RGOS Command Reference

RG-RSR20-14E Series Router RGOS Command Reference

RG-RSR10-02E Series Router RGOS Command Reference

RG-RSR10 (20) Series Router RGOS Command Reference

RG-RSR77 Series Router RGOS Command Reference

- White Paper

White Paper for Ruijie ERPS Technology

White Paper for REF Technology

White Paper for WAN Transmission Acceleration Technology of Routers

Revision History

Date	Change contents	Reviser
2016.5	Initial publication V1.0	TAC Oversea
2017.2	Add now chapters of 1.1.3 Distributed Router Upgrade , 2.1.4 Syslog, 2.4.6 VPDN 2.0, 2.6.5 DLDP, 3.1 4G Solutions, 5.1 Detailed Configuration for Internet Access on publication V1.1	TAC Oversea
2017.10	Add new chapter of 3.3.2 Import Configuration Using FUNC Key	TAC Oversea

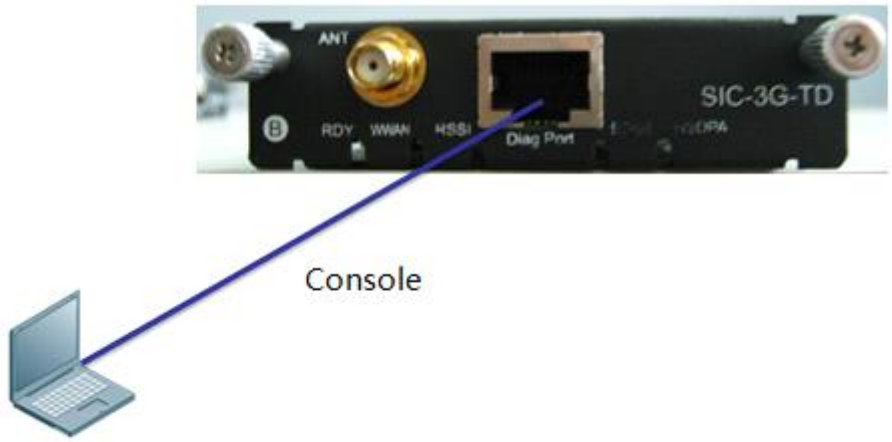
2 Index

3 Maintenance

3.1 Firmware Upgrade

3.1.1 Upgrade in Xmodem Mode

I. Topology



II. Upgrade in Xmodem Mode

Notes:

The default baud rate of the SIC-3G card is 115,200 Bd during startup and the baud rate for accessing the main screen is 9,600 Bd after startup. If the startup baud rate is changed to another value, select the new baud rate for login.

1. Power on the device and press Ctrl+C to access the BootLoader main menu.

```
====== Assign Bus 0 End
==== Assign Resources End
No fixup phys_slot/phys_seq for (PCI device 0x1131:0x1561), use busnumber/slot
No fixup phys_slot/phys_seq for (PCI device 0x1131:0x1562), use busnumber/slot
PCI fixup irq: (PCI device 0x1131:0x1561) got 22
PCI fixup irq: (PCI device 0x1131:0x1562) got 22
MPC PCI Controller finish init...
================ PCI BUS Scan/Setup End ================

Not Found PCI Driver for [0x1131:0x1561], or err in probe.
Not Found PCI Driver for [0x1131:0x1562], or err in probe.
Press Ctrl+C to enter Boot Menu ...
```

2. (Optional) If the current baud rate of the SIC-3G card is 115,200 Bd, skip this step. Otherwise, perform the following step:

Note: Changing the baud rate to 115,200 Bd aims at accelerating transmission speed over Xmodem.

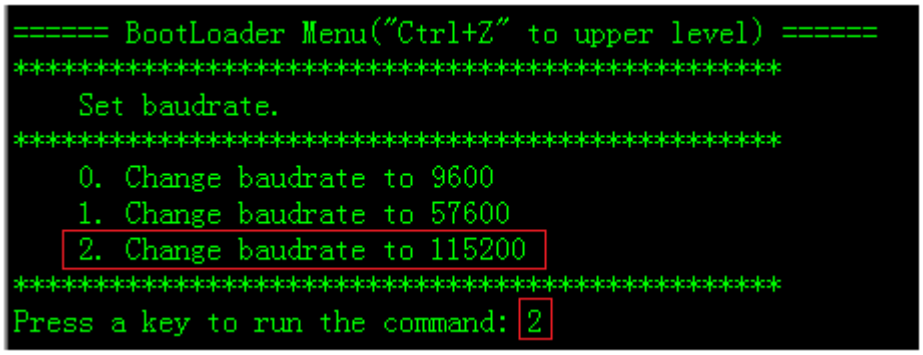
1) Select 6. Scattered utilities.

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
**************************************************
    TOP menu items.
**************************************************
    0. Tftp utilities.
    1. XModem utilities.
    2. Run Main.
    3. Run an Executable file.
    4. File management utilities.
    5. SetMac utilities.
    6. Scattered utilities.
**************************************************
Press a key to run the command: 6
```

2) Select 4. Set baudrate.

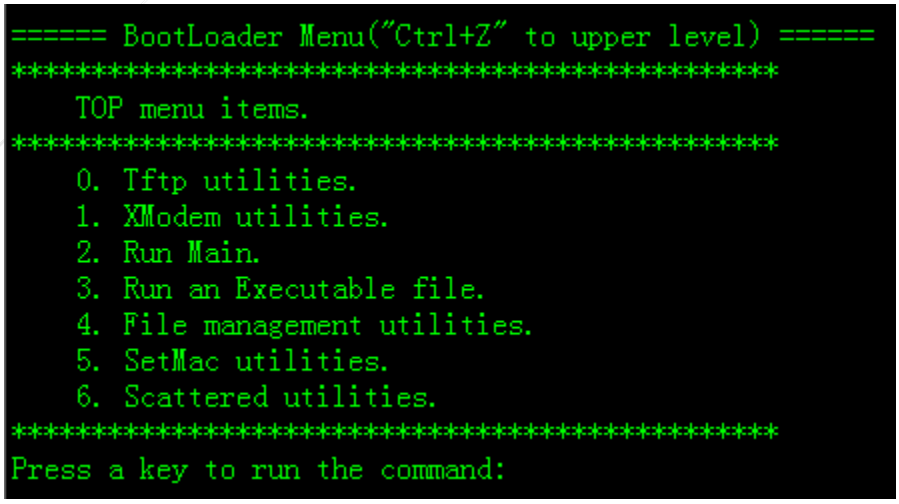
```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
**************************************************
    Scattered utilities.
**************************************************
    0. Show the bootloader/boot/ctrl version.
    1. Open/Close boot/ctrl/main debug switch.
    2. Reload system.
    3. Set the MAIN file name.
    4. Set baudrate.
**************************************************
Press a key to run the command: 4
```

3) Select 2. Change baudrate to 115200.



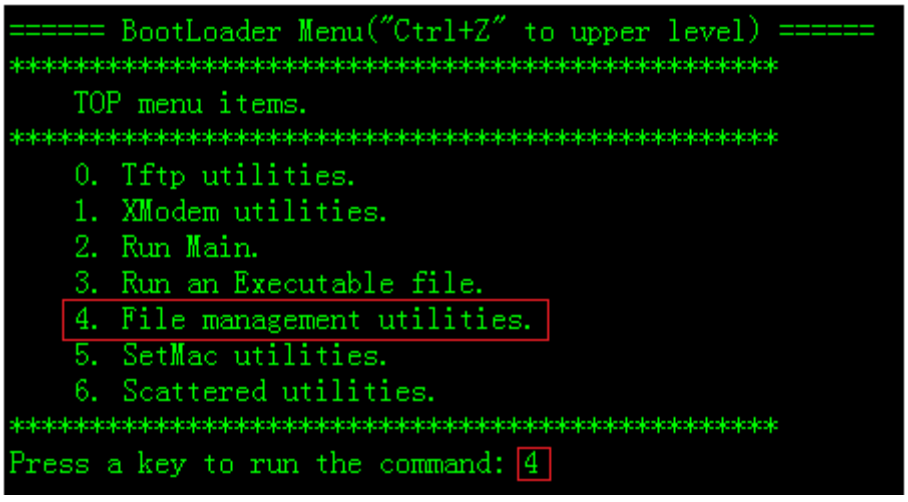
4) Change the baud rate for logging in to a terminal to 115,200 Bd and press **Enter**. The change is successful if the console displays correct information.

3. Press **Ctrl+Z** twice to return to the BootLoader main menu.

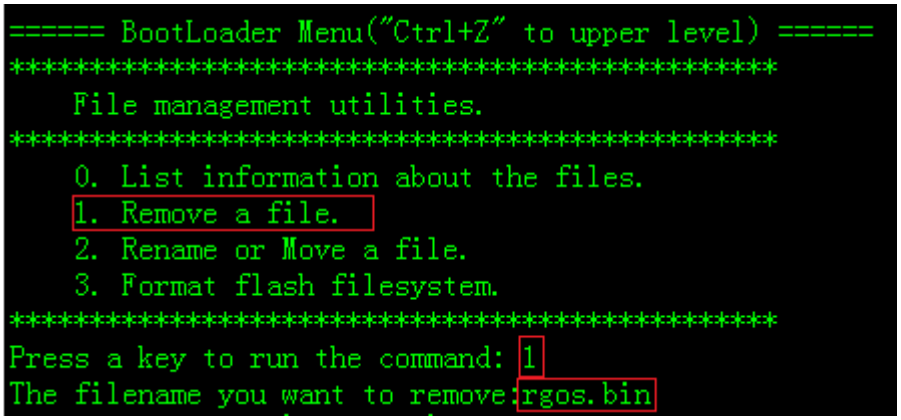


4. (Optional) If the main program of the SIC-3G card is lost, go to Step 4. Otherwise, perform the following step:

1) Select **4. File management utilities** to access the file management submenu.



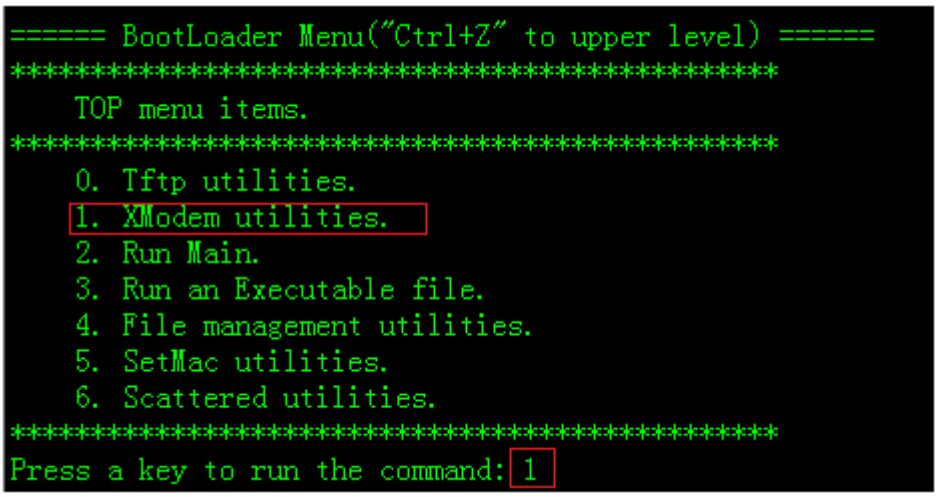
2) Select 1. Remove a file. Enter rgos.bin after the "The filename you want to remove:" prompt is displayed, and then press Enter.



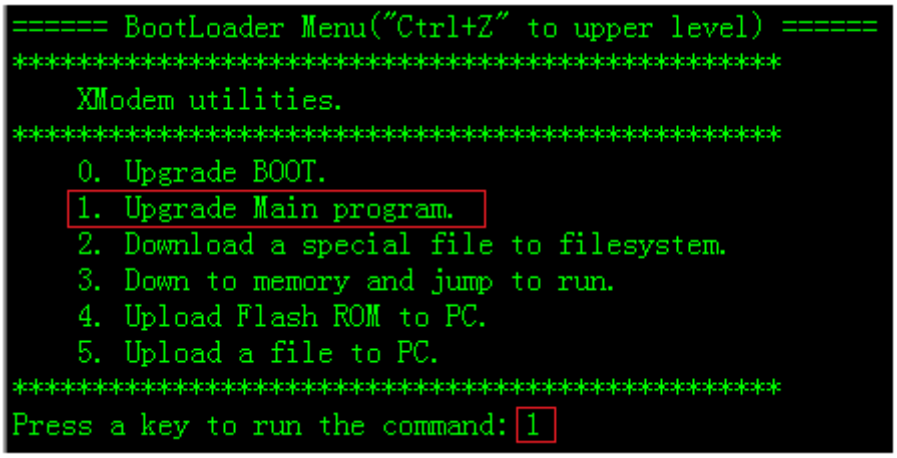
3) Press Ctrl+Z to return to the BootLoader main menu.

5. Transfer the automatic upgrade package to the SIC-3G card.

1) Select 1. XModem utilities.

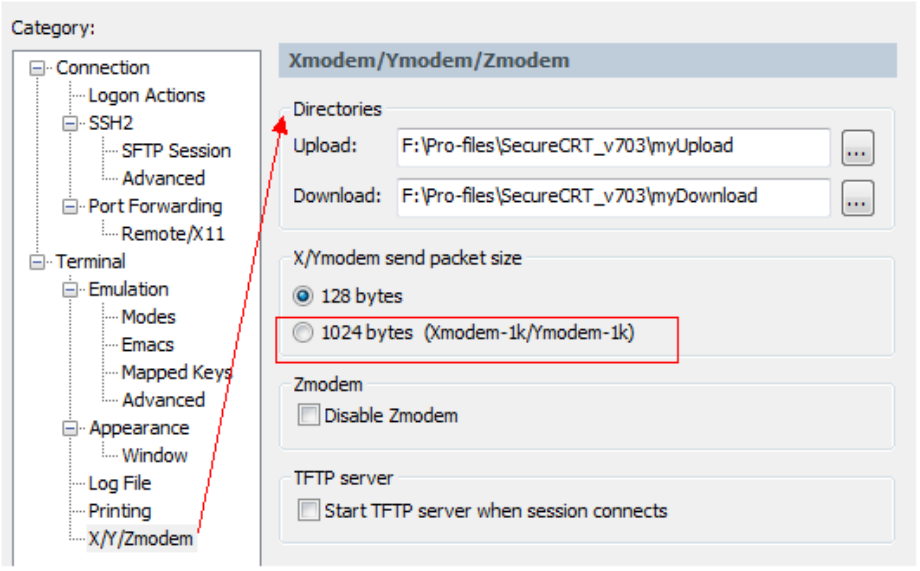


2) Select 1. Upgrade Main program.

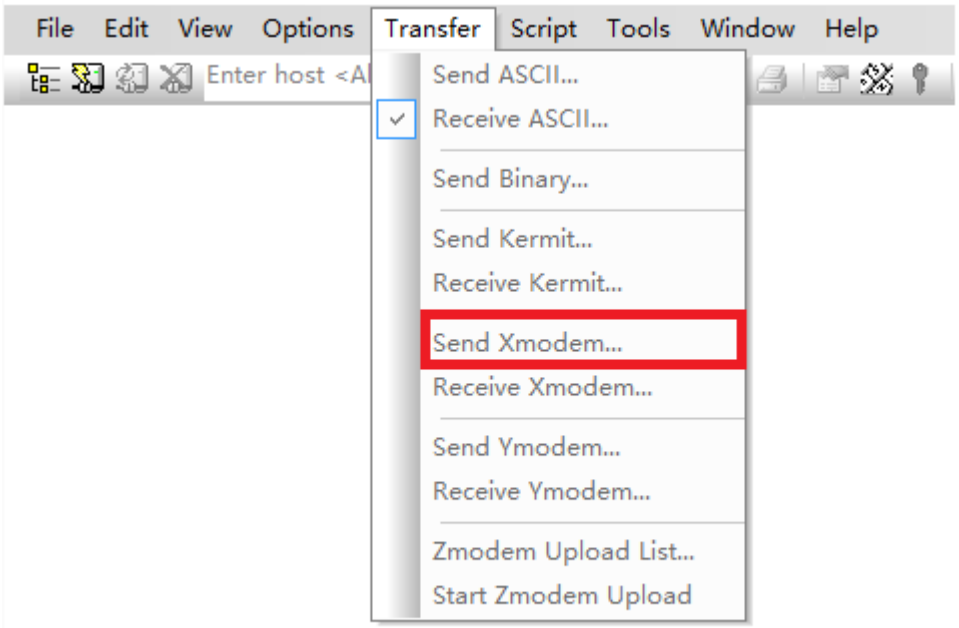


3) Send the Xmodem file.

To send the Xmodem file by using SecureCRT, choose **Option** > **Session Option** from the main menu; in the **Session Option** dialog box, choose **Terminal** > **X/Y/Zmodem** and click **1024 bytes (Xmodem-1k/Ymodem-1k)** in **X/Ymodem send packet size**.

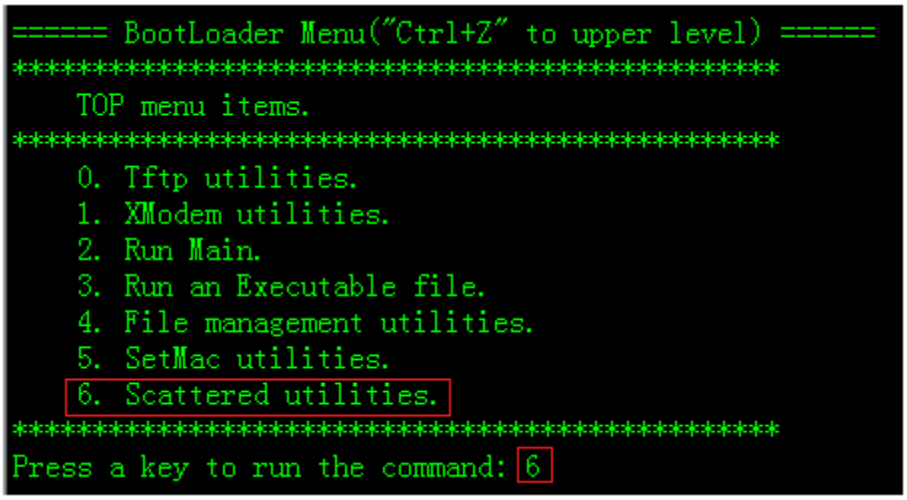


Choose **Transfer** > **Send Xmodem** from the main menu, select the bin file used for upgrade (name the bin file **rgos.bin**), and click **OK** to start upgrade.

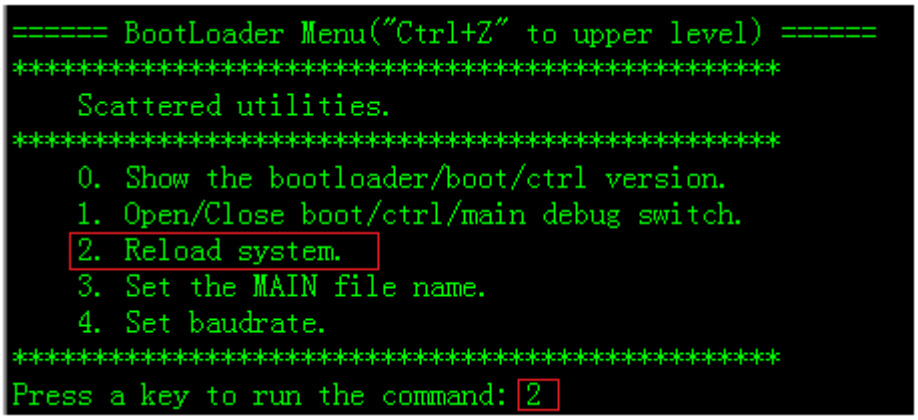


6. Restart the SIC-3G card for the automatic upgrade package to run.

   1) After downloading ends, press Ctrl+Z to return to the BootLoader main menu, and select 6. Scattered utilities.



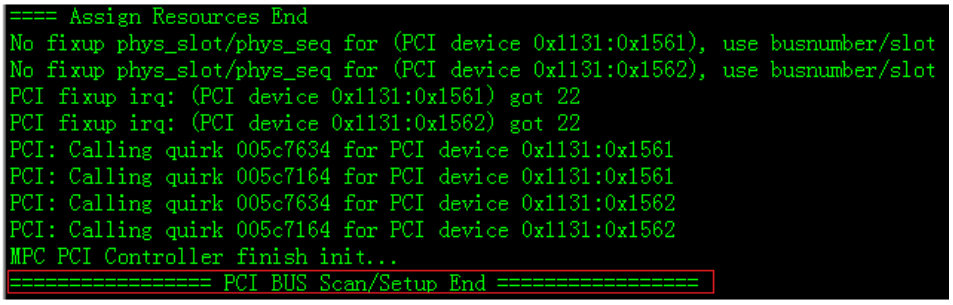
   2) Select 2. Reload system.



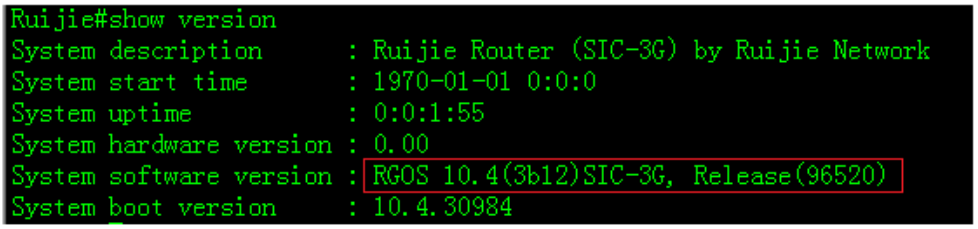
The card upgrade is in progress. Please wait patiently.

III. Upgrade Verification

1) After the upgrade ends, the card automatically restarts and enters the major release till the **PCI BUS Scan/Setup End** screen is displayed.



2) Change the baud rate for the PC to connect to the SIC-3G card console to 9,600 Bd, and press **Enter** to enter the major release environment. Then, the upgrade is complete.



3.1.2 Upgrade in Router Mode

Features

The NMX-24ESW switch fabric module of the RSR20 series routers adopts the distributed system architecture. The NMX-24ESW switch fabric module is equipped with an independent CPU, memory, flash memory, and other hardware, and has an independent main program. The NMX-24ESW switch fabric module can be upgraded in router mode or independently.

Upgrade in router mode:

The software version of the switch fabric module is bound into the software version of the router. An upgrade channel is established between the router and the switch fabric module, and the router directly transmits the software version of the switch fabric module to the flash memory of the latter, thereby achieving remote upgrade of the switch fabric module.

The RSR20 series routers of 10.3(5t86)/10.3 (5b6) p3 and later versions support switch fabric module upgrade in router mode.

Independent upgrade of the switch fabric module

The network port of the switch fabric module is connected to an external TFTP server through a network cable, and the TFTP server transmits the software version of the switch fabric module to the flash memory of the latter.

The switch fabric module of all versions supports this upgrade mode.

I. Upgrade Steps

1. Log in to the switch fabric module from the router.

In router mode, run the **service-module fastEthernet 5/0 session** command to enter the switch fabric module.

RSR20-14#service-module fastEthernet *5/0* session //Enter the switch fabric module. If the switch fabric module is seated in Slot 5,enter5/0; if it is seated in Slot 6, enter 6/0.

Ruijie# //If the device prompt is changed to Ruijie#, you enter the switch fabric module successfully.

2. Back up the original software version of the switch fabric module.

Notes:

If the current main program running on the switch fabric module is **rgos.bin**, run the **copy flash:rgos.bin flash:rgos.bak** command for backup; if the main program is **rgnos.bin**, run the **copy flash:rgnos.bin flash:rgnos.bak** command for backup.

The following example is based on the main program **rgos.bin** running on the switch fabric module.

a. Display the name of the current main program running on the switch fabric module.

```
Ruijie#dir

    Mode Link      Size               MTime Name
-------- ---- --------- ------------------- ------------------
<DIR>    1          0 1970-01-01 08:00:00 dev/
<DIR>    1          0 1970-01-01 08:00:03 ram/
<DIR>    2          0 1970-01-01 08:00:35 tmp/
<DIR>    0          0 1970-01-01 08:00:00 proc/
           1          8 1970-01-04 10:15:00 priority.dat
```

```
1    5885184 1970-01-01 09:42:03 rgos.bin //The current main program running on the switch fabric module is rgos.bin.
            1    5885184 1970-01-01 08:07:19 rgos.10.2(2).33474
-----------------------------------------------------------------
3 Files (Total size 11770376 Bytes), 4 Directories.
Total 31457280 bytes (30MB) in this device, 17907712 bytes (17MB) available.
```

b. Back up the software version of the switch fabric module.

```
Ruijie#copy flash:rgos.bin flash:rgos.bak  //Back up the software version of the switch fabric module as rgos.bak.
Ruijie#dir

    Mode Link      Size               MTime Name
-------- ---- --------- ------------------- ------------------
<DIR>    1          0 1970-01-01 08:00:00 dev/
<DIR>    1          0 1970-01-01 08:00:03 ram/
<DIR>    2          0 1970-01-01 08:00:35 tmp/
<DIR>    0          0 1970-01-01 08:00:00 proc/
            1          8 1970-01-04 10:15:00 priority.dat
1    5885184 1970-01-01 08:05:51 rgos.bak    //The software version of the switch fabric module is backed up successfully.
            1    5885184 1970-01-01 09:42:03 rgos.bin
-----------------------------------------------------------------
3 Files (Total size 11770376 Bytes), 4 Directories.
Total 31457280 bytes (30MB) in this device, 17907712 bytes (17MB) available.
```

c. Press **Ctrl+X** to exit from the switch fabric module to the router mode.

3. Upgrade the main program of the router.

   For the upgrade method, see section "Main Program Upgrade" (choose Daily Maintenance>Software Upgrade>Mid-range and Low-end Series Router Upgrade>10.x Version Upgrade> Main Program Upgrade).

4. Display the software versions of the router and switch fabric module.

   1) Display the software version of the router in router mode.

```
RSR20-14#dir

    Mode Link      Size               MTime Name
-------- ---- --------- ------------------- ------------------
<DIR>    1          0 1970-01-01 00:00:00 dev/
<DIR>    2          0 2013-03-29 02:15:55 esw/ //Directory for storing the software version of the switch fabric module
<DIR>    2          0 2011-05-23 03:40:19 log/
<DIR>    2          0 2013-03-29 04:31:32 mnt/
```

```
<DIR>    1          0 2013-03-29 04:31:26 ram/
<DIR>    2          0 2013-03-29 04:31:46 tmp/
<DIR>    0          0 1970-01-01 00:00:00 proc/
            1       1263 2013-01-31 14:19:56 config_0113.bak
1    7248608 2013-03-29 02:15:36 rgos.bin //Software version of the router
------------------------------------------------------------
2 Files (Total size 7249871 Bytes), 7 Directories.
Total 33030144 bytes (31MB) in this device, 20160512 bytes (19MB) available.
```

2) Display the software version of the switch fabric module in router mode.

Notes:

For RSR20 series routers of 10.3(5t86), 10.3(5b6)p3, and later versions, the software version of the switch fabric module is packaged into the main program of the router. After the router upgrade is complete, the router automatically decompresses the software version of the switch fabric module into the **esw** folder in the flash memory.

```
RSR20-14#cd esw //Access the directory for storing the software version of the switch fabric module.
RSR20-14#dir

    Mode Link      Size               MTime Name
-------- ---- --------- ------------------ ------------------
1    4221664 2013-03-29 02:16:04 esw_install.bin //Main program file of the switch fabric module
------------------------------------------------------------
1 Files (Total size 4221664 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20160512 bytes (19MB) available.
```

5. Return to the main program of the router in the flash memory and enable the terminal monitor function.

```
RSR20-14#cd ..      //Return to the main program of the router in the flash memory.
RSR20-14#terminal monitor    //Enable the terminal monitor function.
```

6. Shut down services of the switch fabric module, and deliver the main program of the switch fabric module from the flash memory of the router to the flash memory of the switch fabric module.

Notes:

1) It takes about 15 minutes to transmit the software version of the switch fabric module from the router to the flash memory of the switch fabric module.

2) When the prompt "Upload completed" is displayed, wait another 8-15 minutes (15 minutes are recommended) to ensure that the version files of the switch fabric module are all received.

3) Do not perform destructive operations such as power-off and restart during upgrade of the switch fabric module. Otherwise, the upgrade of the switch fabric module will fail.

4) If the switch fabric module or router is restarted before version files of the switch fabric module are all received, the version files may be damaged and the switch fabric module may fail to start. In this case, run the **RSR20-14#service-module fastEthernet 5/0 reset** command in router mode to restart the switch fabric module, press **Ctrl+C** to enter the Ctrl layer of the switch fabric module, press **Ctrl+Q** to enter the CLI mode, and then run the **Ctrl>rename rgos.bak rgos.bin**

command to restore the original main program of the switch fabric module. Then, run the **Ctrl>reload** command to restart the switch fabric module and restore services.

```
RSR20-14#esw-switch shut-service    //Shut down services of the switch fabric module.
RSR20-14#esw-upgrade xmodem slot 5 //Transmit the software version of the switch fabric module in the flash memory of the router to the flash memory of the switch fabric module (if the switch fabric module is seated in Slot 5, enter slot 5; if it is seated in Slot 6, enter slot 6).
*Mar 29 06:09:29: %UPGRADE-6-ESW_CARD_UPRADE: Now start transmit file.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!#*Mar 29 06:24:45: %UPGRADE-6-ESW_CARD_UPRADE: Upload completed, 4221664 bytes of valid data has been transferred.
*Mar 29 06:24:45: %UPGRADE-6-ESW_CARD_UPRADE: Please wait a few minutes(about 8-15min) for the switch card upgrading until you can login the card.  //Wait another 8-15 minutes (15 minutes are recommended) to ensure that version files of the switch fabric module are all received.
```

7. Enable services of the switch fabric module, log in to the switch fabric module, and check its software version.

```
RSR20-14#esw-switch open-service   //Enable services of the switch fabric module.
RSR20-14#service-module fastEthernet 5/0 session   //Enter the switch fabric module. If the switch fabric module is seated in Slot 5, enter 5/0; if it is seated in Slot 6, enter 6/0.
```

8. (Optional) Rename the main program file of the switch fabric module.

   If the original main program of the switch fabric module is **rgnos.bin**, skip to Step 9.

   Notes:

- If the original main program file of the switch fabric module is **rgnos.bin**, the version file transmitted over Xmodem directly replaces it and the file does not need to be renamed. The switch fabric module fails if it is renamed.
- If the original main program file of the switch fabric module is **rgos.bin**, the new program file needs to be renamed **rgos.bin** to ensure successful upgrade. The following example is based on the original main program file **rgos.bin** of the switch fabric module.

  1) Display the main program file of the switch fabric module.

```
Ruijie#dir

    Mode Link      Size                MTime Name
-------- ---- --------- ------------------- -------------------
<DIR>     1          0 1970-01-01 08:00:00 dev/
<DIR>     1          0 1970-01-01 08:00:03 ram/
<DIR>     2          0 1970-01-01 08:00:35 tmp/
<DIR>     0          0 1970-01-01 08:00:00 proc/
```

```
            1         8 1970-01-04 10:15:00 priority.dat
1    4221696 1970-01-01 08:51:00 rgnos.bin //New main program of the switch fabric module
1    5885184 1970-01-01 08:05:51 rgos.bak //Original main program backup of the switch fabric module
1    5885184 1970-01-01 09:42:03 rgos.bin //Original main program of the switch fabric module
-----------------------------------------------------------------
4 Files (Total size 15992072 Bytes), 4 Directories.
Total 31457280 bytes (30MB) in this device, 12918784 bytes (12MB) available.
```

2) Rename the new main program of the switch fabric module rgos.bin.

Ruijie#rename flash:rgnos.bin flash:rgos.bin //The new main program directly replaces the original main program.

3) Check whether the new main program is renamed successfully.

```
Ruijie#dir

    Mode Link      Size               MTime Name
-------- ---- --------- ------------------- ------------------
<DIR>    1          0 1970-01-01 08:00:00 dev/
<DIR>    1          0 1970-01-01 08:00:03 ram/
<DIR>    2          0 1970-01-01 08:00:35 tmp/
<DIR>    0          0 1970-01-01 08:00:00 proc/
            1          8 1970-01-04 10:15:00 priority.dat
            1    5885184 1970-01-01 08:05:51 rgos.bak
1    4221696 1970-01-01 08:51:00 rgos.bin //The new main program is successfully renamed rgos.bin.
```

9. Press Ctrl+X to exit the switch fabric module and restart the router to complete upgrade of the switch fabric module.

Notes:

1) The switch fabric module can be managed on the screen of the router. It is not recommended that the switch fabric module be independently restarted and upgraded. If some management commands become available after the switch fabric module is independently restarted, the router needs to be restarted.

2) When the system reaches the state "FastEthernet 0/0, changed state to up" after router restart, wait 4-5 minutes for the switch fabric module to complete upgrade. Then, the system is restarted completely. This waiting is required only after the upgrade of the switch fabric module is complete, and is not required in normal restart.

```
RSR20-14#reload   //Restart the router to complete the upgrade.
Proceed with reload? [no]y
```

II. Upgrade Verification

Check whether the software versions of both the router and switch fabric module are upgraded successfully.

1) Check whether the router is upgraded successfully.

```
RSR20-14#show version
System description      : Ruijie Router (RSR20-14) by Ruijie Networks
System start time       : 2013-03-29 7:7:40
System uptime           : 0:0:3:36
System hardware version : 1.00
System software version : RGOS 10.3(5T86), Release(154167)
System BOOT version     : 10.3.154167
```

2) Enter the switch fabric module and check whether it is upgraded successfully.

```
Ruijie#show version
System description      : Ruijie Switch Service Module(NM2-24ESW) by Ruijie Network Co., Ltd..
System start time       : 1970-1-1 8:0:0
System hardware version : 2.0
System software version : RGOS 10.2(3T42), Release(153542)
System boot version     : 10.2.21580
System CTRL version     : 10.2.45595
System serial number    : 0000000000000
Device information:
  Device-1
    Hardware version : 2.0
    Software version : RGOS 10.2(3T42), Release(153542)
    BOOT version     : 10.2.21580
CTRL version     : 10.2.45595
    Serial Number    : 0000000000000
```

3.1.3 Distributed Router Upgrade

Instructions for Distributed Router Upgrade

I. RSR distributed routers include the following series:

RSR30-X SPU10 V2

RSR50E-40

RSR77 series (RSR7704/RSR7708/RSR7716)

RSR77-X series (RSR7708-X/RSR7716-X)

Upgrade in CTRL mode

II. Upgrade at the CTRL Layer

1) Generally only when an upgrade fails or the main program is lost, the upgrade is performed at the CTRL layer. To upgrade at the CTRL layer, you must connect the cable between a router and a PC to the MGMT interface on the main processing unit (MPU) of the router.

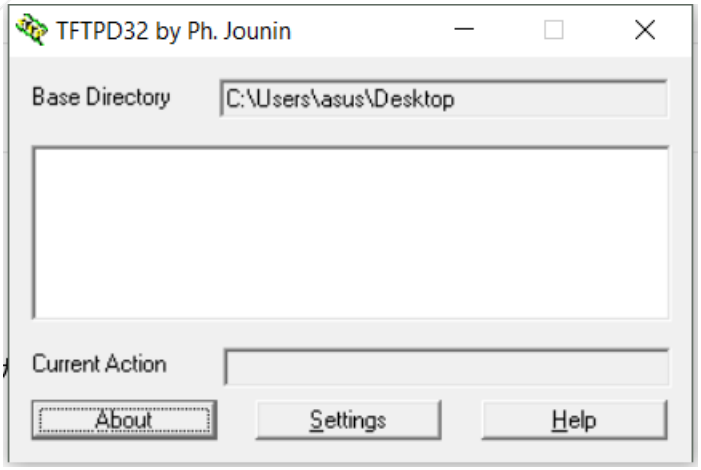
2) If **send download request** is displayed during startup and the device cannot enter the user mode, it indicates that functions of the current software version are lost and you need to upgrade the version at the CTRL layer.

III. Upgrade Steps

1. Prepare the upgrade file on the PC and start the TFTP Server.

   1) Put the software upgrade file and the Trivial File Transfer Protocol (TFTP) Server in the same folder (rename the software version to rgos.bin).

   2) Double click startftp.exe to start the TFTP Server.



2. Restart the router and enter command mode at the CTRL layer.

   Restart the router. When **Press Ctrl+C to enter Ctrl ....** is displayed, press Ctrl+C to enter command mode at the CTRL layer. **Ctrl>** prompt is displayed.

```
System bootstrap ...
Nor Flash ID: 0x01490000, SIZE: 2097152Bytes
Press Ctrl+B to enter Boot Menu .....
Load Ctrl Program ...

Load CTRL with ECC......
Executing program, launch at: 0x01000000

RDND-6-ROLE: M1 MASTER
Ctrl Version: RGOS 10.4(3b15)p1 Release(154247)
MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 536870912) detected
MTD_DRIVER-5-MTD_NAND_FOUND: 1 nand chip(s) found on the target.
RDND-6-HBU: PCIE data channal set over.
Press Ctrl+C to enter Ctrl ....

Hot Commands:
------------------------------------------------------------
F1. upgrade -slot all -force
F2. tftp 192.168.1.200 192.168.1.100 rgos.bin -main
F3. xmdown -main
------------------------------------------------------------
Ctrl>
```

3. Check card identification.

Before the upgrade, check card identification. If any card fails to be identified, please stop the process in case all cards fail to be upgraded. If any card is in UNKNOWN status, it indicates that this card fails to be upgraded and you need to restart the device. If the card is still in UNKNOWN status after restart, contact Ruijie technical support engineers for upgrade guidance.

Run the **upgrade–slot** command to check the upgrade path of the device. The following is an example:

```
Ctrl>upgrade -slot
Usage: upgrade -slot <all | 1..8 [excard 1..2] | M1 | M2> [-type <boot | ctrl | main>] [-force]
--------------------------------
   SLOT CARD
   --------------------------------
   [1/0] SIP1
   [1/1] FNM-2CPOS-STM1
   [1/2] FNM-4POS-STM1
   [2/0] NONE
   [2/1] NONE
   [2/2] NONE
   [3/0] NONE
   [3/1] NONE
   [3/2] NONE
   [4/0] SIP2
   [4/1] NONE
   [4/2] NONE
   --------------------------------
Ctrl>
```

Note:Perform upgrade only when all cards are identified.

4. Transmit the automatic upgrade package to the router.

Connect the cable between the PC and the router to the MGMT interface on the MPU of the router. Run the **TFTP** command to transmit the automatic upgrade package.

```
Ctrl>tftp 192.168.1.1 192.168.1.2 rgos.bin -main
          Router address  PC address   file name(Path)

Now, begin download program through Tftp...

Host IP[192.168.1.2]  Target IP[192.168.1.1]  File name[rgos.bin]
                  %Now Begin Download File rgos.bin From 192.168.1.2 to 192.168.1.1


send download request.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

When the prompt **SUCCESS: UPGRADING OK** is displayed on the router, it indicates that the upgrade package has been transmitted to the router.

5. Upgrade line cards.

Run the **upgrade -slot all -force** command to upgrade the version of line cards.

The router automatically upgrades all line cards.

6. Reset the system to run the automatic upgrade package.

```
Ctrl>reload
```

Note:

1. Do not perform any dangerous operation such as reset or power cutoff when running the automatic upgrade package until the upgrade process is finished.
2. After the running process is finished, the system is automatically reset to boot a new system.

IV. Verification

1) Run the **show version** command to display the device version and check whether the upgrade is successful.

```
Ruijie#show version
System description      : Ruijie Router (RSR7708) by Ruijie Networks
System start time       : 2013-03-08 12:13:7
System uptime           : 0:0:42:51
System hardware version : 1.00
System software version : RGOS 10.4(3b15)p1 Release(153172)
System BOOT version     : 10.4(3b15)p1 Release(153172)
System CTRL version     : 10.4(3b15)p1 Release(153172)
Module information:
  Slot-M1 : RSR7708-SRCMI
    System hardware version : 1.00
    System software version : RGOS 10.4(3b15)p1 Release(153172)
    Flash MAIN version      : 10.4(3b15)p1 Release(153172)
    Flash CTRL version      : 10.4(3b15)p1 Release(153172)
    Flash BOOT version      : 10.4(3b15)p1 Release(153172)
  Slot-M2 : RSR7708-SRCMI
    System hardware version : 1.00
    System software version : RGOS 10.4(3b15)p1 Release(153172)
    Flash MAIN version      : 10.4(3b15)p1 Release(153172)
    Flash CTRL version      : 10.4(3b15)p1 Release(153172)
    Flash BOOT version      : 10.4(3b15)p1 Release(153172)
  Slot-1/0 : RSR77-SIP1
    System hardware version : 1.00
    System software version : RGOS 10.4(3b15)p1 Release(153172)
    Flash MAIN version      : 10.4(3b15)p1 Release(153172)
    Flash CTRL version      : 10.4(3b15)p1 Release(153172)
    Flash BOOT version      : 10.4(3b15)p1 Release(153172)
```

Note:

Run the **show version** command to display the MAIN, CTRL, and BOOT versions of the MPU and all line cards. If all of these are the latest versions, the upgrade is successful.

2) Run the **show version slot** command to display the status of each slot card. Confirm that the software status of each line card is running. The following is an example:

```
Ruijie#show version slots
Dev  Slot   MaxPorts   Configured-Module   Online-Module       Status
---  ----   --------   -----------------   -----------------   ------
1    M1     1          RSR7708-SRCMI       RSR7708-SRCMI       master
1    M2     1          RSR7708-SRCMI       RSR7708-SRCMI       slave
1    1/0    0          RSR77-SIP1          RSR77-SIP1          running
1    1/1    2          FNM-2CPOS-STM1      FNM-2CPOS-STM1      running
1    1/2    4          FNM-4POS-STM1       FNM-4POS-STM1       running
1    2/0    0                                                  none
1    3/0    0                                                  none
1    4/0    2          RSR77-SIP2          RSR77-SIP2          running
1    4/1    8          DNME-8E1/CE1        DNME-8E1/CE1        running
1    4/2    0                                                  none
Ruijie#
```

If the status is installed or runing-config for a long time after software upgrade, please immediately contact Ruijie for technical support.

Upgrade in Main Program Mode (via TFTP)

I. Upgrade Steps

1. Configure an IP address for the router Ethernet interface.

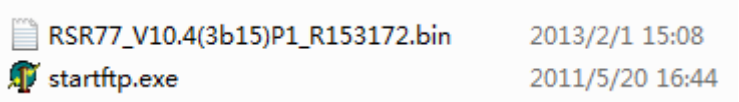
Configure an IP address for the router.

Note:

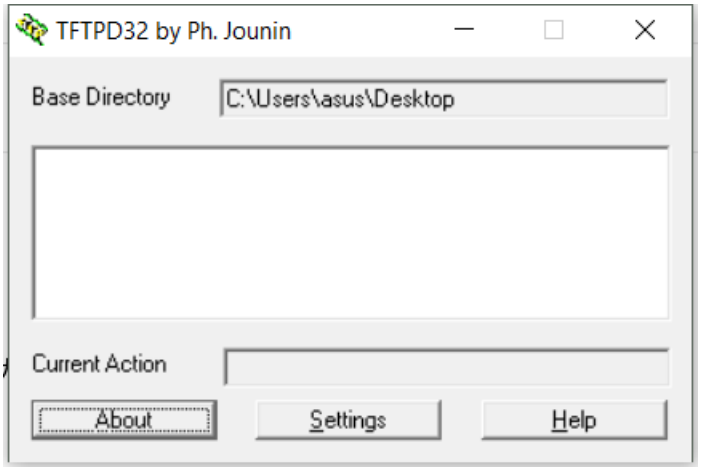
Ensure that the PC can ping the router. Disable the firewall of the PC before upgrade.

2. Prepare the upgrade file on the PC and start the TFTP Server.

1) Put the software upgrade file and the TFTP server in the same folder.



2) Double click **startftp.exe** to start the TFTP Server.



3. Check card identification.

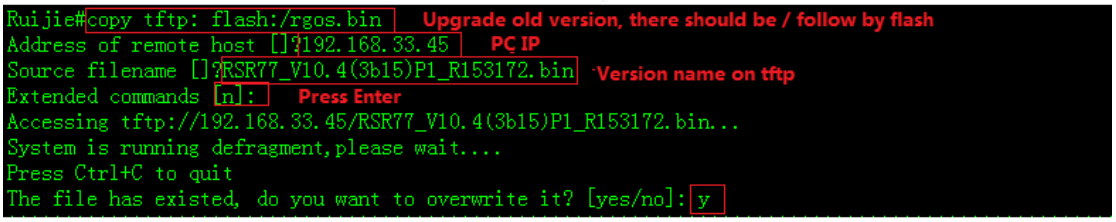
Before the upgrade, check card identification. If any card fails to be identified, please stop the process in case all cards fail to be upgraded. If any card is in no card status, it indicates that this card fails to be upgraded and you need to restart the device. If the card is still in no card status after restart, contact Ruijie technical support engineers for upgrade guidance.

Run the **show upgrade** command to check the upgrade path of the device.The following is an example:

Perform upgrade only when all cards are identified. Only the line cards or engines of the version to be released are displayed while the slot number of the active engine is not displayed. That is, if RSR77 has two engines, the standby engine instead of the active engine is displayed; if RSR77 has only one engine, the slot number of the engine is not displayed.

4. Transmit the automatic upgrade package to the router.

Run the **copy tftp: flash:/rgos.bin** command to transmit the upgrade file to the router.



After transmission, the system automatically verifies the validity of the file. If the standby supervisor module has been inserted before upgrade, the installation package is automatically synchronized to the standby supervisor module. When the prompt **SUCCESS: UPGRADING OK** is displayed, it indicates that the automatic upgrade package has been transmitted to the router.

Note:

1) If the prompt **Verify the image .....[ok]** is displayed, it indicates successful transmission and verification.

2) If the prompt **System is running defragment, please wait....Press Ctrl+C to quit.....** is displayed, it indicates that the router is running defragment and please wait.

3) If the prompt **Transmission fail** or **.....** is displayed, it indicates that transmission fails. Check whether the PC can ping the router, whether the designated directory of TFTP Server is correct, and whether the file name is correct.

4) If the prompt **ERROR: THE BINARY FILE CANNOT BE USED IN CURRENT PRODUCT !!!** is displayed, it indicates that validity verification fails (the automatic upgrade package is not applicable to the current product). Please check whether the correct automatic upgrade package is used.

5. **Decompress the upgrade package to line cards** (if the current version is 3b21 or a later version, it is recommended but not mandatory to upgrade it to a later version).

Note:

1) The new and old versions of RSR77 series routers have the same upgrade command: upgrade system rgos.bin, and are only different in the user interface (UI). If the current version is 10.4 (3b15) p1 or a later version, as the upgrade function is optimized and the upgrade time is reduced, the UI is different from that of an earlier version.

2) After the **upgrade system rgos.bin** command is run to upgrade and restart the device, the old version of the BOOT layer may remain but it does not matter. If it is required to keep the versions of the MAIN layer, CTRL layer, and BOOT layer consistent, run the following command.

   a. The following is a upgrade UI example for 10.4 (3b15) p1 and a later version.

   After the automatic upgrade package is downloaded to the device, run the **upgrade system rgos.bin** command to upgrade line cards.

```
Ruijie#upgrade system rgos.bin
These images in linecard will be updated:
     Slot      image     linecard
    -------   -----     -----------------------
       M1     CTRL                       SRCMI
       M2     CTRL                       SRCMI
              MAIN                       SRCMI
      1/0     CTRL                        SIP1
              MAIN                        SIP1
      4/0     CTRL                        SIP2
              MAIN                        SIP2
      1/1     CTRL                FNM-2CPOS-STM1
              MAIN                FNM-2CPOS-STM1
----------------------------------------------
Installing CTRL,DO NOT POWER OFF!
Releasing files...
Upgrading...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
CTRL installed
Installing MAIN
Releasing files...
Upgrading...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
MAIN installed
Upgrade result:
```

Note:

The device is upgraded automatically. The following red box indicates the line cards and corresponding MAIN layer, CTRL layer, and BOOT layer to be upgraded.

```
Upgrade result:
     Slot      Image     Result
    -------   -----     --------
       M1     CTRL           OK
       M2     CTRL           OK
              MAIN           OK
      1/0     CTRL           OK
              MAIN           OK
      4/0     CTRL           OK
              MAIN           OK
      1/1     CTRL           OK
              MAIN           OK
-------------------------------
```

Note:

After the upgrade process is finished, the upgrade result is displayed, specifying the line cards implementing image upgrade in this process, image type, and upgrade results. OK indicates successful upgrade. FAIL indicates failed upgrade.

3) The following is a upgrade UI example for 10.4 (3b15) p1 and an earlier version.

After the automatic upgrade package is downloaded to the device, run the **upgrade system rgos.bin** command to upgrade line cards.

```
Ruijie#upgrade system rgos.bin
These images in linecard will be updated:
     Slot     image    linecard
    ------    -----    ------------------------
      M1      CTRL                        SRCMI
      M2      CTRL                        SRCMI
              MAIN                        SRCMI
      1/0     CTRL                         SIP1
              MAIN                         SIP1
      4/0     CTRL                         SIP2
              MAIN                         SIP2
      1/1     CTRL               FNM-2CPOS-STM1
              MAIN               FNM-2CPOS-STM1
-----------------------------------------------
(Slot M1): Installing CTRL
Upgrading CTRL...
DO NOT POWER OFF!
Erasing device...eeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash ######################## [OK - 1,331,968 bytes]
(Slot M1): CTRL installed.
(Slot M1): Install finish in slot M1 (SRCMI).
(Slot M2): Installing CTRL
(Slot M2): Download image!!!!!!!!!!!!!!!!!!!![OK - 1,331,712 bytes]
Waiting for image installed...Complete
Erasing device...eeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash ################### [OK - 1,331,968 bytes]
```

Note:

The device is upgraded automatically. The following red box indicates the line cards and corresponding MAIN layer, CTRL layer, and BOOT layer to be upgraded.

6. Reset the system to run the automatic upgrade package.

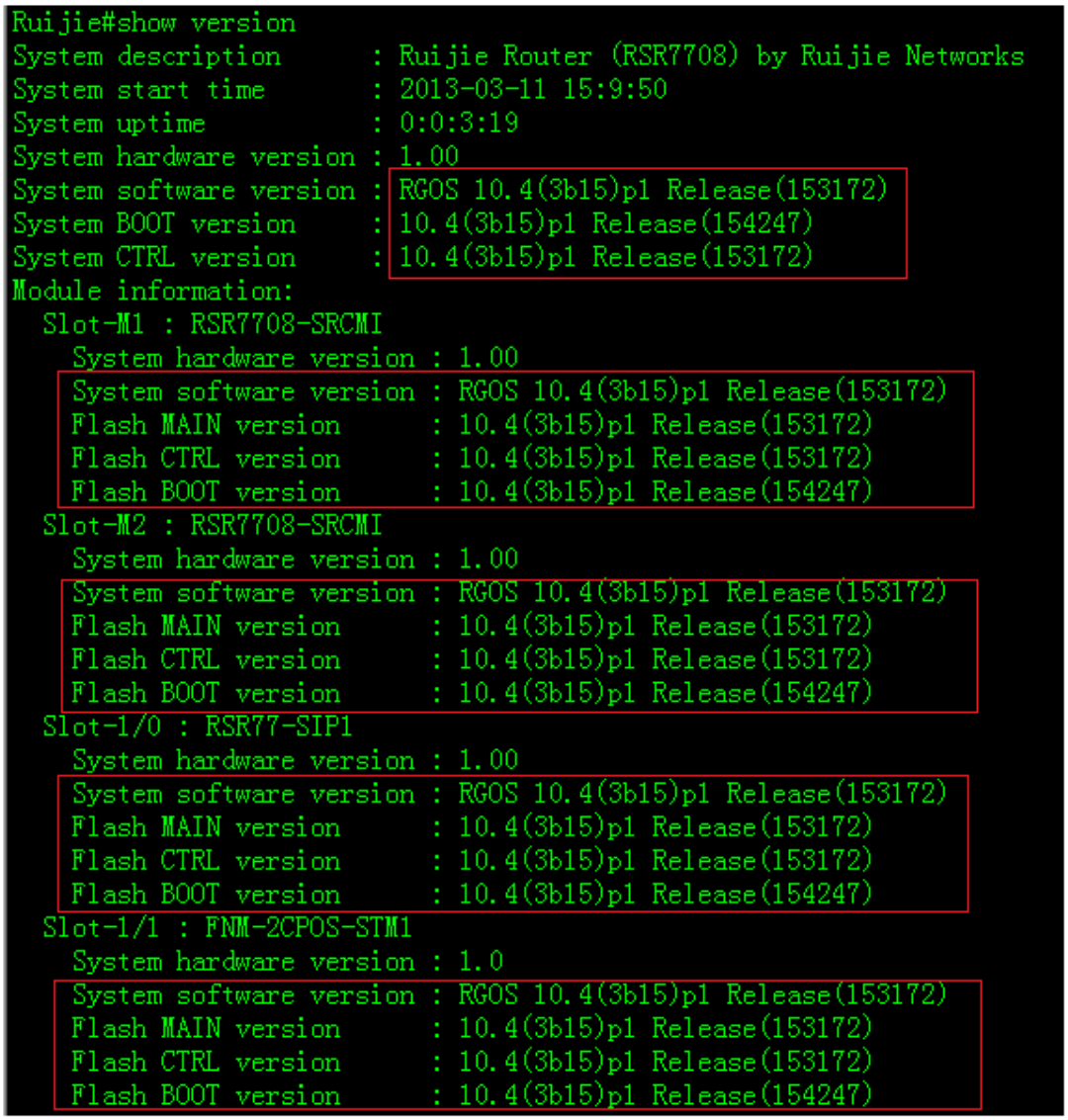
```
Ruijie#reload
Proceed with reload? [no]y
```

Note:

Do not perform any dangerous operation such as reset or power cutoff when running the automatic upgrade package until the upgrade process is finished.

II. Verification

1) Run the **show version** command to display the device version and check whether the upgrade is successful.



Note:

a) Run the **show version** command to display the MAIN versions of the MPU and all line cards. If all of these are the latest versions, the upgrade is successful.

b) The MAIN, CTRL, and BOOT versions can be inconsistent. When the manual upgrade is performed, the upgrade system automatically determines whether to upgrade CTRL/BOOT versions based on the upgrade policy in the installation package. Upgrade versions as required.

2) Run the **show version slot** command to display the status of each slot card. Confirm that the software status of each slot card is running. The following is an example:

```
Ruijie#show version slots
Dev  Slot   MaxPorts   Configured-Module   Online-Module       Status
---  ----   --------   -----------------   -----------------   ------
1    M1     1          RSR7708-SRCMI       RSR7708-SRCMI       master
1    M2     1          RSR7708-SRCMI       RSR7708-SRCMI       slave
1    1/0    0          RSR77-SIP1          RSR77-SIP1          running
1    1/1    2          FNM-2CPOS-STM1      FNM-2CPOS-STM1      running
1    1/2    0                                                  none
1    2/0    0                                                  none
1    3/0    0                                                  none
1    4/0    2          RSR77-SIP2          RSR77-SIP2          running
1    4/1    8          DNME-8E1/CE1        DNME-8E1/CE1        running
1    4/2    0                                                  none
```

If the status is installed or runing-config for a long time after software upgrade, please immediately contact Ruijie for technical support.

Upgrade in Main Program Mode (via FTP)

I. Note to Upgrade via FTP

As the PC where the new version is stored is translating a private Intranet address to a public address, the device cannot be upgraded via TFTP. By upgrade via File Transfer Protocol (FTP), enable FTP Server on the PC and transmit the software version to the device via FTP.

II. Upgrade Tips

1. Enable FTP Server on the device.
2. Transmit the software version to the device with the PC as an FTP client.
3. Restart the device to confirm the upgrade result.

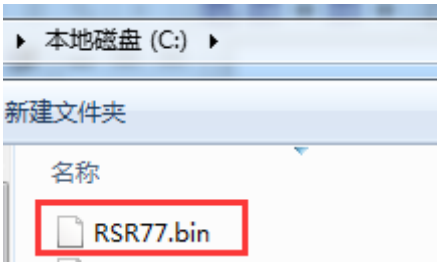
III. Upgrade Steps

1. Log in to the device to be upgraded and enable FTP Server.

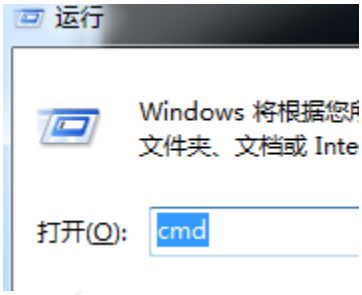
```
Ruijie(config)#ftp-server enable    --->Enables FTP Server.
Ruijie(config)#ftp-server username ruijie --->Configures FTP Server user name.
Ruijie(config)#ftp-server password ruijie --->Configures FTP Server password.
Ruijie(config)#ftp-server topdir /  --->Configures the directory where received files are stored for FTP Server. For the upgrade file, the directory must be indicated by "/".
```

2. Configure FTP parameters for the PC to log in to the device and transmit the new version to the device.

   Put the bin file to be uploaded in a root directory of a disk, such as C:\.

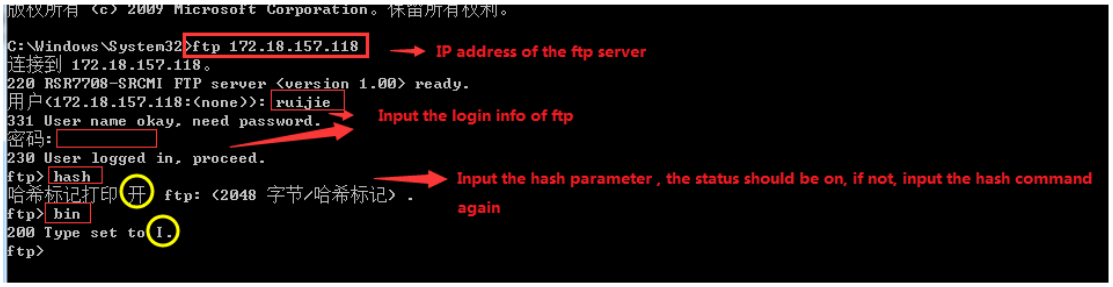


Choose **Menu** > **Run** > **CMD**, and then press Enter.

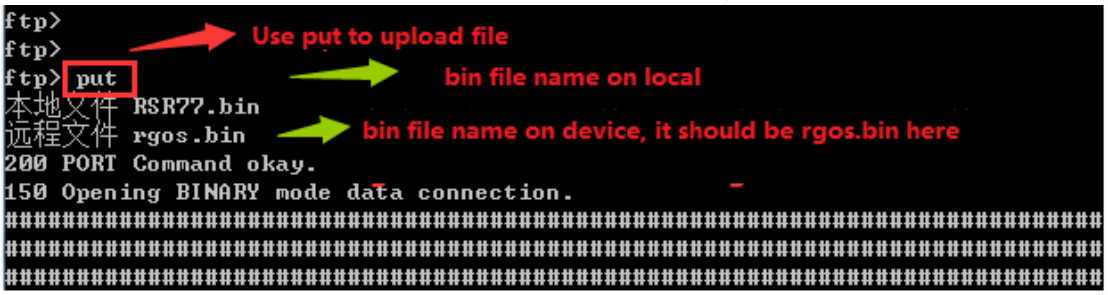


Enter disk C (where the bin file is stored) and enable FTP Server.

Log in to the device to configure parameters.

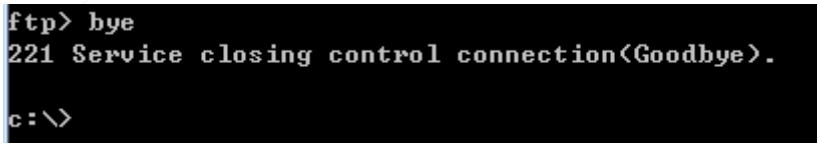


3. Transmit the bin file to the device.



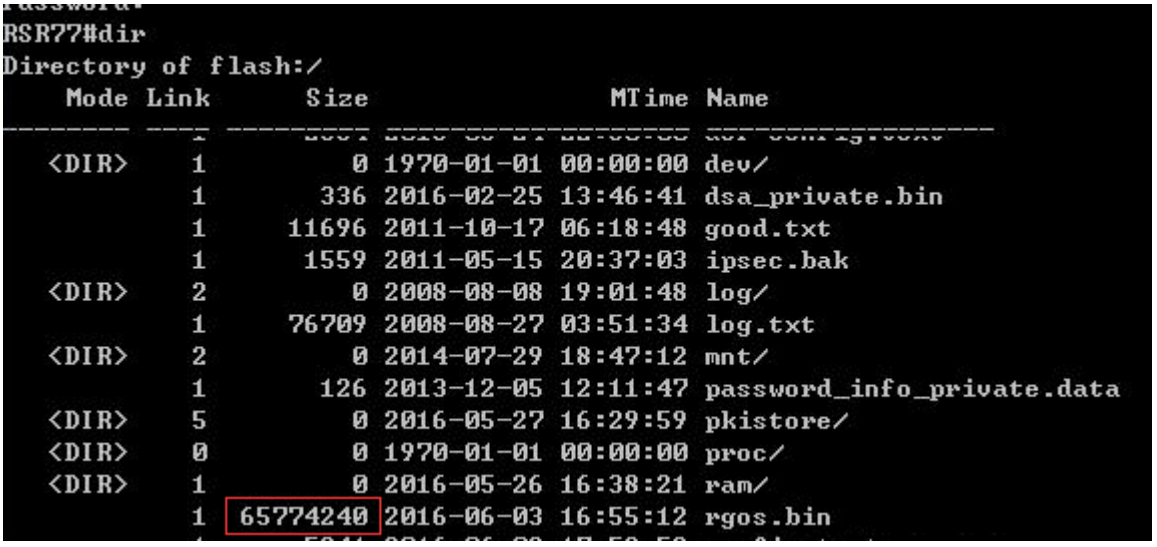
The file is transmitted.

Run the **bye** command to disable the connection to FTP Server.



4. Restart the device to check the upgrade result.

Log in to the device and run the **DIR** command to confirm whether the size in bytes of the rgos.bin file is consistent with the size in the release notes.



For a RSR77/77-X/50E-40 device, upgrade line cards.

```
Ruijie#upgrade system rgos.bin
These images in linecard will be updated:
     Slot     image    linecard
    ------    -----    ----------------------
      M1      CTRL                      SRCMI
      M2      CTRL                      SRCMI
              MAIN                      SRCMI
      1/0     CTRL                       SIP1
              MAIN                       SIP1
      4/0     CTRL                       SIP2
              MAIN                       SIP2
      1/1     CTRL             FNM-2CPOS-STM1
              MAIN             FNM-2CPOS-STM1
-----------------------------------------------
(Slot M1): Installing CTRL
Upgrading CTRL...
DO NOT POWER OFF!
Erasing device...eeeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash ######################## [OK - 1,331,968 bytes]
(Slot M1): CTRL installed.
(Slot M1): Install finish in slot M1 (SRCMI).
(Slot M2): Installing CTRL
(Slot M2): Download image!!!!!!!!!!!!!!!!!!!![OK - 1,331,712 bytes]
Waiting for image installed...Complete
Erasing device...eeeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash ######################## [OK - 1,331,968 bytes]
```

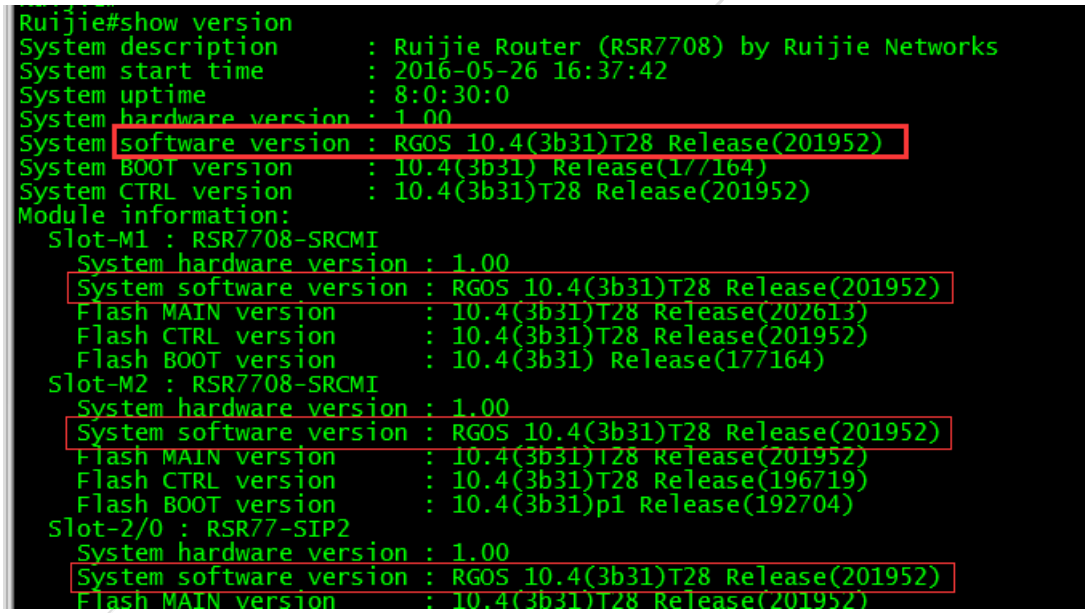
Save the configuration of the device, and restart the device.

Run the **Ruijie#write** command to save the configuration:

Run the **Ruijie#reload** command to restart the device:

```
Ruijie#reload
Proceed with reload? [no]y
```

After restart, run the **show version** command to confirm whether the device has been upgraded to the target version.



3.2 Password Restoration

3.2.1 Password Restoration with RGOS Version 10.X

I. Password Restoration Requirements

If an administrator forgets the login password, the administrator can enter the Boot layer to restore the password by using a configuration cable, and previous configuration needs to be reserved.

II. Password Restoration Principle

The device reads the **config.text** file during startup and the password is stored in the **config.text** file. Therefore, enter the BootLoader mode of the device and rename the file. When the device fails to locate the **config.text** file during startup, it directly enters the system. After the device enters the system, name the configuration file **config.text**, set a new password and save it. Then, you can log in to the device by using the new password next time.

III. Password Restoration

1. Get a configuration cable ready for password restoration. The device needs to be restarted and password restoration needs to be completed at the Boot layer.

2. Rename the configuration file rather than delete it during password restoration. Otherwise, the configuration will be lost.

IV. Configuration Steps

1. Restart the router to enter the CLI mode of the Boot layer.

Notes:

The operations of entering the CLI mode of the Boot layer from RSR routers are different for routers with RGOS later than or earlier than 10.4. You can directly enter the CLI mode of routers with RGOS later than 10.4, and you need to enter the menu mode first if the routers run RGOS earlier than 10.4.

1) Enter the CLI mode of the Boot layer from the router with RGOS later than 10.4.

Restart the router. When the "Press Ctrl+C to enter Boot ..." prompt is displayed, press **Ctrl+C** to enter the CLI mode of the Boot layer. The **BootLoader>** prompt is displayed.

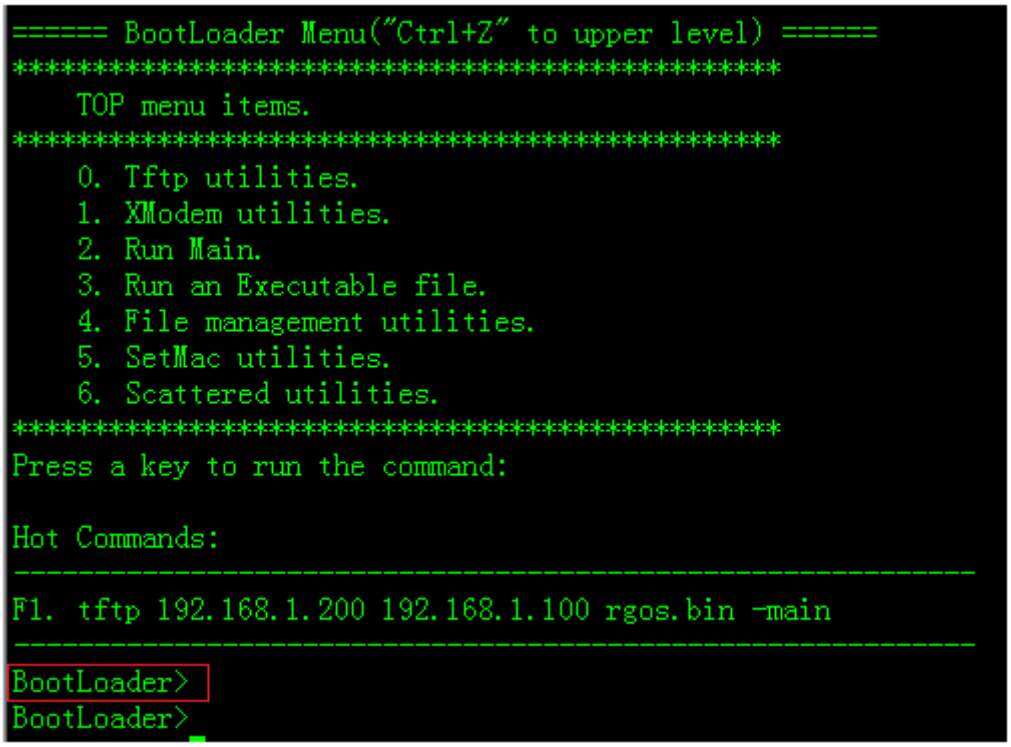
```
System bootstrap ...
Boot Version: RGOS 10.4(3b12) Release(151012)
Nor Flash ID: 0x017E1000, SIZE: 8388608Bytes
Using 500.000 MHz high precision timer.
MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 134217728) detected
Press Ctrl+C to enter Boot ...

Hot Commands:
------------------------------------------------------------
F1. tftp 192.168.64.3 192.168.64.1 rsr20-14e_5b8_111018_factory.bin_ -main
------------------------------------------------------------
BootLoader>
```

2) Enter the CLI mode of the Boot layer from the router with RGOS earlier than 10.4.

a. Restart the router. When the "Press Ctrl+C to enter Boot Menu ..." prompt is displayed, press **Ctrl+C** to enter the menu mode of the Boot layer.

```
Boot Version: RGOS 10.3(5b7), Release(115666)
Nor Flash ID: 0x00010049, SIZE: 2097152Bytes
MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 33554432) detected
MTD_DRIVER-5-MTD_NAND_FOUND: 1 nand chip(s) found on the target.
Waiting for subcard to initialize ..................
Press Ctrl+C to enter Boot Menu ...
```

b. In menu mode of the Boot layer, press **Ctrl+Q** to enter the CLI mode of the Boot layer. The **BootLoader>** prompt is displayed.



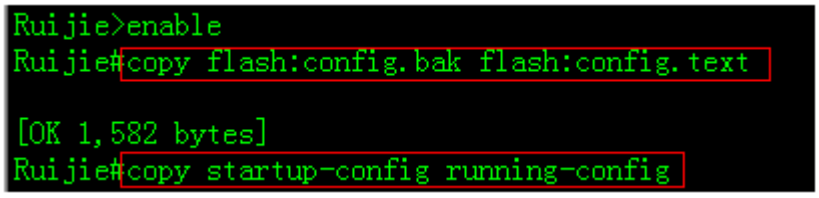
2. Rename the configuration file.

BootLoader>rename config.text config.bak

3. Restart the device.

BootLoader>reload

4. Restore the configuration file.



5. Set a new password and save device configuration.

```
RSR20-14E#configure terminal
RSR20-14E(config)#enable secret ruijie      //Set a new password.
RSR20-14E(config)#end
RSR20-14E#write        //Save device configuration.
```

After a new password is set, you can use it to log in to the system. Other configuration keeps unchanged.

3.2.2 Password Restoration on RSR77

I. Password Restoration Requirements

If an administrator forgets the login password, the administrator can enter the Ctrl layer to restore the password by using a configuration cable, and previous configuration needs to be reserved.

II. Password Restoration Principle

The device reads the **config.text** file during startup and the password is stored in the **config.text** file. Therefore, enter the Ctrl layer of the device and rename the file. When the device fails to locate the **config.text** file, it directly enters the system. After the device enters the system, name the configuration file **config.text**, set a new password and save it. Then, you can log in to the device by using the new password next time.

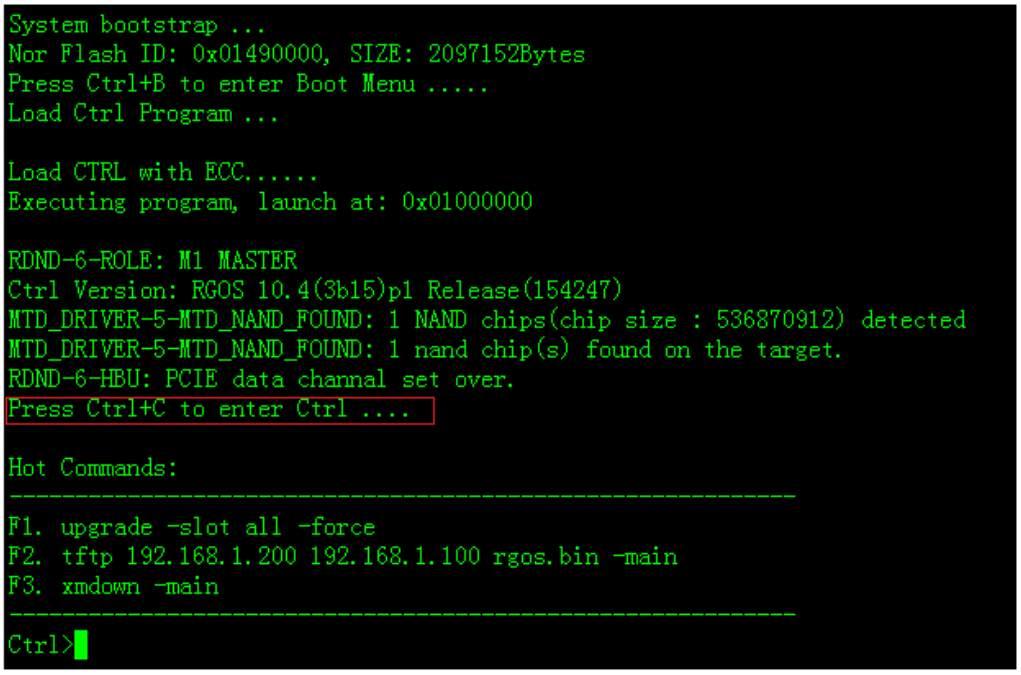
III. Password Restoration

1. Get a configuration cable ready for password restoration. The device needs to be restarted and password restoration needs to be completed at the Ctrl layer.
2. Rename the configuration file rather than delete it during password restoration. Otherwise, the configuration will be lost.

IV. Steps

1. Restart the router to enter the CLI mode of the Ctrl layer.

Restart the router. When the "Press Ctrl+C to enter Ctrl ..." prompt is displayed, press **Ctrl+C** to enter the CLI mode of the Ctrl layer. The **Ctrl>** prompt is displayed.



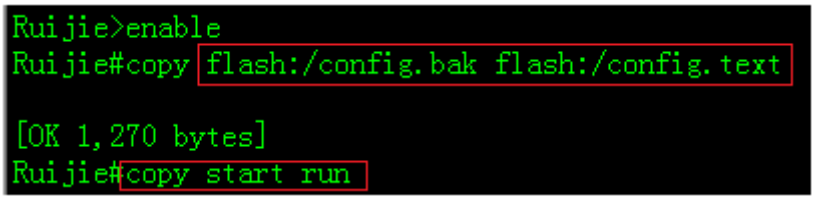
2. Rename the configuration file.

Ctrl>rename config.text config.bak // Rename the configuration file config.bak.

3. Restart the device.

Ctrl>reload

4. Restore the configuration file.



Note:

To copy the configuration file of routers with RGOS earlier than 10.4, the command must be **copy flash:/config.bak flash:/config.text** and a slash (/) must be added behind **flash:** to indicate the absolute path. The slash (/) does not need to be added for routers with RGOS later than 10.4.

5. Set a new password and save device configuration.

```
RSR7708#configure terminal
RSR7708(config)#enable secret ruijie
RSR7708(config)#end
RSR7708#*Mar  8 10:36:56: %SYS-5-CONFIG_I: Configured from console by console
*Mar  8 10:36:56: %PARAM-6-CONFIG_SYNC: Sync'ing the running configuration to the standby supervisor.
```

```
*Mar  8 10:36:56: %PARAM-6-CONFIG_SYNC: The running configuration has been successfully synchronized to the standby supervisor.
RSR7708#write
Building configuration...
[OK]
RSR7708#*Mar  8 10:37:01: %PARAM-6-CONFIG_SYNC: Sync'ing the startup configuration to the standby supervisor.
*Mar  8 10:37:01: %PARAM-6-CONFIG_SYNC: The startup configuration has been successfully synchronized to the standby supervisor.
```

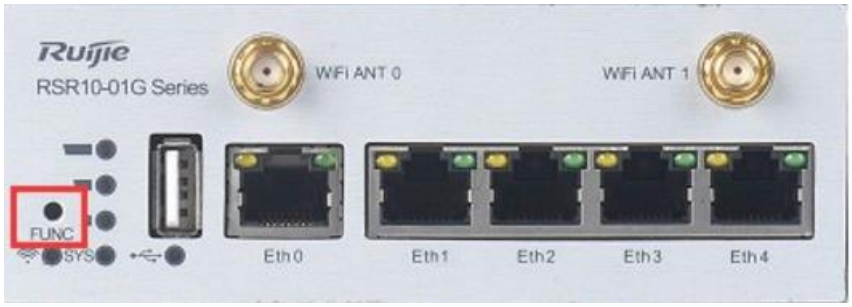
After a new password is set, you can use it to log in to the system. Other configuration keeps unchanged.

3.2.3 Password Restoration on 4G Router

I. Steps

RSR10-01G series 4G routers realize the password recovery by utilizing the “FUNC” button of devices. The recovery steps are as follows:

1. Restart the device, and press the “FUNC” key immediately for 6-10s.



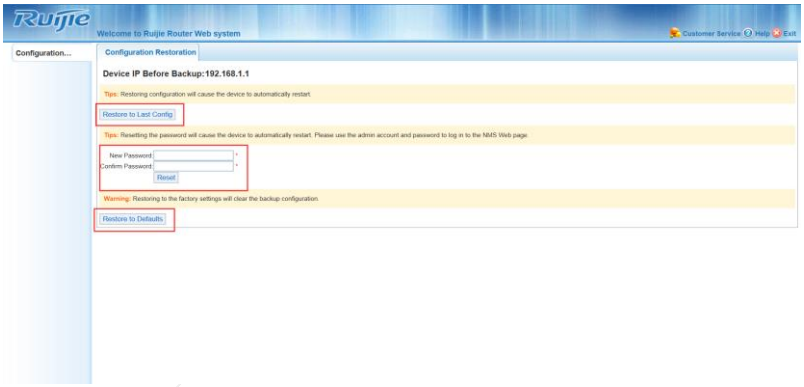
2. Changed the IP address of PC in same segment as router, using the default IP address to login the router Web interface

   1) Change the IP address of PC into 192.168.1.0/24 segment, we suggest modify the IP address to be the unique IP address of network, such as 192.168.1.2.

   2) Access http://192.168.1.1 with Chrome or Firefox browser, using account and password: admin/admin

.

3) The web interface will redirect to a recovery page.

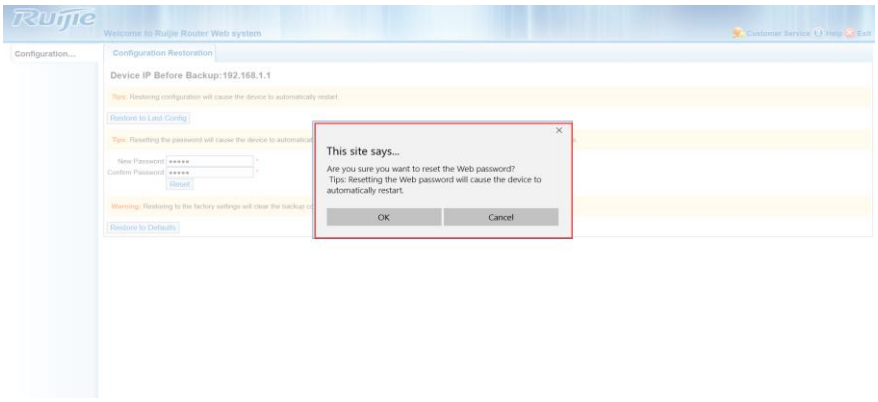


The recovery interface displays the original IP address of this device, the IP address usually is LAN gateway of Intranet. And this page also provides three options at the same time.

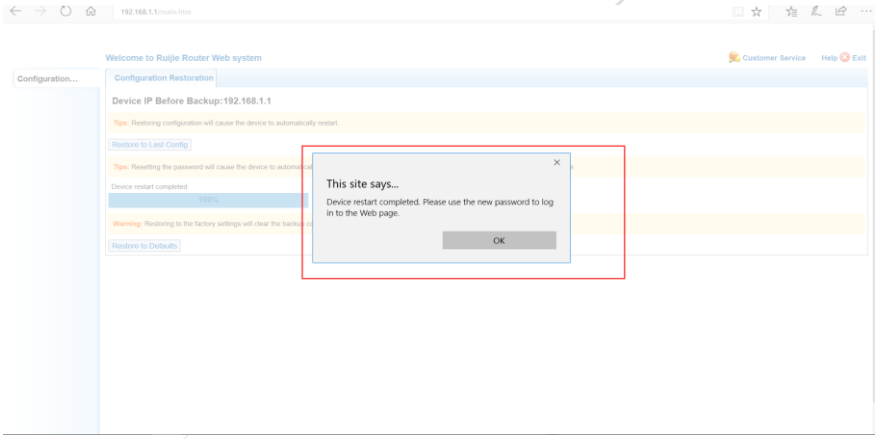
A. Recover to the latest configuration: use this function, the configuration of device will not be changed, it is used to the circumstance that the customer remembers the account and password of the device, but forget the IP address.

B. Reset the login password of web only: using this function, users can login the device by using “admin” as username and password, but all configuration is same as before (Attention: you need to login the router by using original IP address instead of 192.168.1.1 after using this function)

1) Perform the operation of resetting the password



input the new password and click the reset button t reset the web password



2) Access the original IP address

(the IP address is 192.168.100.254 during the instance.)

Change the IP address of PC to be any address during the 192.168.100.0 segment. Then open http://192.168.100.254 using web browser, login with admin (username) and ruijie(new password).

C. Factory reset, it will clear all configuration and recover the device into default login account and IP address.

3.3 Upgrade Firmware and Import Configuration Using FUNC Key

3.3.1 Upgrade Firmware Using Fun Key

Features

You can upgrade the device software in one-key mode by using the **FUNC** key. No commands need to be executed for the upgrade.

Notes:

1. The **FUNC** key must exist on the device or supervisor module (this key does not exist on devices of earlier versions and therefore, the one-key upgrade is not supported in such devices).
2. Access and convergence switches support one-key upgrade since version 3b12.
3. The RSR77 router supports one-key upgrade since version 3b21.

Principle

After the device is normally started and successfully identifies a USB flash drive or SD card, press the **FUNC** key. The system interrupts the current task and executes the FUNC key processing task. In the FUNC key processing task, the system detects whether an SD card or USB flash drive is inserted into the current device. If not, the system directly resets. If a storage medium is identified, the system scans the storage medium to detect whether an installation package in the specified file name format exists in the root directory. If an installation package in the correct format is detected, the system upgrades the device. After the upgrade ends, the system resets and restarts using the new software version.

Upgrade Steps

1. Get ready the bin file required for upgrade.

Copy the bin file into the root directory of the USB flash drive and rename it **rgos.bin**. It is strongly recommended that only one bin file be stored in the USB flash drive.

2. Insert the USB flash drive into the USB port of the device.

Wait till the USB indicator on the panel turns solid green, indicating that the device has correctly identified the USB flash drive.

3. Press FUNC to upgrade the device (the device cannot be powered off).

Use a small object to press the **FUNC** key. After **FUNC** is pressed, the device automatically starts upgrade. The USB indicator blinks and the device automatically resets after upgrade. After the SYS indicator turns solid green, the upgrade is complete. Log in to the device to check the version.

Verification

Run the **show version** command to check whether the device is upgraded successfully.

```
Ruijie#show version
System description      : Ruijie Router (RSR20-14-E) by Ruijie Networks
System start time       : 2015-01-29 11:53:33
System uptime           : 11:2:44:28
System hardware version : 1.00
System software version : RGOS 10.3(3b23), Release(174201)
System BOOT version     : 10.3.150859
System serial number    : 123456789efagd
Ruijie#
```

For RSR77 routers, run the **show version slot** command to display operating status of cards in slots and check that **Software Status** of each card is **running**. The following figure shows an example.

```
Ruijie#show version slots
Dev  Slot   MaxPorts   Configured-Module   Online-Module       Status
---  ----   --------   -----------------   -----------------   ------
1    M1     1          RSR7708-SRCMI       RSR7708-SRCMI       master
1    M2     1          RSR7708-SRCMI       RSR7708-SRCMI       slave
1    1/0    0          RSR77-SIP1          RSR77-SIP1          running
1    1/1    2          FNM-2CPOS-STM1      FNM-2CPOS-STM1      running
1    1/2    0                                                  none
1    2/0    0                                                  none
1    3/0    0                                                  none
1    4/0    2          RSR77-SIP2          RSR77-SIP2          running
1    4/1    8          DNME-8E1/CE1        DNME-8E1/CE1        running
1    4/2    0                                                  none
```

If you wait for a long time after software upgrade but **Status** is always **installed** or **running-config**, immediately contact Ruijie Network to seek technical support.

4 Configuration

4.1 Basic Function Configuration

4.1.1 Initial Configuration

Features

There is no startup configuration on Ruijie routers by default. You can log in to the management device by using a console cable. The following initial configuration is recommended to facilitate management and maintenance of devices.

Configuration

Host name (recommended):

```
Ruijie(config)#hostname XWRJ    //Name the device XWRJ.
XWRJ(config)#
```

Interface description (recommended):

```
XWRJ(config)#interface f0/0
XWRJ(config-if-FastEthernet 0/0)#description To_BJ
```

System clock (mandatory):

```
System time is very important. Fault logs and the CA certificate rely on timestamp.
Ruijie>enable
Ruijie#clock set 10:00:00 12 1 2012     //Set the clock in the format of hh:mm:ssmmddyyyy.
Ruijie#configure terminal        //Enter global configuration mode.
Ruijie(config)#clock timezone beijing 8    /Set the device time zone to East Area 8 (Beijing time).
```

Log recording (recommended):

Record logs in the flash memory. History logs are very useful for locating a fault. Note: Debug logs can be recorded only after the log level is set to 7.

```
XWRJ(config)#logging file flash:log 2000000 7
```

Management IP address (recommended):

In general, loopback 0 is used as the management interface according to customer network planning.

```
XWRJ(config)#interface loopback 0
XWRJ(config-if-Loopback 0)#ip address 1.1.1.1 255.255.255.255
```

Telnet (recommended):

Configure the telnet function for all network devices. If the telnet function is not configured, faults can be handled only at site.

```
XWRJ(config)#enable secret 0 ruijie     //The enable password must be configured for the telnet function.
XWRJ(config)#line vty 0 4
XWRJ(config-line)#password 0 ruijie
XWRJ(config-line)#login
```

Password encryption (recommended):

```
Router (config)# service password-encryption      //This command encrypts all passwords configured on the device.
```

4.1.2 Ruijie Express Forwarding (REF)

Features

Ruijie Express Forwarding (REF) is Ruijie-specific fast forwarding technology. All functions of the current router software version are implemented based on the REF platform. The IP REF function must be configured on all Layer-3 interfaces. If the REF function is not correctly enabled, device functions may be unavailable or the device may run abnormally.

The following exceptions may arise if the REF function is not correctly enabled on the device:

1. The CPU utilization of the device is high.
2. High delay, packet loss, and other exceptions occur on customer services forwarded or processed by the device.
3. Some functions are unavailable on the device.
4. The device runs abnormally and the device breaks down or restarts.

The REF function needs to be configured on the following devices:

RSR10, RSR20, RSR30, NPE50, RSR50, and RSR50E-80 series routers

The REF function does not need to be configured on the following devices:

RSR810, RSR820, RSR10-02E, RSR20-14E/F, RSR30-X, RSR50E-40, RSR77, RSR77-X series routers and new products released later, on which the IP REF function is enabled for all Layer-3 interfaces by default

Enabling the REF

1. Ensure that the IP REF function is configured on all Layer-3 interfaces of routers during project testing and engineering implementation.
2. Pay attention to the REF configuration of Layer-3 interfaces of routers during network inspection. If the REF function is not correctly configured, configure IP REF in a timely manner.

   Note: Services may be interrupted instantaneously when IP REF is configured. Therefore, configure it in non-peak hours of services.
3. The interfaces, on which the IP REF function needs to be configured, are as follows:

Ethernet interfaces:

```
interface FastEthernet
  ip ref
interface GigabitEthernet
  ip ref
```

Virtual interfaces:

```
interface Dialer
  ip ref
interface Group-Async
  ip ref
 interface Multilink
    ip ref
interface Tunnel
    ip ref
interface Virtual-ppp
    ip ref
interface Virtual-template
    ip ref
interface Vlan
    ip ref
```

WAN interfaces:

```
interface Async
  ip ref
interface ATM
  ip ref
interface  Pos
  ip ref
interface Serial
  ip ref
Controller e1
```

```
    ip ref
  Controller sonet
 ip ref
```

Note: The IP REF function cannot be configured on some interfaces of routers with RGOS earlier than 10.4. You do not need to memorize such interfaces but remember the following configuration principle: In interface configuration mode, run the **ip ref** command. If **ip ref** is executed, the IP REF function is needed on the interface.

4.1.3 DHCP

4.1.3.1 DHCP Basic Configuration

Features

The Dynamic Host Configuration Protocol (DHCP) operates based on client/server mode. The DHCP server dynamically allocates IP addresses, gateway addresses, DNS server addresses, and other parameters for clients.

DHCP supports two mechanisms for IP address allocation:

- Dynamic allocation: The DHCP server allocates an IP address to a client for a limited period of time (or until the client explicitly relinquishes the IP address).
- Manual allocation: Network administrators specify IP addresses for clients. Administrators can allocate specified IP addresses to clients by using DHCP.

Scenarios

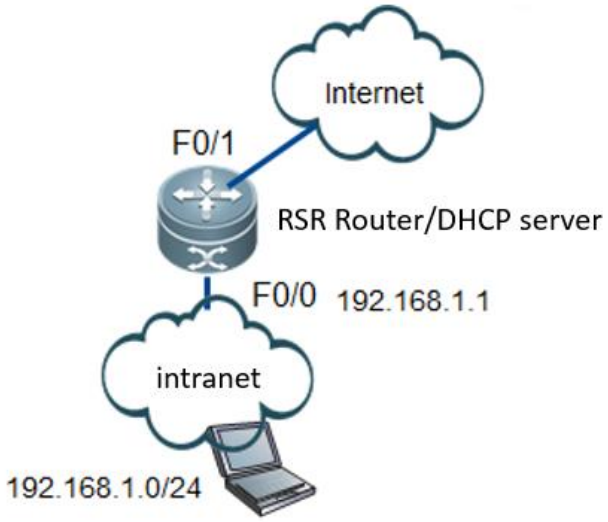
DHCP needs to be enabled on routers to meet enterprises' requirement that a host connecting to the network should be able to automatically obtain an IP address without extra configuration.

I.Networking Requirements

Requirement 1: common DHCP configuration

Requirement 2: Static IP addresses need to be allocated to specific PCs.

II. Networking Topology



III. Configuration Tips

1. Enable the DHCP service.
2. Configure the DHCP address pool.
3. (Optional) Configure IP addresses that cannot be allocated to PCs.
4. (Optional) Specify static IP addresses that need to be allocated to specific PCs.
5. Verify and save the configuration.

IV. Configuration Steps

Requirement 1: common DHCP configuration

1. Enable the DHCP service.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#service dhcp     //Enable the DHCP service(the DHCP service is disabled on RSR series routers by default and this command must be executed to enable it).
```

2. Configure the DHCP address pool.

```
Ruijie(config)#ip dhcp pool ruijie  //Create a DHCP address pool named ruijie.
Ruijie(dhcp-config)#lease 1 2 3 //1, 2, and 3 indicate day, hour, and minute respectively (addresses are released after 24 hours by default).
Ruijie(dhcp-config)#network 192.168.1.0 255.255.255.0 //The range of addresses that can be allocated is 192.168.1.1 to 192.168.1.254.
Ruijie(dhcp-config)#dns-server 8.8.8.8  6.6.6.6 //8.8.8.8 indicates the IP address of the primary DNS server and 6.6.6.6 indicates the IP address of the secondary DNS server.
```

```
Ruijie(dhcp-config)#default-router 192.168.1.1 //Gateway address. Only the IP address is required while the subnet mask is not needed.
Ruijie(dhcp-config)#exit
```

4. (Optional) Configure IP addresses that cannot be allocated to PCs.

```
Ruijie(config)#ip dhcp excluded-address 192.168.1.1  192.168.1.10   //192.168.1.1 to 192.168.1.10 should not be allocated by the DHCP server.
```

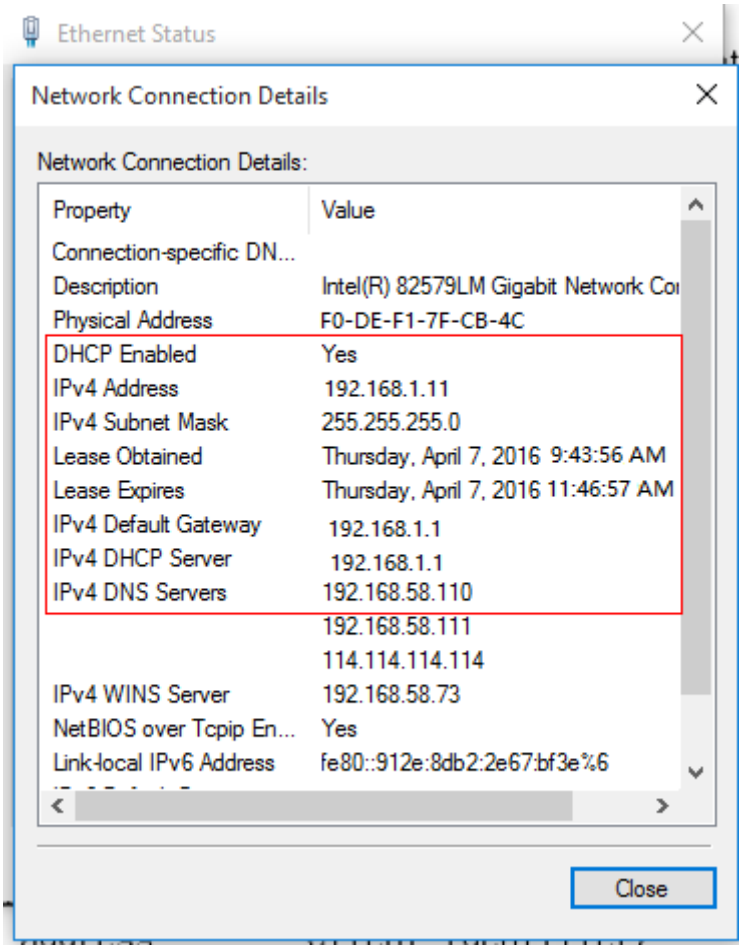
5. Verify and save the configuration.

```
Ruijie(config)#end
Ruijie#write      //Verify and save the configuration.
```

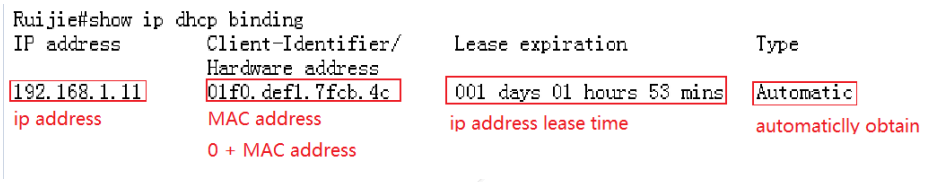
Verification

1) Set the network adapter of a PC to automatically obtain an IP address and then check whether the network adapter successfully obtains an IP address.

Right-click the network adapter of the PC, choose **Status** from the shortcut menu, and then click **Details**. The IP address obtained by the network adapter and other parameter values are displayed.



2) Display information about the IP address dynamically allocated on the router.



Requirement 2: Static IP addresses need to be allocated to specific PCs.

DHCP manual allocation. Assume that the PC with the MAC address of f0de.f17f.cb4c is required to automatically obtain the IP address 192.168.1.88.

Therefore, the DHCP server needs to allocate static IP addresses to clients with specific MAC addresses. There are two methods of allocating IP addresses based on the client MAC address identifier in the clients' DHCP requests:

1) Run the **client-identifier 01+mac** *address* command (**01** indicates that the network type is Ethernet).

2) Run the **hardware-address mac** *address* command.

Notes:

It is recommended that the **client-identifier** command be executed to allocate static IP addresses to clients with specific MAC addresses. If IP addresses fail to be manually allocated using the **client-identifier** command, run the **hardware-address** command.

1. Enable the DHCP service.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#service dhcp      //Enable the DHCP service(the DHCP service is disabled on RSR series routers by default and this command must be executed to enable it).
```

2. Specify static IP addresses that need to be allocated to specific PCs.

```
Ruijie(config)#ip dhcp pool zhangsan //Set the name of the static IP address pool to zhangsan.
Ruijie(dhcp-config)#client-identifier01f0.def1.7fcb.4c//Configure the client MAC address (this mode is recommended).
(Optional) Ruijie(dhcp-config)#hardware-address f0de.f17f.cb4c  //Configure the client MAC address (attempt this command if an IP address fails to be manually allocated using the client-identifier command).
Ruijie(dhcp-config)#host 192.168.1.88 255.255.255.0   //Configure the static IP address to be allocated and its subnet mask.
Ruijie(dhcp-config)#dns-server 8.8.8.8  6.6.6.6 //8.8.8.8 indicates the IP address of the primary DNS server and 6.6.6.6 indicates the IP address of the secondary DNS server.
Ruijie(dhcp-config)#default-router 192.168.1.1 //Configure the user gateway.
```

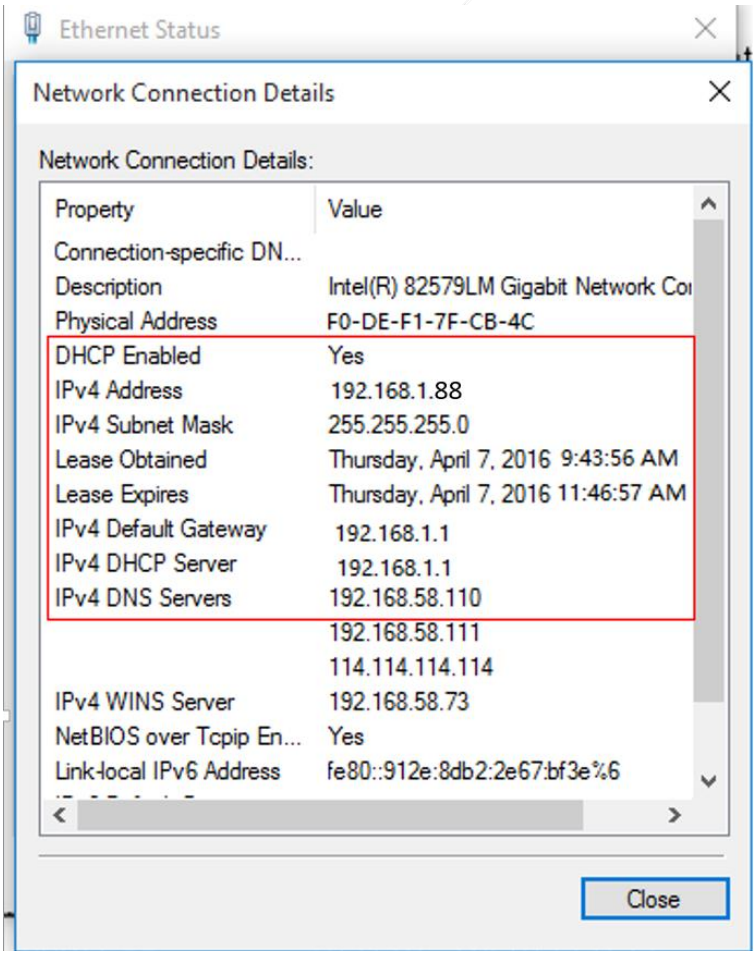
3. Verify and save the configuration.

```
Ruijie(config)#end
Ruijie#write      //Verify and save the configuration.
```

Verification

1) Set the network adapter of a PC to automatically obtain an IP address and then check whether the network adapter successfully obtains an IP address.

Right-click the network adapter of the PC, choose **Status** from the shortcut menu, and then click **Details**. The IP address obtained by the network adapter and other parameter values are displayed.



2) Display information about the allocated IP address on the router.

```
Ruijie#show ip dhcp binding
IP address        Client-Identifier/          Lease expiration        Type
                  Hardware address
192.168.1.88      01f0.def1.7fcb.4c           Infinite                Manual
```

IP address

MAC address

01 + MAC address

Infinite lease time

Manually obtain IP address

4.1.3.2 DHCP Relay

Features

The Dynamic Host Configuration Protocol (DHCP) relay is also called DHCP relay agent. If a DHCP client is in the same IP network segment as the DHCP server, the DHCP client can correctly obtain an IP address that is dynamically allocated. If a DHCP client is not in the same IP network segment as the DHCP server, DHCP relay agent is required. DHCP relay agent breaks the limitation that a DHCP server must exist in each IP network segment. It is capable of transmitting DHCP messages to a DHCP server in a different IP network segment and transmitting messages from a server to a DHCP client that is not in the same IP network segment as the DHCP server.

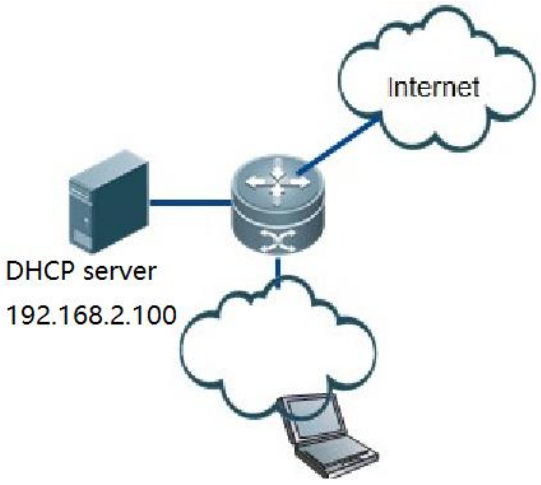
Scenarios

An enterprises needs to deploy a DHCP server but intranet users are not in the same network segment as the DHCP server. The DHCP relay function needs to be enabled on the gateway router of the users.

I.Networking Requirements

1) The DHCP server is an intranet server with the IP address of 192.168.2.100.
2) Intranet user hosts are connected to a router, which is in a different IP network segment from the DHCP server. The user hosts can automatically obtain IP addresses only by using DHCP relay.

II. Networking Topology



III. Configuration Tips

1. Enable the DHCP service.

2. Enable DHCP relay.

3. Verify and save the configuration.

IV. Configuration Steps

Notes:

1) The DHCP server can be a Windows- or Linux-based host with the DHCP service enabled or a router or switch configured with the DHCP service.

2) If an RSR router functions as a DHCP server, see section "DHCP" for the configuration (choose **Typical Configuration**>**Basic Function Configuration**>**DHCP**>**DHCP**).

3) Ensure that the DHCP server functions properly. Test method: Connect a PC to a switch that is in the same network segment as the DHCP server and set the server IP address to be in the same IP address segment as the DHCP client. Then, check whether the PC automatically obtains an IP address.

1. Enable the DHCP service.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#service dhcp      //Enable the DHCP service (the DHCP service is disabled on RSR series routers by default and this command must be executed to enable it).
```

2. Enable DHCP relay.

```
Ruijie(config)#ip helper-address 192.168.2.100 //Set the address of the DHCP relay to 192.168.2.100.
```

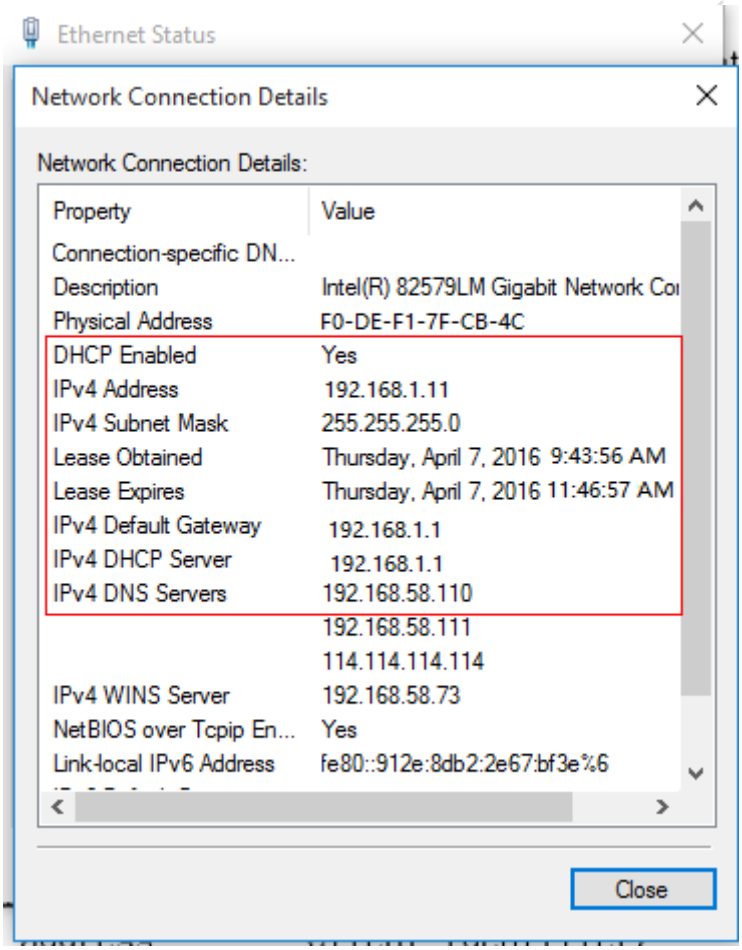
3. Verify and save the configuration.

```
Ruijie(config)#end
Ruijie#write      //Check that the configuration is correct and save the configuration.
```

V. Verification

1) Set the network adapter of a PC to automatically obtain an IP address and then check whether the network adapter successfully obtains an IP address.

Right-click the network adapter of the PC, choose **Status** from the shortcut menu, and then click **Details**. The IP address obtained by the network adapter and other parameter values are displayed.



2) Display information about the IP address dynamically allocated on the router.

```
Ruijie#show ip dhcp binding
IP address        Client-Identifier/          Lease expiration            Type
                  Hardware address
192.168.1.11      01f0.def1.7fcb.4c           001 days 01 hours 53 mins   Automatic
```

ip address

MAC address

0 + MAC address

ip address lease time

automaticlly obtain

4.1.4 Syslog

Features:

During operation, the device may encounter status changes (for example, the link status may switch between UP and DOWN) and some events (such as abnormal packets and handling exceptions). Ruijie product logs provide a mechanism where in case of status changes or events, messages in a fixed format are automatically generated and displayed in related windows (such as the console and Virtual Teletype Terminal (VTY)) or saved in related media (such as the memory buffer and flash) or transmitted to a set of log servers on the network for network diagnosis and troubleshooting by the administrator. To facilitate the administrator to read and manage logs and packets, the logs and packets can be marked with timestamps and numbers and classified by priorities.

I.Networking Requirements

When an exception occurs in the device, the administrator can check the cause via logs, and analyze and locate faults.

II. Configuration Tips

1. Enable/disable logs.
2. Enable log display on the VTY window.
3. Configure the buffer memory space for logs.
4. Save logs in the flash.
5. Send logs to the Syslog Server on the network.
6. Enable the log timestamp.
7. Run the **CLI** command to save logs.

III. Configuration Steps

1. Enable/disable logs.

Logs are enabled by default. If logs are disabled, the device will not print logs on the user window or send them to the Syslog Server or save them in related media (such as the buffer memory or flash).

```
Ruijie(config)#logging on      //Enables logs.
Ruijie(config)#no logging on    //Disables logs. Generally it is not recommended.
```

2. Enable log display on the VTY window.

Note:

Log in to the device through Telnet and SSH. Logs are not displayed by default. To display them, run the terminal monitor command.

```
Ruijie#terminal monitor //Enables log display on the VTY window.
Ruijie#terminal no monitor      //Disables log display on the VTY window.
```

3. Configure the buffer memory space for logs.

```
Ruijie(config)#logging buffered 1000000  7       //1000000 indicates that the buffer memory space of logs
is 1,000,000 bytes (when logs exceed the threshold, old logs are overwritten). 7 indicates that all logs
(including debugging data) are saved.
```

4. Save logs in the flash.

```
Ruijie(config)#logging file flash:log 6000000  7     //6000000 indicates that the buffer memory space of logs is 6,000,000 bytes (when logs exceed the threshold, old logs are overwritten). 7 indicates that all logs (including debugging data) are saved. 16 log.txt files are generated by default. Each file has a size of 6 MB and all files occupy 6*16=72 MB in the flash. Please rationally assign the value based on the total size of the flash.
```

Note:

When an exception occurs in the device, you need to collect logs and it is recommended to save them in the flash (logs are saved only in the memory by default and may be lost in case of power failure or device restart.)

a) Send logs to the Syslog Server on the network.

```
Ruijie(config)#logging server 192.168.1.2            //192.168.1.2 indicates the address of the Syslog Server.
Ruijie(config)#logging trap 7            //(Optional) Configures logs to be sent to the Syslog Server. 7 indicates that all logs (including debugging data) are saved.
Ruijie(config)#logging source interface loopback 0       //(Optional) Configures the source IP address where the device sends the syslog packets.
```

Note:

When an exception occurs in the device, you need to collect logs and it is recommended to send them to the Syslog Server on the network (logs are saved only in the memory by default and may be lost in case of power failure or device restart.)

5. Enable the log timestamp.

```
Ruijie(config)#service timestamps debug datetime msec //Enables the timestamp for debugging data.
Ruijie(config)#service timestamps log datetime msec  //Enables the timestamp for common logs.
```

6. Run the CLI command to save logs.

```
Ruijie(config)#logging userinfo command-log
```

4.2 IP routing

4.2.1 Static Route

4.2.1.1 Basic Configuration of Static Route

Features

Static routes are manually configured routes. With static routes, data packets can be transmitted to a specified target network along preset paths. When no dynamic routing protocol is available for learning routes to some target networks, configuring static routes is very significant.

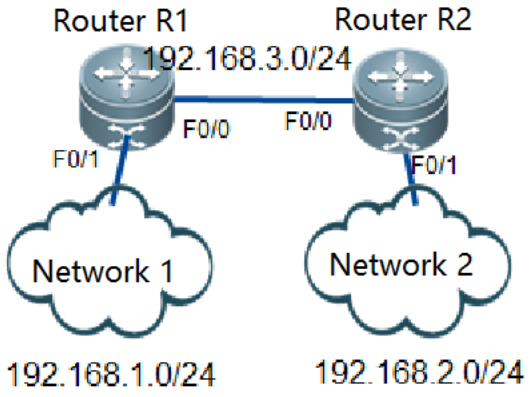
Scenarios

The network scale of an enterprise is small, with less than five routers, and mutual communication and data sharing are required throughout the network. Static routes can be configured on all routers in the network to meet this requirement.

I.Networking Requirements

Configure static routes to implement network connectivity.

II. Networking Topology



III. Configuration Tips

1. Configure IP addresses for interfaces of Router R1.
2. Configure IP addresses for interfaces of Router R2.
3. Configure a static route for Router R1.
4. Configure a static route for Router R2.
5. Save the configuration.

IV. Configuration Steps

1. Configure IP addresses for interfaces of Router R1.

```
Ruijie>enable    //Enter privileged EXEC mode.
Ruijie#configure terminal     //Enter global configuration mode.
Ruijie(config)#interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)#interface fastethernet 0/0
Ruijie(config-if-FastEthernet 0/0)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/0)#exit
```

2. Configure IP addresses for interfaces of Router R2.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.2.254 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)#interface fastethernet 0/0
Ruijie(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
Ruijie(config-if-FastEthernet 0/0)#exit
```

3. Configure a static route for Router R1.

Notes:

1) The next hop of static routes can be configured to two forms (next-hop IP address and local outbound interface). If the next hop of a static route is configured to local outbound interface, it is considered that the static route is a directly-connected route. In an Ethernet link, ARP information about each destination address needs to be parsed. If default routes are configured for a network egress and the next hop is configured to local outbound interface, a large number of ARP packets need to be parsed, which occupies large space in the ARP table. If the ARP proxy function is disabled at the peer end, the network may fail. If the next hop of a static route is configured to next-hop IP address, the static route is deemed to be a common recursive route.

2) When configuring static routes in an Ethernet link, configure the next hop in the form of outbound interface + next-hop IP address. If default routes are configured for a network egress, do not configure the next hop to local outbound interface.

3) It is recommended that the next hop of static routes be configured to local outbound interface for PPP and HDLC WAN links.

```
Ruijie(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2   //Configure a static route for
forwarding data packets with the destination IP address of 192.168.2.0/24 to the device with the IP
address of 192.168.3.2.
```

4. Configure a static route for Router R2.

```
Ruijie(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1   //Configure a static route for
forwarding data packets with the destination IP address of 192.168.1.0/24 to the device with the IP
address of 192.168.3.1.
```

5. Save the configuration.

```
Ruijie(config)#end  //Return to privileged EXEC mode.
Ruijie#write      //verify and save the configuration.
```

V. Verification

1. Ping the intranet address of the peer end from an intranet PC. If the ping succeeds, the static route is configured correctly.

To ping the intranet address of the peer end, do as follows: Choose **Start>Run**. In the **Run** dialog box, enter **cmd**. In the window that is displayed, enter **ping** *X.X.X.X* (*X.X.X.X* indicates the intranet IP address of the peer end).

2. Run the **Ruijie#show ip route** command to display information about routes.

Example of the static route configured for Router R1:

```
Ruijie#show ip route
Codes:C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
S192.168.2.0/24 [1/0] via 192.168.3.2
C192.168.3.0/24 is directly connected, FastEthernet 0/0
C192.168.3.1/32 is local host.
C192.168.1.0/24 is directly connected, FastEthernet 0/1
C192.168.1.254/32 is local host.
```

4.2.1.2 Floating Static Route

Features

When multiple routes with the same prefix exist on a network, the route with a smaller administrative distance (AD) value (route reliability, a smaller value indicates a higher route priority) is selected as the active route and the route with a larger AD value is used as a standby route. When the next hop of the active route is unreachable, the active route disappears and the standby route takes effect and becomes active. When multiple paths are reachable to a destination network, you can configure multiple static routes and set the AD value for the static routes to implement backup of active and standby links. This function is called floating static routing.

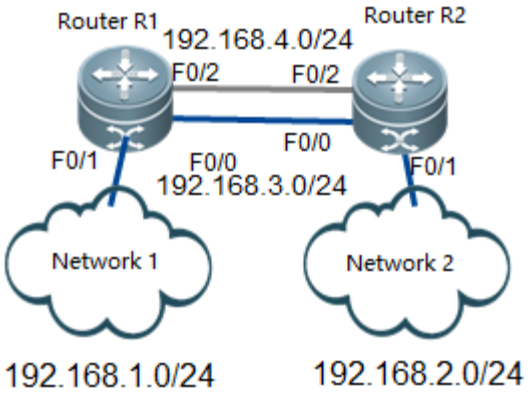
Scenarios

An enterprise has two egress links, with one functioning as active and the other functioning as standby. Normally, users of the enterprise access the network through the active link. When the active link fails, the router automatically switches traffic to the standby link, ensuring normal operation of the network. In this case, the floating static routing function can be enabled on the router.

I.Networking Requirements

1. The router has two paths reachable to the destination network.
2. When the active link (F0/0 in the example) fails (the interface is down or the link is disconnected), the standby link becomes active.

II. Networking Topology



III. Configuration Tips

1. Configure interface IP addresses for Router R1.
2. Configure interface IP addresses for Router R2.
3. Configure a static route for Router R1.
4. Configure a static route for Router R2.

IV. Configuration Steps

1. Configure interface IP addresses for Router R1.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface fastethernet 0/2
Ruijie(config-if-FastEthernet 0/2)#ip address 192.168.4.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/2)#interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)#interface fastethernet 0/0
Ruijie(config-if-FastEthernet 0/0)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/0)#exit
```

2. Configure interface IP addresses for Router R2.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface fastethernet 0/2
Ruijie(config-if-FastEthernet 0/2)#ip address 192.168.4.2 255.255.255.0
Ruijie(config-if-FastEthernet 0/2)#interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.2.254 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)#interface fastethernet 0/0
Ruijie(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
Ruijie(config-if-FastEthernet 0/0)#exit
```

3. Configure a static route for Router R1.

Notes:

1) The next hop of static routes can be configured to two forms (next-hop IP address and local outbound interface). If the next hop of a static route is configured to local outbound interface, it is considered that the static route is a directly-connected route. In an Ethernet link, ARP information about each destination address needs to be parsed. If default routes are configured for a network egress and the next hop is configured to local outbound interface, a large number of ARP packets need to be parsed, which occupies large space in the ARP table. If the ARP proxy function is disabled at the peer end, the network may fail. If the next hop of a static route is configured to next-hop IP address, the static route is deemed to be a common recursive route.

2) It is recommended that the next hop of a static route be configured to next-hop IP address in an Ethernet link. If default routes are configured for a network egress, do not configure the next hop to local outbound interface.

3) The next hop of static routes can be configured to local outbound interface or next-hop IP address in PPP and HDLC WAN links, because PPP and HDLC links are point-to-point links and Layer-2 address resolution is not involved.

4) If the next hop of a static route is configured to local outbound interface, it is considered that the static route is a directly-connected route and the default AD is 0. If the next hop of a static route is configured to next-hop IP address, it is considered that the static route is a common recursive route and the default AD is 1.

```
Ruijie(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2      //Configure a static route for
forwarding data packets with the destination IP address of 192.168.2.0/24 to the device with the IP
address of 192.168.3.2.
```

```
Ruijie(config)#ip route 192.168.2.0 255.255.255.0 192.168.4.2 10 //Configure a static route for forwarding data packets with the destination IP address of 192.168.2.0/24 to the device with the IP address of 192.168.4.2 and set AD to 10 (the default AD is 1 and a smaller AD indicates a higher route priority).
```

4. Configure a static route for Router R2.

```
Ruijie(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1  //Configure a static route for forwarding data packets with the destination IP address of 192.168.1.0/24 to the device with the IP address of 192.168.3.1.
Ruijie(config)#ip route 192.168.1.0 255.255.255.0 192.168.4.1 10   //Configure a static route for forwarding data packets with the destination IP address of 192.168.1.0/24 to the device with the IP address of 192.168.4.1 and set AD to 10 (the default AD is 1 and a smaller AD indicates a higher route priority).
```

V. Verification

Example of the static route configured for Router R1:

1. Remove the cable of the active link (F0/0) connected to Router R1 and run the **Ruijie#show ip route** command to display the route and check whether the route is switched to the standby link:

   Example of the static route configured for Router R1:

2. When the active link (F0/0 in the example) is normal, run the **Ruijie#show ip route** command to display the route:

```
Ruijie#show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
S    192.168.2.0/24 [1/0] via 192.168.3.2       //Data packets destined for 192.168.2.0 are transmitted along the active link F0/0 and the next hop is 192.168.3.2.
C    192.168.1.0/24 is directly connected, FastEthernet 0/1
C    192.168.1.254/32 is local host.
C    192.168.3.0/24 is directly connected, FastEthernet 0/0
C    192.168.3.1/32 is local host.
C    192.168.4.0/24 is directly connected, FastEthernet 0/2
C    192.168.4.1/32 is local host.
```

```
Ruijie#show ip route
```

```
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
S    192.168.2.0/24 [10/0] via 192.168.4.2       //Data packets destined for 192.168.2.0 are transmitted along the standby link F0/2 and the next hop is 192.168.4.2. The active/standby links are switched successfully.
C    192.168.1.0/24 is directly connected, FastEthernet 0/1
C    192.168.1.254/32 is local host.
C    192.168.4.0/24 is directly connected, FastEthernet 0/2
C    192.168.4.2/32 is local host.
```

4.2.1.3 VRF Static Route

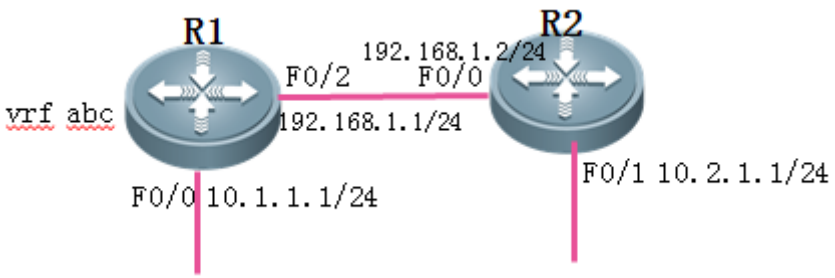
Features

When multiple interfaces on a router belong to the same Virtual Routing & Forwarding (VRF) table and data needs to be forwarded by these interfaces, VRF static routing needs to be configured for data forwarding.

I.Networking Requirements

As shown in the following figure, Interfaces F0/0 and F0/2 of Router R1 belong to the VRF table named abc, Router R2 is a common global router, and network-wide interworking needs to be implemented.

II. Networking Topology



III. Configuration Tips

1. Configure a VRF table named abc on Router R1.
2. Configure basic IP addresses.
3. Add interfaces on Router R1 to the VRF table.
4. Configure static routes.

IV. Configuration Steps

1. Configure a VRF table named abc on Router R1.

Notes:

VRF is locally effective. When VRF is enabled at the local end, interfaces on the local router that belong to the same VRF table can interwork with each other. Interfaces that belong to different VRF tables are logically isolated, regardless of whether VRF is enabled on the peer router.

```
Ruijie(config)#hostname R1
R1(config)#ip vrf abc //Enable a VRF table named abc on the router.
R1(config-vrf)#exit
```

2. Configure basic IP addresses.

```
R1(config)#interface fastEthernet 0/2
R1(config-if-FastEthernet 0/2)#ip ref
R1(config-if-FastEthernet 0/2)#ip address 192.168.1.1 255.255.255.0
R1(config-if-FastEthernet 0/2)#exit
R1(config)#interface fastEthernet 0/0
R1(config-if-FastEthernet 0/0)#ip ref
R1(config-if-FastEthernet 0/0)#ip address 10.1.1.1 255.255.255.0
R1(config-if-FastEthernet 0/0)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface fastEthernet 0/0
R2(config-if-FastEthernet 0/0)#ip ref
R2(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-if-FastEthernet 0/0)#exit
R2(config)#interface fastEthernet 0/1
R2(config-if-FastEthernet 0/1)#ip ref
R2(config-if-FastEthernet 0/1)#ip address 10.2.1.1 255.255.255.0
R2(config-if-FastEthernet 0/1)#exit
```

3. Add interfaces on Router R1 to the VRF table.

Notes:

When an interface is added to a VRF table and an IP address has been configured for the interface, the IP address will be deleted and you need to reconfigure an IP address for the interface.

```
R1(config)#interface fastEthernet 0/2
R1(config-if-FastEthernet 0/2)#ip vrf forwarding abc //Configure the VRF table named ABC.
% Interface FastEthernet 0/2 IP address 192.168.1.1 removed due to enabling VRF abc
R1(config-if-FastEthernet 0/2)#ip address 192.168.1.1 255.255.255.0       //Reconfigure an IP address for Interface F0/2.
R1(config-if-FastEthernet 0/2)#exit
R1(config)#interface fastEthernet 0/0
R1(config-if-FastEthernet 0/0)#ip vrf forwarding abc    //Add the interface to the VRF table named abc.
% Interface FastEthernet 0/0 IP address 10.1.1.1 removed due to enabling VRF abc
R1(config-if-FastEthernet 0/0)#ip address 10.1.1.1 255.255.255.0    //Reconfigure an IP address for the interface.
R1(config-if-FastEthernet 0/0)#exit
```

4. Configure static routes.

Notes:

In addition to commands for configuring static routes, the **vrf** *abc* command needs to be executed for configuring VRF static routes. The precautions for configuring VRF static routes are the same as those for configuring common static routes. For details, see static route configuration.

```
R1(config)#ip route vrf abc 10.2.1.0 255.255.255.0 192.168.1.2          //Configure a static route in the VRF table named abc.
R2(config)#ip route 10.1.1.0 255.255.255.0 192.168.1.1        //Configure a common static route on R2 because VRF is not enabled on Router R2.
```

V. Verification

1. Ping the intranet address of the peer end from an intranet PC. If the ping operation succeeds, the VRF static routing is configured correctly.

   To ping the intranet address of the peer end, do as follows: Choose Start > Run. In the Run dialog box, enter cmd. In the window that is displayed, enter ping X.X.X.X (X.X.X.X indicates the intranet IP address of the peer end).

2. Run the **show ip route vrf abc** command to display the VRF route.

```
R1#show ip route vrf abc
Routing Table: abc

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.1.0/24 is directly connected, FastEthernet 0/0
C    10.1.1.1/32 is local host.
S    10.2.1.0/24 [1/0] via 192.168.1.2
C    192.168.1.0/24 is directly connected, FastEthernet 0/2
C    192.168.1.1/32 is local host.
```

4.2.2 RIP

4.2.2.1 Basic configuration of RIP

Features

The Routing Information Protocol (RIP) is an old routing protocol, which is widely applied in small-sized networks and networks using the same medium. RIP adopts the distance vector algorithm and therefore it is a distance vector protocol. RIPv1 is defined in RFC 1058 and RIPv2 is defined in RFC 2453. Ruijie RGOS software supports both RIPv1 and RIPv2. RIP uses UDP packets to exchange routing information and the UDP port ID is 520. Normally, RIPv1 packets are broadcast packets while RIPv2 packets are multicast packets, with the multicast address of 224.0.0.9. RIP sends an update packet every other 30 seconds. If a device fails to receive a route update packet from the peer end within 180 seconds, it marks all routes from the peer end as unreachable. After that, if the device still fails to receive a route update packet from the peer end within 120 seconds, the device deletes the routes from the routing table.

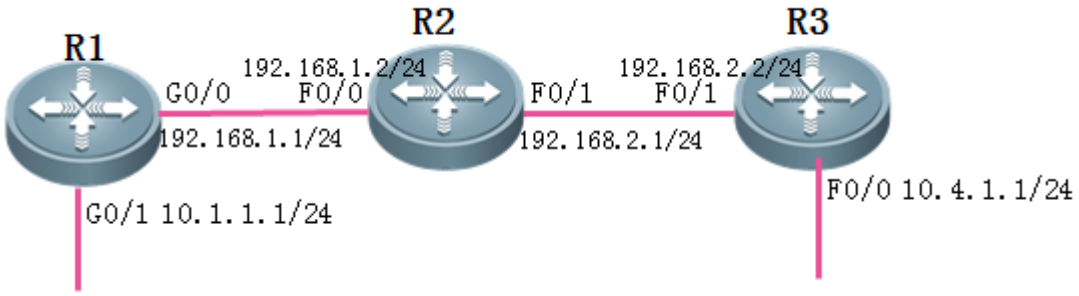
Scenarios

The network scale of an enterprise is small, with less than ten routers, and mutual communication and data sharing are required throughout the network. Therefore, RIP needs to be enabled on all routers in the network.

I.Networking Requirements

The RIP protocol needs to run on routers throughout the network so that routes across the network are reachable.

II. Networking Topology



III. Configuration Tips

1. Configure basic IP addresses for routers throughout the network.
2. Enable RIP on routers throughout the network and advertise interfaces to the RIP process.

IV. Configuration Steps

1. Configure basic IP addresses for routers throughout the network.

```
Ruijie(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
R1(config-GigabitEthernet 0/0)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
R1(config-GigabitEthernet 0/1)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface fastEthernet 0/0
R2(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-if-FastEthernet 0/0)#exit
R2(config)#interface fastEthernet 0/1
R2(config-if-FastEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
R2(config-if-FastEthernet 0/1)#exit
```

```
Ruijie(config)#hostname R3
R3(config)#interface fastEthernet 0/0
R3(config-if-FastEthernet 0/0)#ip address 10.4.1.1 255.255.255.0
R3(config-if-FastEthernet 0/0)#exit
R3(config)#interface fastEthernet 0/1
R3(config-if-FastEthernet 0/1)#ip address 192.168.2.2 255.255.255.0
R3(config-if-FastEthernet 0/1)#exit
```

2. Enable RIP on routers throughout the network and advertise interfaces to the RIP process.

Notes:

1) There are two RIP versions: RIPv1 and RIPv2. RIPv2 uses multicast update packets to replace broadcast update packets and carries mask information of routes in the packets. Therefore, RIPv2 is recommended.

2) When the **network** command is executed to advertise a network over RIP, only the classful network is advertised even if a subnet address is entered in this command. All interfaces that belong to this classful network will be advertised to the RIP process.

3) By default, RIP performs automatic summarization at the border of the classful network. If the classful network is discontinuous, a routing learning exception will be incurred. Therefore, it is recommended that automatic summarization be disabled after RIP is enabled, and manual summarization be adopted.

```
R1(config)#router rip
R1(config-router)#version 2          //Enable RIPv2.
R1(config-router)#no auto-summary       //Disable automatic summarization.
R1(config-router)#network 192.168.1.0     //Advertise the network segment 192.168.1.0 to the RIP process.
R1(config-router)#network 10.0.0.0
R1(config-router)#exit
```

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#exit
```

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#no auto-summary
R3(config-router)#network 192.168.2.0
R3(config-router)#network 10.0.0.0
R3(config-router)#exit
```

V. Verification

Check routes on routers throughout the network. If each router successfully learns routes throughout the network, RIP is configured correctly.

```
R1#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    1.1.1.1/32 is local host.
C    10.1.1.0/24 is directly connected, GigabitEthernet 0/1
C    10.1.1.1/32 is local host.
R    10.4.1.0/24 [120/2] via 192.168.1.2, 00:00:17, GigabitEthernet 0/0
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.1.1/32 is local host.
R    192.168.2.0/24 [120/1] via 192.168.1.2, 00:07:19, GigabitEthernet 0/0
```

4.2.2.2 RIP in VRF

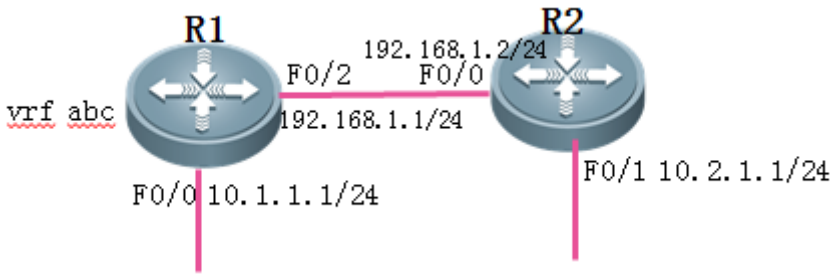
Features

The Routing Information Protocol (RIP) is an old routing protocol, which is widely applied in small-sized networks and networks using the same medium. RIP adopts the distance vector algorithm and therefore it is a distance vector protocol. RIPv1 is defined in RFC 1058 and RIPv2 is defined in RFC 2453. Ruijie RGOS software supports both RIPv1 and RIPv2. RIP uses UDP packets to exchange routing information and the UDP port ID is 520. Normally, RIPv1 packets are broadcast packets while RIPv2 packets are multicast packets, with the multicast address of 224.0.0.9. RIP sends an update packet every other 30 seconds. If a device fails to receive a route update packet from the peer end within 180 seconds, it marks all routes from the peer end as unreachable. After that, if the device still fails to receive a route update packet from the peer end within 120 seconds, the device deletes the routes from the routing table.

I.Networking Requirements

As shown in the following figure, Interfaces F0/0 and F0/2 of Router R1 belong to a VRF table named abc, and Router R2 is a common global router. The RIP protocol needs to be configured on routers throughout the network to so that routes across the network are reachable.

II. Networking Topology



III. Configuration Tips

1. Configure a VRF table named abc on Router R1.
2. Configure basic IP addresses.
3. Add interfaces on Router R1 to the VRF table.
4. Enable RIP on routers throughout the network and advertise interfaces to the RIP process.

IV. Configuration Steps

1. Configure a VRF table named abc on Router R1.

Notes:

VRF is locally effective. When VRF is enabled at the local end, interfaces on the local router that belong to the same VRF table can interwork with each other. Interfaces that belong to different VRF tables are logically isolated, regardless of whether VRF is enabled on the remote router.

```
Ruijie(config)#hostname R1
R1(config)#ip vrf abc //Enable a VRF table named abc on the router.
R1(config-vrf)#exit
```

2. Configure basic IP addresses.

```
R1(config)#interface fastEthernet 0/2
R1(config-if-FastEthernet 0/2)#ip address 192.168.1.1 255.255.255.0
R1(config-if-FastEthernet 0/2)#exit
R1(config)#interface fastEthernet 0/0
R1(config-if-FastEthernet 0/0)#ip address 10.1.1.1 255.255.255.0
R1(config-if-FastEthernet 0/0)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface fastEthernet 0/0
R2(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-if-FastEthernet 0/0)#exit
R2(config)#interface fastEthernet 0/1
R2(config-if-FastEthernet 0/1)#ip address 10.2.1.1 255.255.255.0
```

```
R2(config-if-FastEthernet 0/1)#exit
```

3. Add interfaces on Router R1 to the VRF table.

Notes:

When an interface is added to a VRF table and an IP address has been configured for the interface, the IP address will be deleted and you need to reconfigure an IP address for the interface.

```
R1(config)#interface fastEthernet 0/2
R1(config-if-FastEthernet 0/2)#ip vrf forwarding abc
% Interface FastEthernet 0/2 IP address 192.168.1.1 removed due to enabling VRF abc
R1(config-if-FastEthernet 0/2)#ip address 192.168.1.1 255.255.255.0       //Reconfigure an IP address for Interface F0/2.
R1(config-if-FastEthernet 0/2)#exit
R1(config)#interface fastEthernet 0/0
R1(config-if-FastEthernet 0/0)#ip vrf forwarding abc
% Interface FastEthernet 0/0 IP address 10.1.1.1 removed due to enabling VRF abc
R1(config-if-FastEthernet 0/0)#ip address 10.1.1.1 255.255.255.0
R1(config-if-FastEthernet 0/0)#exit
```

4. Enable RIP on routers throughout the network and advertise interfaces to the RIP process.

Notes:

To configure VRF RIP, run the **address-family ipv4 vrf** command after enabling RIP. The precautions for configuring VRF RIP are the same as those for configuring common RIP. For details, see RIP basic configuration.

```
R1(config)#router rip
R1(config-router)#address-family ipv4 vrf abc //Enable RIP after enabling the VRF table named abc.
R1(config-router-af)#version 2     //Enable RIPv2.
R1(config-router-af)#no auto-summary    //Disable automatic summarization.
R1(config-router-af)#network 192.168.1.0   //Advertise the network segment 192.168.1.0 to the RIP process.
R1(config-router-af)#network 10.0.0.0
R1(config-router-af)#exit
R1(config-router)#exit
```

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.1.0
R2(config-router)#network 10.0.0.0
R2(config-router)#exit
```

V. Verification

Check the VRF routing table on Router R1 and global routing tables on other routers. If each router successfully learns routes throughout the network, VRF RIP is configured correctly.

```
R1#show ip route vrf abc
Routing Table: abc

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.1.0/24 is directly connected, FastEthernet 0/0
C    10.1.1.1/32 is local host.
R    10.2.1.0/24 [120/1] via 192.168.1.2, 00:02:53, FastEthernet 0/2
C    192.168.1.0/24 is directly connected, FastEthernet 0/2
C    192.168.1.1/32 is local host.
```

4.2.2.3 Redistribution

Features

The route redistribution function imports routes learnt from other routing protocols to the Routing Information Protocol (RIP) domain.

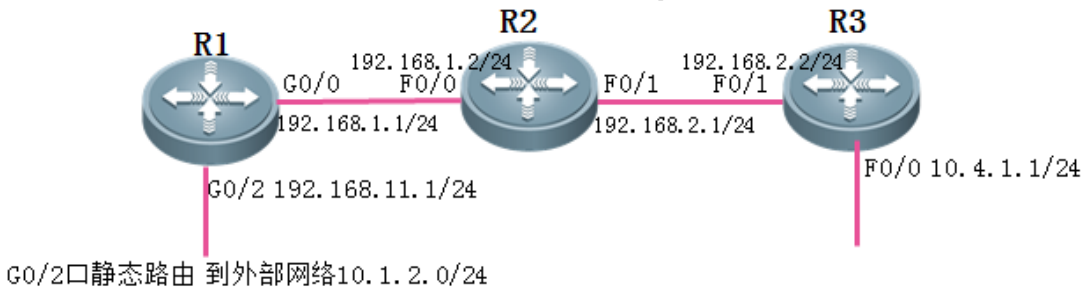
Scenarios

Multiple routing protocols are enabled on the network of an enterprise, and mutual communication and data sharing are required throughout the network. Therefore, routes learnt by other routing protocol need to be imported to the RIP domain.

I.Networking Requirements

In addition to RIP, other routing protocols run on the network, and routes learnt by other routing protocols need to be redistributed to RIP.

II. Networking Topology



III. Configuration Tips

1. Configure IP addresses and basic RIP information for routers throughout the network.
2. Configure a static route destined for the network 10.1.2.0/24 on Router R1.
3. Redistribute the static route to the RIP domain.

IV. Configuration Steps

1. Configure IP addresses and basic RIP information for routers throughout the network.

For the configuration, see RIP basic configuration (choose **Typical Configuration**>**IP Routing**>**RIP**>**Basic Configuration**).

2. Configure a static route destined for the network 10.1.2.0/24 on Router R1.

```
R1(config)#ip route 10.1.2.0 255.255.255.0 192.168.11.2
```

3. Redistribute the static route to the RIP domain.

Notes:

1) The commands for RIP to redistribute routes learnt by other routing protocols are as follows:

```
R1(config)#router rip
R1(config-router)#redistribute ?
  bgp        Border Gateway Protocol (BGP)
  connected   Connected
  ospf        Open Shortest Path First (OSPF)
  static       Static routes
```

1) External routes imported by RIP are effective routes on the local router and must be the routes that can be displayed after the **show ip route** command is executed on the local router.

2) A metric must be specified for external routes imported by RIP. The default metric value is infinite and the imported external routes with the metric unspecified are ineffective.

The following example is based on import of a static route by RIP. The import of other routes is the same as that of a static route.

```
R1(config)#router rip
```

```
R1(config-router)#redistribute static metric 1      //Redistribute the static route to the RIP domain and set metric to 1.
R1(config-router)#exit
```

V. Verification

Check routes on other routers. If the other routers successfully learn the route destined for the external network 10.1.2.0/24, redistribution is configured correctly.

```
R2#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    2.2.2.2/32 is local host.
R    10.1.1.0/24 [120/1] via 192.168.1.1, 00:18:37, FastEthernet 0/0
R    10.1.2.0/24 [120/1] via 192.168.1.1, 00:00:53, FastEthernet 0/0
R    10.4.1.0/24 [120/1] via 192.168.2.2, 00:11:35, FastEthernet 0/1
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
```

4.2.2.4 Summarization

Features

The route summarization function enables the Routing Information Protocol (RIP) to summarize specific routes learnt by or generated by RIP and transfer them to RIP neighbors, so as to reduce route entries on routers.

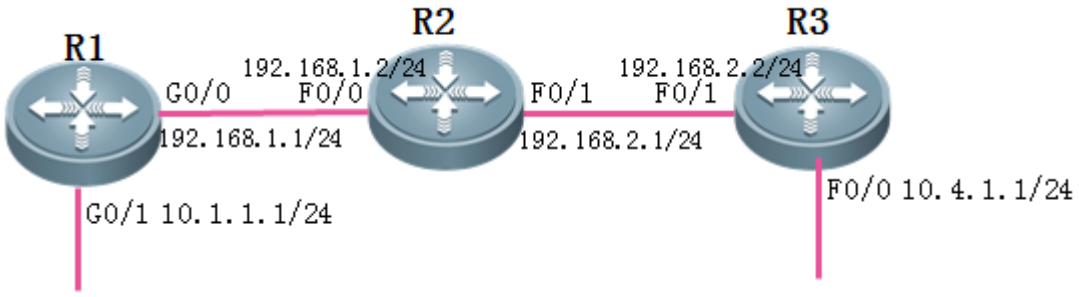
Scenarios

There are numerous IP network segments in the network of an enterprise. Route summarization can be configured on routers to reduce route entries on the routers and improve router performance.

I.Networking Requirements

Specific routes learnt by RIP need to be summarized to reduce route entries.

II. Networking Topology



III. Configuration Tips

1. Configure IP addresses and basic RIP information for routers throughout the network.
2. Configure route summarization.

IV. Configuration Steps

1. Configure IP addresses and basic RIP information for routers throughout the network.

For the configuration, see RIP basic configuration (choose **Typical Configuration** > **IP Routing** > **RIP** > **Basic Configuration**).

2. Configure route summarization.

Notes:

1) RIP can summarize routes generated by RIP or learnt from neighbors on outbound interfaces, but cannot perform supernetting summarization on these routes.

2) Automatic summarization must be disabled before routes learnt or generated by RIP are manually summarized.

```
R1(config)#router rip
R1(config-router)#no auto-summary       //Disable automatic summarization.
R1(config-router)#exit
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip rip summary-address 10.1.0.0 255.255.0.0     //Summarize the route as
10.1.0.0/16.
R1(config-GigabitEthernet 0/0)#exit
```

V. Verification

Check routes on routers throughout the network. If all the routers correctly learn the summarized route, route summarization of RIP is configured correctly.

```
R2#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    2.2.2.2/32 is local host.
R    10.1.0.0/16 [120/1] via 192.168.1.1, 00:02:59, FastEthernet 0/0
R    10.4.1.0/24 [120/1] via 192.168.2.2, 00:25:46, FastEthernet 0/1
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
```

4.2.3 OSPF

4.2.3.1 Basic Configuration of OSPF

Features

The Open Shortest Path First (OSPF) protocol is a link status-based internal gateway routing protocol, developed by the OSPF Working Group of Internet Engineering Task Force (IETF). OSPF is exclusively designed for IP. It directly runs at the IP layer and the protocol ID is 89. OSPF packets are exchanged in multicast mode, with the multicast address of 224.0.0.5 (to all OSFP routers) or 224.0.0.6 (to designated routers). When an OSPF routing domain is large, a hierarchical structure is often adopted. That is, an OSPF routing domain is divided into several areas, which are interconnected through a backbone area. Each non-backbone area needs to be directly connected to the backbone area.

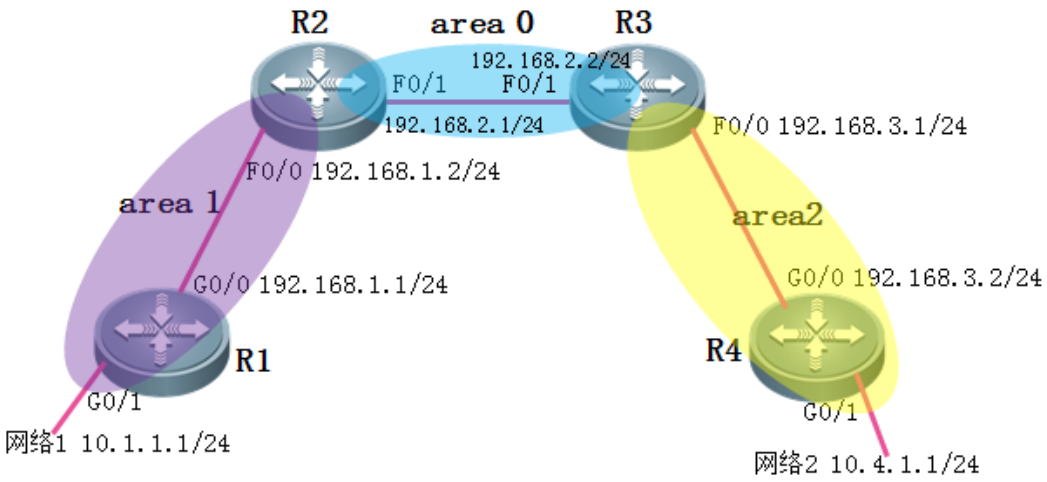
Scenarios

The network scale of an enterprise is large, with more than ten routers, and mutual communication and data sharing are required throughout the network. Therefore, OSPF needs to be enabled on all routers in the network.

I.Networking Requirements

The OSPF protocol needs to run on routers throughout the network so that routes across the network are reachable.

II. Networking Topology



III. Configuration Tips

1. Configure basic IP addresses for routers throughout the network.
2. Enable OSPF on routers throughout the network and advertise interfaces to a specified area.
3. (Optional) Adjust the OSPF network type for Ethernet interfaces.

IV. Configuration Steps

1. Configure basic IP addresses for routers throughout the network.

```
Ruijie(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
R1(config-GigabitEthernet 0/0)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
R1(config-GigabitEthernet 0/1)#exit
R1(config)#interface loopback 0        //Configure the address of Interface loopback 0 as router ID of
OSPF.
R1(config-Loopback 0)#ip address 1.1.1.1 255.255.255.255
R1(config-Loopback 0)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface fastEthernet 0/0
R2(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-if-FastEthernet 0/0)#exit
```

```
R2(config)#interface fastEthernet 0/1
R2(config-if-FastEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
R2(config-if-FastEthernet 0/1)#exit
R2(config)#interface loopback 0
R2(config-if-Loopback 0)#ip address 2.2.2.2 255.255.255.255
R2(config-if-Loopback 0)#exit
```

```
Ruijie(config)#hostname R3
R3(config)#interface fastEthernet 0/0
R3(config-if-FastEthernet 0/0)#ip address 192.168.3.1 255.255.255.0
R3(config-if-FastEthernet 0/0)#exit
R3(config)#interface fastEthernet 0/1
R3(config-if-FastEthernet 0/1)#ip address 192.168.2.2 255.255.255.0
R3(config-if-FastEthernet 0/1)#exit
R3(config)#interface loopback 0
R3(config-if-Loopback 0)#ip address 3.3.3.3 255.255.255.255
R3(config-if-Loopback 0)#exit
```

```
Ruijie(config)#hostname R4
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
R1(config-GigabitEthernet 0/0)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip address 10.4.1.1 255.255.255.0
R1(config-GigabitEthernet 0/1)#exit
R1(config)#interface loopback 0
R1(config-Loopback 0)#ip address 4.4.4.4 255.255.255.255
R1(config-Loopback 0)#exit
```

2. Enable OSPF on routers throughout the network and advertise interfaces to a specified area.

Notes:

1) An OSPF process ID only indicates an OSPF process on the local router. OSPF process IDs of routers throughout the network can be different.

2) When establishing a neighbor relationship, OSPF detects the area ID in the hello packet from the peer end. If the local router and peer router are in the same link, the OSPF area IDs at both ends must be the same.

3) The **network** command is described as follows: It is used to define an interface on which OSPF is to be enabled. Such an interface is matched using the form of IP network segment + wildcard mask (0 means that the equivalent bit must match and 1 means that the equivalent bit does not matter). It is recommended that the interface IP address be appended behind **network** and the wildcard mask be set to 0.0.0.0. Then, the interface with the IP address will be advertised to the OSPF process.

```
R1(config)#router ospf 1      //Enable OSPF and set the process ID to 1.
```

```
R1(config-router)#network 192.168.1.1 0.0.0.0 area 1     //Advertise the interface with the IP address of 192.168.1.1 to the OSPF area 1.
R1(config-router)#network 10.1.1.1 0.0.0.0 area 1
R1(config-router)#exit
```

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.1.2 0.0.0.0 area 1
R2(config-router)#network 192.168.2.1 0.0.0.0 area 0
R2(config-router)#exit
```

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.2.2 0.0.0.0 area 0
R3(config-router)#network 192.168.3.1 0.0.0.0 area 2
R3(config-router)#exit
```

```
R4(config)#router ospf 1
R4(config-router)#network 192.168.3.2 0.0.0.0 area 2
R4(config-router)#network 10.4.1.1 0.0.0.0 area 2
R4(config-router)#exit
```

3. (Optional) Adjust the OSPF network type for Ethernet interfaces.

Notes:

The default OSPF network type of Ethernet interfaces is broadcast. A Designated Router (DR)/Backup Designated Router (BDR) is elected within 40 seconds of waiting time. For point-to-point Ethernet interconnection interfaces, it is recommended that the OSPF network type of interfaces at both ends be set to point-to-point, to accelerate convergence of the OSPF neighbor relationship.

```
R2(config)#interface fastEthernet 0/1
R2(config-if-FastEthernet 0/1)#ip ospf network point-to-point        //Set the OSPF network type of the interface to point-to-point (The OSPF network type at both ends of a link must be the same).
R2(config-if-FastEthernet 0/1)#exit

R3(config)#interface fastEthernet 0/1
R3(config-if-FastEthernet 0/1)#ip ospf network point-to-point
R3(config-if-FastEthernet 0/1)#exit
```

V. Verification

1. Check whether an OSPF neighbor relationship is established between adjacent routers and the neighbor status. If adjacent routers successfully establish a neighbor relationship and the neighbor status is full, OSPF runs properly.

Notes:

When the OSPF network type is multi-access network, the neighbor relationship between DR others is 2-way and the neighbor status cannot be full.

```
R2#show ip ospf neighbor

OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID     Pri   State           BFD State  Dead Time   Address         Interface
1.1.1.1           1   Full/DR         -          00:00:33    192.168.1.1     FastEthernet 0/0
3.3.3.3           1   Full/BDR        -          00:00:29    192.168.2.2     FastEthernet 0/1
```

neighbor's router ID; neighbor state; IP address of neighbor's interface; neighbor's local interface

2. Check routes on routers throughout the network. If each router successfully learns routes throughout the network, OSPF is configured correctly.

```
R1#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    1.1.1.1/32 is local host.
C    10.1.1.0/24 is directly connected, GigabitEthernet 0/1
C    10.1.1.1/32 is local host.
O IA 10.4.1.0/24 [110/4] via 192.168.1.2, 00:00:35, GigabitEthernet 0/0
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.1.1/32 is local host.
O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 01:40:00, GigabitEthernet 0/0
O IA 192.168.3.0/24 [110/3] via 192.168.1.2, 01:39:05, GigabitEthernet 0/0
```

4.2.3.2 OSPF in VRF

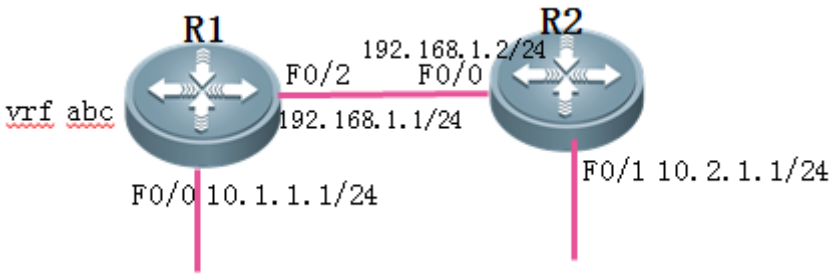
Features

The Open Shortest Path First (OSPF) protocol is a link status-based internal gateway routing protocol, developed by the OSPF Working Group of Internet Engineering Task Force (IETF). OSPF is exclusively designed for IP. It directly runs at the IP layer and the protocol ID is 89. OSPF packets are exchanged in multicast mode, with the multicast address of 224.0.0.5 (to all OSFP routers) or 224.0.0.6 (to designated routers). When an OSPF routing domain is large, a hierarchical structure is often adopted. That is, an OSPF routing domain is divided into several areas, which are interconnected through a backbone area. Each non-backbone area needs to be directly connected to the backbone area.

I.Networking Requirements

As shown in the following figure, Interfaces F0/0 and F0/2 of Router R1 belong to a VRF table named abc and Router R2 is a common global router. The OSPF protocol needs to be configured on routers throughout the network (the entire network is in Area 0) so that routes across the network are reachable.

II. Networking Topology



III. Configuration Tips

1. Configure a VRF table named abc on Router R1.
2. Configure basic IP addresses.
3. Add interfaces on Router R1 to the VRF table.
4. Enable OSPF on routers throughout the network and advertise interfaces to the OSPF process.

IV. Configuration Steps

1. Configure a VRF table named abc on Router R1.

Notes:

VRF is locally effective. When VRF is enabled at the local end, interfaces on the local router that belong to the same VRF table can interwork with each other. Interfaces that belong to different VRF tables are logically isolated, regardless of whether VRF is enabled on the remote router.

```
Ruijie(config)#hostname R1
R1(config)#ip vrf abc //Enable a VRF table named abc on the router.
R1(config-vrf)#exit
```

2. Configure basic IP addresses.

```
R1(config)#interface fastEthernet 0/2
R1(config-if-FastEthernet 0/2)#ip address 192.168.1.1 255.255.255.0
R1(config-if-FastEthernet 0/2)#exit
R1(config)#interface fastEthernet 0/0
R1(config-if-FastEthernet 0/0)#ip address 10.1.1.1 255.255.255.0
R1(config-if-FastEthernet 0/0)#exit
```

```
R1(config)#interface loopback 0        //Configure the address of Interface loopback 0 as router ID of
OSPF.
R1(config-Loopback 0)#ip address 1.1.1.1 255.255.255.255
R1(config-Loopback 0)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface fastEthernet 0/0
R2(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-if-FastEthernet 0/0)#exit
R2(config)#interface fastEthernet 0/1
R2(config-if-FastEthernet 0/1)#ip address 10.2.1.1 255.255.255.0
R2(config-if-FastEthernet 0/1)#exit
R2(config)#interface loopback 0
R2(config-if-Loopback 0)#ip address 2.2.2.2 255.255.255.255
R2(config-if-Loopback 0)#exit
```

3. Add interfaces on Router R1 to the VRF table.

Notes:

1) When an interface is added to a VRF table and an IP address is configured for the interface, the IP address will be deleted and you need to reconfigure an IP address for the interface.

2) When the address of the loopback interface is used as router ID of OSPF, the loopback interface does not need to be added to the VRF table.

```
R1(config)#interface fastEthernet 0/2
R1(config-if-FastEthernet 0/2)#ip vrf forwarding abc  //Add the interface to the VRF table.
% Interface FastEthernet 0/2 IP address 192.168.1.1 removed due to enabling VRF abc
R1(config-if-FastEthernet 0/2)#ip address 192.168.1.1 255.255.255.0       //Reconfigure an IP address for
Interface F0/2.
R1(config-if-FastEthernet 0/2)#exit
R1(config)#interface fastEthernet 0/0
R1(config-if-FastEthernet 0/0)#ip vrf forwarding abc
% Interface FastEthernet 0/0 IP address 10.1.1.1 removed due to enabling VRF abc
R1(config-if-FastEthernet 0/0)#ip address 10.1.1.1 255.255.255.0
R1(config-if-FastEthernet 0/0)#exit
```

4. Enable OSPF on routers throughout the network and advertise interfaces to the OSPF process.

Notes:

To configure VRF OSPF, associate the OSPF process with a relevant VRF table during enabling of the OSFP process. The precautions for configuring VRF OSPF are the same as those for configuring common OSPF. For details, see OSPF basic configuration.

```
R1(config)#router ospf 1 vrf abc//Enable OSPF process 1 in the VRF table named abc.
```

```
R1(config-router)#network 192.168.1.1 0.0.0.0 area 0   //Advertise the interface with the IP address of
192.168.1.1 to the OSPF area 1.
R1(config-router)#network 10.1.1.1 0.0.0.0 area 0
R1(config-router)#exit

R2(config)#router ospf 1
R2(config-router)#network 192.168.1.2 0.0.0.0 area 0
R2(config-router)#network 10.2.1.1 0.0.0.0 area 0
R2(config-router)#exit
```

V. Verification

1. Check whether an OSPF neighbor relationship is established between adjacent routers and the neighbor status. If adjacent routers successfully establish a neighbor relationship and the neighbor status is full, OSPF runs properly.

```
R1#show ip ospf neighbor

OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           BFD State  Dead Time   Address         Interface
2.2.2.2           1   Full/BDR              -        00:00:36    192.168.1.2     FastEthernet
0/2
```

Check the VRF routing table on Router R1 and global routing tables on other routers. If each router successfully learns routes throughout the network, VRF OSPF is configured correctly.

```
R1#show ip route vrf abc
Routing Table: abc

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.1.0/24 is directly connected, FastEthernet 0/0
C    10.1.1.1/32 is local host.
O    10.2.1.0/24 [110/2] via 192.168.1.2, 00:10:21, FastEthernet 0/2
C    192.168.1.0/24 is directly connected, FastEthernet 0/2
C    192.168.1.1/32 is local host.
```

4.2.3.3 Redistribution

Features

The route redistribution function imports routes learnt from other routing protocols to the Open Shortest Path First (OSPF) domain.

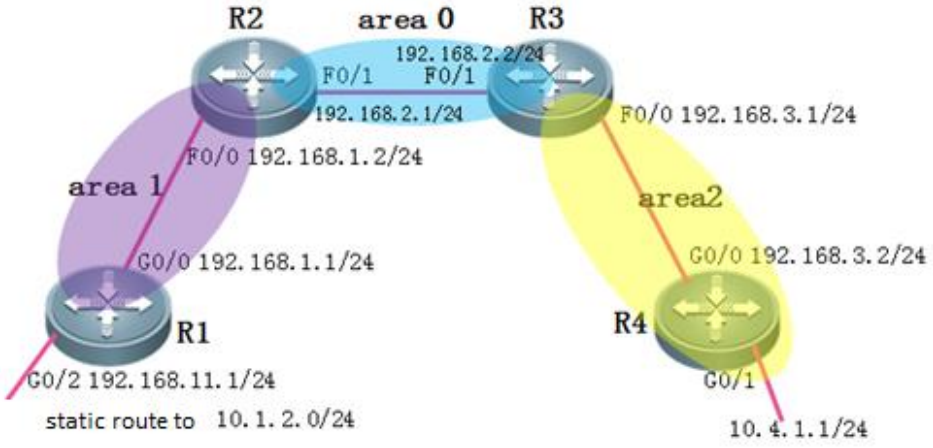
Scenarios

Multiple routing protocols are enabled on the network of an enterprise, and mutual communication and data sharing are required throughout the network. Therefore, routes learnt by other routing protocol need to be imported to the OSPF domain.

I.Networking Requirements

In addition to OSPF, other routing protocols run on the network, and routes learnt by other routing protocols need to be redistributed to OSPF.

II. Networking Topology



III. Configuration Tips

1. Configure IP addresses and basic OSPF information for routers throughout the network.
2. Configure a static route destined for the network 10.1.2.0/24 on Router R1.
3. Redistribute the static route to the OSPF domain.

IV. Configuration Steps

1. Configure IP addresses and basic OSPF information for routers throughout the network.

For the configuration, see OSPF basic configuration (choose **Typical Configuration** > **IP Routing** > **OSPF** > **Basic Configuration**).

2. Configure a static route destined for the network 10.1.2.0/24 on Router R1.

```
R1(config)#ip route 10.1.2.0 255.255.255.0 192.168.11.2
```

3. Redistribute the static route to the OSPF domain.

Notes:

1) The commands for OSPF to redistribute routes learnt from other routing protocols are as follows:

```
R1(config)#router ospf 1
R1(config-router)#redistribute ?
  bgp        Border Gateway Protocol (BGP)
  connected  Connected
  ospf       Open Shortest Path First (OSPF)
  rip        Routing Information Protocol (RIP)
  static     Static routes
```

2) There are two metric types for external routes imported by OSPF: type 1 and type 2.

a. Metric type 1: The internal cost is superposed when routes are transmitted within the OSPF domain. If an internal network needs to select a route for an imported external route, type 1 is recommended (the default metric type is 2 for imported external routes).

b. Metric type 2: The internal cost is not superposed when routes are transmitted within the OSPF domain.

```
R1(config)#router ospf 1
R1(config-router)#redistribute static metric-type ?
  1  Set OSPF External Type 1 metrics
  2    Set OSPF External Type 2 metrics
```

3) External routes imported by OSPF are effective routes on the local router and must be the routes that can be displayed after the **show ip route** command is executed on the local router.

4) When a route is redistributed to the OSPF domain, subnets must be appended. Otherwise, only main class network routes are redistributed.

The following example is based on import of a static route by OSPF. The import of other routes is the same as that of a static route.

```
R1(config)#router ospf 1
R1(config-router)#redistribute static subnets //Redistribute the static route.
R1(config-router)#exit
```

V. Verification

Check routes on other routers. If the routers successfully learn the route destined for the external network 10.1.2.0/24, redistribution is configured correctly.

```
R2#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    2.2.2.2/32 is local host.
O    10.1.1.0/24 [110/2] via 192.168.1.1, 02:16:22, FastEthernet 0/0
O E2 10.1.2.0/24 [110/20] via 192.168.1.1, 00:11:03, FastEthernet 0/0
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
O IA 192.168.3.0/24 [110/2] via 192.168.2.2, 01:19:29, FastEthernet 0/1
```

4.2.3.4 Summarization

Features

The route summarization of the Open Shortest Path First (OSPF) reduces the size of the routing table on routers. The OSPF route summarization can be configured only on Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs). ABRs summarize routes inside an OSPF domain while ASBRs summarize routes outside an OSPF domain. OSPF cannot summarize intra-area routes.

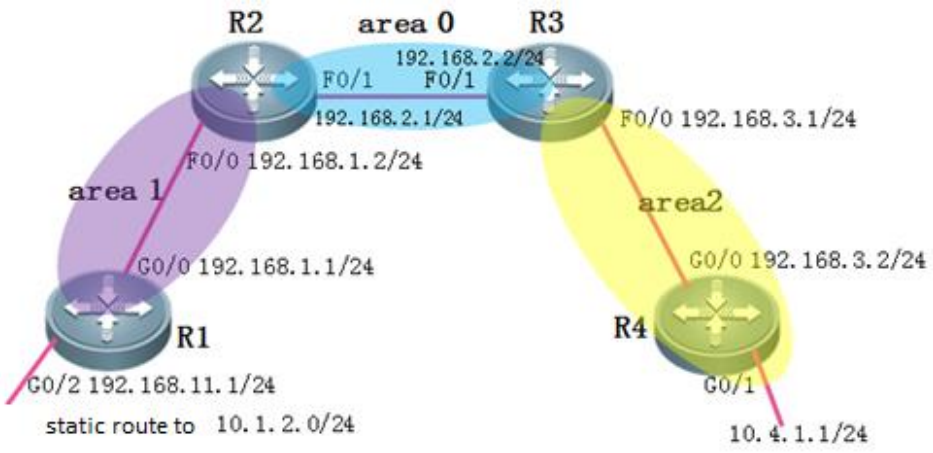
Scenarios

There are numerous IP network segments in the network of an enterprise. Route summarization can be configured on routers to reduce route entries on routers and improve router performance.

I.Networking Requirements

Specific routes learnt by OSPF need to be summarized to reduce route entries.

II. Networking Topology



III. Configuration Tips

1. Configure IP addresses and basic OSPF information for routers throughout the network.
2. Redistribute the external static route 10.1.2.0/24 to the OSPF domain.
3. Summarize the intra-domain route.
4. Summarize the inter-domain route.

IV. Configuration Steps

1. Configure IP addresses and basic OSPF information for routers throughout the network.

For the configuration, see OSPF basic configuration (choose **Typical Configuration**>**IP Routing**>**OSPF**>**Basic Configuration**).

2. Redistribute the external static route 10.1.2.0/24 to the OSPF domain.

For the configuration, see OSPF redistribution (choose **Typical Configuration**>**IP Routing**>**OSPF**>**Redistribution**).

3. Summarize the intra-domain route.

Summarize the route 10.4.1.0/24 on Router R4 as the route 10.4.0.0/16 on Router R3.

```
R3(config)#router ospf 1
R3(config-router)#area 2 range 10.4.0.0 255.255.0.0    //Summarize the intra-domain route (the area appended behind area must be the area from which the route comes).
R3(config-router)#exit
```

4. Summarize the inter-domain route.

Notes:

OSPF only summarizes external routes on ASBRs from which the external routes are distributed.

Summarize the static route 10.1.2.0/16 that is distributed to Router R1 as 10.1.0.0/16 on Router R1.

```
R1(config)#router ospf 1
R1(config-router)#summary-address 10.1.0.0 255.255.0.0      //Summarize the inter-domain route.
R1(config-router)#exit
```

V. Verification

Check routes on routers throughout the network. If intra-domain and inter-domain routes are all correctly summarized, route summarization of OSPF is configured correctly.

```
R2#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    2.2.2.2/32 is local host.
O E2 10.1.0.0/16 [110/20] via 192.168.1.1, 00:02:02, FastEthernet 0/0
O    10.1.1.0/24 [110/2] via 192.168.1.1, 02:42:53, FastEthernet 0/0
O IA 10.4.0.0/16 [110/3] via 192.168.2.2, 00:04:23, FastEthernet 0/1
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.1/32 is local host.
O IA 192.168.3.0/24 [110/2] via 192.168.2.2, 01:46:01, FastEthernet 0/1
```

4.2.3.5 Stub Area

Features

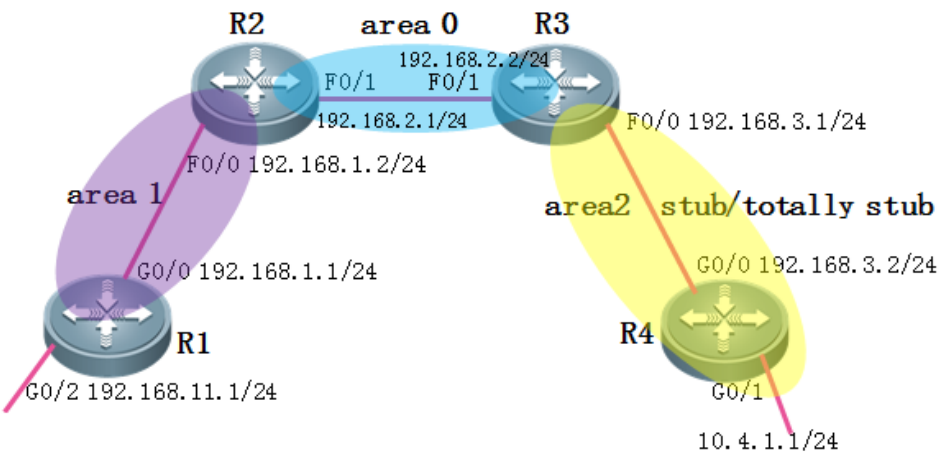
A stub area, located at the distal end of an OSPF domain, is capable of filtering out type4 and type5 Link State Advertisements (LSAs) to reduce the size of the link status database and routing table.

I.Networking Requirements

Requirement 1: Configure Area 2 as a stub area to filter out type 4 and type 5 LSAs.

Requirement 2: Configure Area 2 as a totally stub area to filter out type 3, type 4, and type 5 LSAs.

II. Networking Topology



III. Configuration Tips

1. A stub area is capable of filtering out type 4 and type 5 LSAs and one type 3 LSA default route is generated on the Area Border Router (ABR).
2. A totally stub area is capable of filtering out type 3, type 4, and type 5 LSAs and one type 3 LSA default route is generated on the ABR.
3. Routers in a stub area are not allowed to import routes outside an OSPF domain.

IV. Configuration Steps

Requirement 1: Configure Area 2 as a stub area to filter out type 4 and type 5 LSAs.

1. Configure IP addresses and basic OSPF information for routers throughout the network.

   For the configuration, see OSPF basic configuration (choose **Typical Configuration**>**IP Routing**>**OSPF**>**Basic Configuration**).

2. Configure a static route on Router R1 and distribute it to the OSPF domain.

   For the configuration, see OSPF redistribution (choose **Typical Configuration**>**IP Routing**>**OSPF**>**Redistribution**).

3. Configure Area 2 as a stub area.

Notes:

1) When an area is configured as a stub area, all routers in the area must be configured as the stub area.
2) The backbone area (Area 0) cannot be configured as a stub area.
3) Virtual links cannot traverse a stub area.

```
R3(config)#router ospf 1
R3(config-router)#area 2 stub      //Configure Area 2 as a stub area.
R3(config-router)#exit
```

```
R4(config)#router ospf 1
R4(config-router)#area 2 stub
R4(config-router)#exit
```

Requirement 2: Configure Area 2 as a totally stub area to filter out type 3, type 4, and type 5 LSAs.

1. Configure IP addresses and basic OSPF information for routers throughout the network.

   For the configuration, see OSPF basic configuration (choose **Typical Configuration**>**IP Routing**>**OSPF**>**Basic Configuration**).

2. Configure a static route on Router R1 and distribute it to the OSPF domain.

   For the configuration, see OSPF redistribution (choose **Typical Configuration**>**IP Routing**>**OSPF**>**Redistribution**).

3. Configure Area 2 as a totally stub area.

Notes:

When an area is configured as a totally stub area, all routers in the area must be configured as the stub area and the **no-summary** parameter must be set on the ABR.

```
R3(config)#router ospf 1
R3(config-router)#area 2 stub no-summary    //Configure Area 2 as a totally stub area.
R3(config-router)#exit
```

```
R4(config)#router ospf 1
R4(config-router)#area 2 stub
R4(config-router)#exit
```

V. Verification

1. Verification of the stub area

Check routes on routers in the stub area. If inter-domain routes are filtered out but inter-area routes persist, and an OIA default route is generated, the stub area is configured correctly.

```
R4#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 192.168.3.1 to network 0.0.0.0
O*IA 0.0.0.0/0 [110/2] via 192.168.3.1, 00:06:06, GigabitEthernet 0/0
C    4.4.4.4/32 is local host.
O IA 10.1.1.0/24 [110/4] via 192.168.3.1, 00:05:55, GigabitEthernet 0/0
C    10.4.1.0/24 is directly connected, GigabitEthernet 0/1
C    10.4.1.1/32 is local host.
O IA 192.168.1.0/24 [110/3] via 192.168.3.1, 00:05:55, GigabitEthernet 0/0
O IA 192.168.2.0/24 [110/2] via 192.168.3.1, 00:06:06, GigabitEthernet 0/0
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.3.2/32 is local host.
```

2. Verification of the totally stub area

Check routes on routers in the totally stub area. If both inter-domain routes and inter-area routes are filtered out and an OIA default route is generated, the totally stub area is configured correctly.

```
R4#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 192.168.3.1 to network 0.0.0.0
O*IA 0.0.0.0/0 [110/2] via 192.168.3.1, 00:15:23, GigabitEthernet 0/0
C    4.4.4.4/32 is local host.
C    10.4.1.0/24 is directly connected, GigabitEthernet 0/1
C    10.4.1.1/32 is local host.
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.3.2/32 is local host.
```

4.2.3.6 NSSA Area

Features

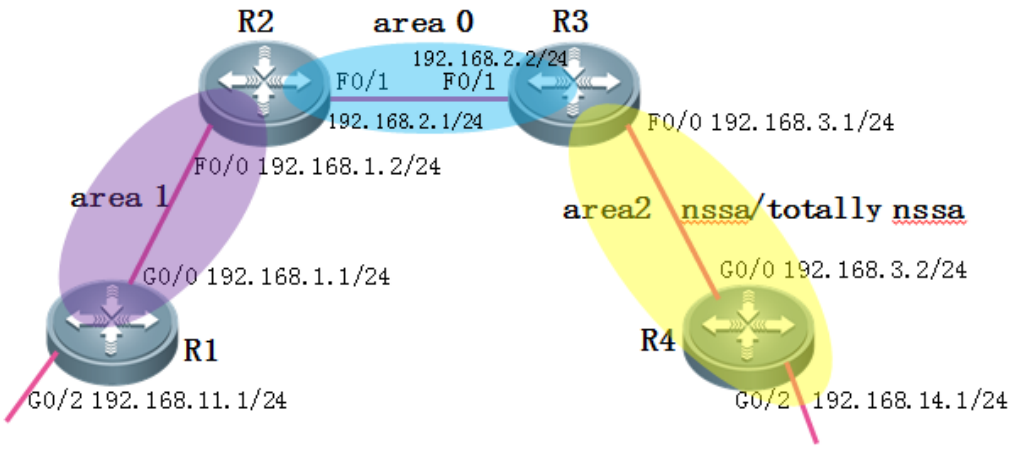
A Not-So-Stubby Area (NSSA), located at the distal end of an OSPF domain, is capable of filtering out type 4 and type 5 Link State Advertisements (LSAs) to reduce the size of the link status database and routing table.

I.Networking Requirements

Requirement 1: Configure Area 2 as an NSSA to filter out type 4 and type 5 LSAs, and import external static routes.

Requirement 2: Configure Area 2 as a totally NSSA to filter out type 3, type 4, and type 5 LSAs, and import external static routes.

II. Networking Topology



III. Configuration Tips

1. An NSSA is capable of filtering out type 4 and type 5 LSAs and no type 3 LSA default route is generated on the Area Border Router (ABR).
2. A totally NSSA is capable of filtering out type 3, type 4, and type 5 LSAs and one type 3 LSA default route will be generated on the ABR.
3. Routers in an NSSA are allowed to import routes outside an OSPF domain.

IV. Configuration Steps

Requirement 1: Configure Area 2 as an NSSA to filter out type 4 and type 5 LSAs, and import external static routes.

1. Configure IP addresses and basic OSPF information for routers throughout the network.

   For the configuration, see OSPF basic configuration (choose **Typical Configuration** > **IP Routing** > **OSPF** > **Basic Configuration**).

2. Configure a static route on Router R1 and Router R4 each, and distribute them to the OSPF domain.

   For the configuration, see OSPF redistribution (choose **Typical Configuration** > **IP Routing** > **OSPF** > **Redistribution**).

3. Configure Area 2 as an NSSA.

Notes:

1) When an area is configured as an NSSA, all routers in the area must be configured as the NSSA.

2) The backbone area (Area 0) cannot be configured as an NSSA.

```
R3(config)#router ospf 1
R3(config-router)#area 2 nssa      //Configure Area 2 as an NSSA.
R3(config-router)#exit
```

```
R4(config)#router ospf 1
R4(config-router)#area 2 nssa
R4(config-router)#exit
```

Requirement 2: Configure Area 2 as a totally NSSA to filter out type 3, type 4, and type 5 LSAs, and import external static routes.

1. Configure IP addresses and basic OSPF information for routers throughout the network.

   For the configuration, see OSPF basic configuration (choose **Typical Configuration** > **IP Routing** > **OSPF** > **Basic Configuration**).

2. Configure a static route on Router R1 and Router R2 each, and distribute them to the OSPF domain.

   For the configuration, see OSPF redistribution (choose **Typical Configuration** > **IP Routing** > **OSPF** > **Redistribution**).

3. Configure Area 2 as a totally NSSA.

Notes:

When an area is configured as a totally NSSA, all routers in the area must be configured as the totally NSSA and the **no-summary** parameter must be set on the ABR.

```
R3(config)#router ospf 1
R3(config-router)#area 2 nssa no-summary   //Configure Area 2 as a totally NSSA.
R3(config-router)#exit
```

```
R4(config)#router ospf 1s
R4(config-router)#area 2 nssa
R4(config-router)#exit
```

V. Verification

1. Verification of the NSSA

Check routes on routers in the NSSA. If inter-domain routes are filtered out but inter-area routes persist, and routes outside the OSPF domain can be successfully imported (other routers in the NSSA learns the OSPF NSSA routes), the NSSA is configured correctly.

```
R4#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    4.4.4.4/32 is local host.
O IA 10.1.1.0/24 [110/4] via 192.168.3.1, 00:12:03, GigabitEthernet 0/0
C    10.4.1.0/24 is directly connected, GigabitEthernet 0/1
C    10.4.1.1/32 is local host.
S    10.4.2.0/24 [1/0] via 192.168.14.2
O IA 192.168.1.0/24 [110/3] via 192.168.3.1, 00:12:03, GigabitEthernet 0/0
O IA 192.168.2.0/24 [110/2] via 192.168.3.1, 00:12:03, GigabitEthernet 0/0
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.3.2/32 is local host.
C    192.168.14.0/24 is directly connected, GigabitEthernet 0/2
C    192.168.14.1/32 is local host.

R3#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    3.3.3.3/32 is local host.
O IA 10.1.1.0/24 [110/3] via 192.168.2.1, 00:44:30, FastEthernet 0/1
O E2 10.1.2.0/24 [110/20] via 192.168.2.1, 00:44:30, FastEthernet 0/1
O    10.4.1.0/24 [110/2] via 192.168.3.2, 00:13:26, FastEthernet 0/0
O N2 10.4.2.0/24 [110/20] via 192.168.3.2, 00:02:48, FastEthernet 0/0
O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:44:30, FastEthernet 0/1
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.2/32 is local host.
C    192.168.3.0/24 is directly connected, FastEthernet 0/0
C    192.168.3.1/32 is local host.
```

2. Verification of the totally NSSA

Check routes on routers in the totally NSSA. The totally NSSA is configured correctly if inter-domain routes and inter-area routes are filtered out, routes outside the OSPF domain can be successfully imported (other routers in the NSSA learns the OSPF NSSA routes), and one OIA default route is generated.

```
R4#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 192.168.3.1 to network 0.0.0.0
O*IA 0.0.0.0/0 [110/2] via 192.168.3.1, 00:01:49, GigabitEthernet 0/0
C    4.4.4.4/32 is local host.
C    10.4.1.0/24 is directly connected, GigabitEthernet 0/1
C    10.4.1.1/32 is local host.
S    10.4.2.0/24 [1/0] via 192.168.14.2
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.3.2/32 is local host.
C    192.168.14.0/24 is directly connected, GigabitEthernet 0/2
C    192.168.14.1/32 is local host.

R3#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    3.3.3.3/32 is local host.
O IA 10.1.1.0/24 [110/3] via 192.168.2.1, 00:50:49, FastEthernet 0/1
O E2 10.1.2.0/24 [110/20] via 192.168.2.1, 00:50:49, FastEthernet 0/1
O    10.4.1.0/24 [110/2] via 192.168.3.2, 00:19:45, FastEthernet 0/0
O N2 10.4.2.0/24 [110/20] via 192.168.3.2, 00:09:06, FastEthernet 0/0
O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:50:49, FastEthernet 0/1
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.2/32 is local host.
C    192.168.3.0/24 is directly connected, FastEthernet 0/0
C    192.168.3.1/32 is local host.
```

4.2.4 BGP

4.2.4.1 Basic Configuration of IBGP

Features

The Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) used for communication between routers in different Autonomous Systems (ASs). BGP is used to exchange network accessibility information between different ASs and eliminate routing loops by using its own mechanism. BGP uses TCP as the transmission protocol. The reliable transmission

mechanism of TCP ensures transmission reliability of BGP. Routers running BGP are called BGP speakers. BGP speakers between which a BGP session is established are called BPG peers.

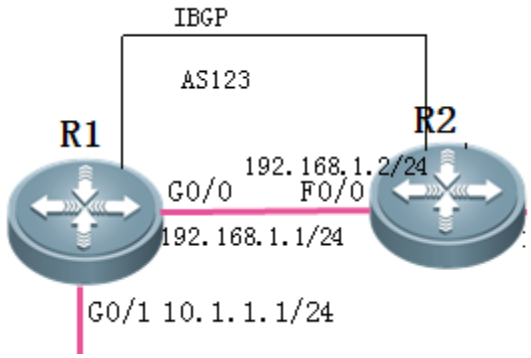
Two modes can be used to establish BGP peers between BGP speakers: Internal BGP (IBGP) and External BGP (EBGP). IBGP refers to a BGP connection established within an AS while EBGP refers to a BGP connection established between different ASs. In a word, EBGP completes exchange of routing information between different ASs while IBGP completes transfer of routing information within an AS.

I.Networking Requirements

1) Router R1 and Router R2 both belong to AS123 and an IBGP neighbor relationship needs to be established between Router R1 and Router R2.

2) Routes are advertised to neighbors over IBGP.

II. Networking Topology



III. Configuration Tips

1. Configure basic IP addresses for routers throughout the network.
2. Configure a static route on Router R1 and Router R2 to ensure Interfaces Loopback 0 of Router R1 and Router R2 are reachable.
3. Configure an IBGP neighbor relationship.
4. Advertise routes to BGP.

IV. Configuration Steps

1. Configure basic IP addresses for routers throughout the network.

```
Ruijie(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
```

```
R1(config-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
R1(config-GigabitEthernet 0/0)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
R1(config-GigabitEthernet 0/1)#exit
R1(config)#interface loopback 0        //Configure the address of Interface Loopback 0 as the update source address of BGP.
R1(config-Loopback 0)#ip address 1.1.1.1 255.255.255.255
R1(config-Loopback 0)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface fastEthernet 0/0
R2(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-if-FastEthernet 0/0)#exit
R2(config)#interface fastEthernet 0/1
R2(config-if-FastEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
R2(config-if-FastEthernet 0/1)#exit
R2(config)#interface loopback 0
R2(config-if-Loopback 0)#ip address 2.2.2.2 255.255.255.255
R2(config-if-Loopback 0)#exit
```

3. Configure a static route on Router R1 and Router R2 to ensure Interfaces Loopback 0 of Router R1 and Router R2 are reachable.

```
R1(config)#ip route 2.2.2.2 255.255.255.255 192.168.1.2
R2(config)#ip route 1.1.1.1 255.255.255.255 192.168.1.1
```

4. Configure an IBGP neighbor relationship.

Notes:

1) If the AS ID of a BGP neighbor of a router is consistent with the AS ID of the router, an IBGP neighbor relationship is established; if their AS IDs are different, an EBGP neighbor relationship is established.

2) Selection of the update source address for a BGP neighbor relationship

   a. An EBGP neighbor relationship is established at the border of an AS. It is recommended that the address of a directly connected interface be used as the update source address of the EBGP neighbor. In this way, IGP is not necessary because the directly connected interface is reachable.

   b. An IBGP neighbor relationship is established within an AS. It is recommended that the loopback address be used as the update source address of the IBGP neighbor because the loopback address is reliable (the BGP neighbor flapping will not be incurred due to breakdown of a physical line) and IGP is often used inside the AS to make the route to the update source address reachable.

3) IBGP supports split horizon. That is, routes learnt from an IBGP neighbor will not be transferred to other IBGP neighbors but will be transferred to EBGP neighbors.

```
R1(config)#router bgp 123//Enable the BGP process, with the AS ID of 123.
R1(config-router)#neighbor 2.2.2.2 remote-as 123     //Specify the address of a BGP neighbor and the AS ID of the neighbor.
R1(config-router)#neighbor 2.2.2.2 update-source loopback 0       //Configure the update source address of BGP.
R1(config-router)#exit
```

```
R2(config)#router bgp 123
R2(config-router)#neighbor 1.1.1.1 remote-as 123
R2(config-router)#neighbor 1.1.1.1 update-source loopback 0
R2(config-router)#exit
```

5. Advertise routes to BGP.

Notes:

In BGP, the **network** command is used to specify the routes to be advertised to the BGP process rather than specify the interfaces to be enabled with BGP, which is different from the **network** command in RIP and OSPF. Routes advertised to the BGP process using the **network** command must be the routes that are displayed after the **show ip route** command is executed and whose mask is consistent with the value of the **mask** parameter.

```
R1(config)#router bgp 123
R1(config-router)#network 10.1.1.0 mask 255.255.255.0
R1(config-router)#exit
```

V. Verification

1. Check whether a BGP neighbor relationship is established between routers and the neighbor status. If a BGP neighbor relationship is established normally and **State** is **Established**, IBGP runs normally.

```
R2#sh ip bgp summary
BGP router identifier 2.2.2.2, local AS number 123
BGP table version is 2
1 BGP AS-PATH entries
0 BGP Community entries
1 BGP Prefix entries (Maximum-prefix:4294967295)
                neighbor's update source address
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.1.1.1         4          123       6       5        1    0    0 00:03:08        1
                                                                        nubmer of routes
Total number of neighbors 1
```

2. Check routes on IBGP neighbor routers. If routes advertised by the peer end are learnt, IBGP is configured correctly.

```
R2#sh ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
S    1.1.1.1/32 [1/0] via 192.168.1.1
C    2.2.2.0/24 is directly connected, Loopback 0
C    2.2.2.2/32 is local host.
B    10.1.1.0/24 [200/0] via 1.1.1.1, 00:03:53    AD of IBGP neighbor is 200
C    192.168.1.0/24 is directly connected, VLAN 1
C    192.168.1.2/32 is local host.
R2#
```

```
R2#sh ip bgp
BGP table version is 2, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric      LocPrf      Weight Path
*>i10.1.1.0/24      1.1.1.1                  0         100           0     i
     optimal route
Total number of prefixes 1
```

4.2.4.2 Basic Configuration of EBGP

Features

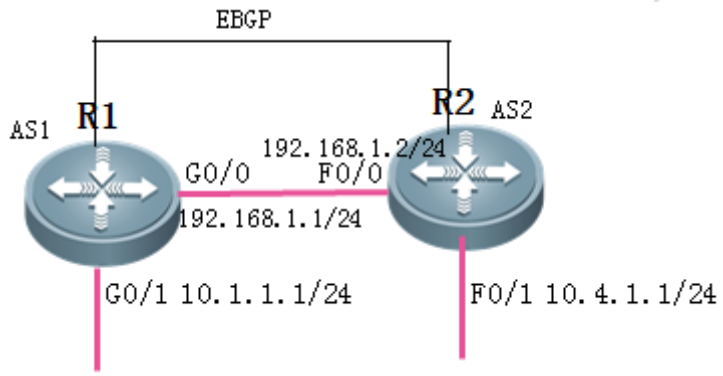
The Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) used for communication between routers in different Autonomous Systems (ASs). BGP is used to exchange network accessibility information between different ASs and eliminate routing loops by using its own mechanism. BGP uses TCP as the transmission protocol. The reliable transmission mechanism of TCP ensures transmission reliability of BGP. Routers running BGP are called BGP speakers. BGP speakers between which a BGP session is established are called BPG peers.

Two modes can be used to establish BGP peers between BGP speakers: Internal BGP (IBGP) and External BGP (EBGP). IBGP refers to a BGP connection established within an AS while EBGP refers to a BGP connection established between different ASs. In a word, EBGP completes exchange of routing information between different ASs while IBGP completes transfer of routing information within an AS.

I.Networking Requirements

1) Router R1 belongs to AS1, Router R2 belongs to AS2, and an EBGP neighbor relationship needs to be established between Router R1 and Router R2.
2) Routes are advertised to neighbors over EBGP.

II. Networking Topology



III. Configuration Tips

1. Configure basic IP addresses for routers throughout the network.
2. Configure an EBGP neighbor relationship.
3. Advertise routes to the BGP process.

IV. Configuration Steps

1. Configure basic IP addresses for routers throughout the network.

```
Ruijie(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
R1(config-GigabitEthernet 0/0)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
R1(config-GigabitEthernet 0/1)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface fastEthernet 0/0
R2(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-if-FastEthernet 0/0)#exit
R2(config)#interface fastEthernet 0/1
R2(config-if-FastEthernet 0/1)#ip address 10.4.1.1 255.255.255.0
R2(config-if-FastEthernet 0/1)#exit
```

2. Configure an EBGP neighbor relationship.

   Notes:

   1) If the AS ID of a BGP neighbor of a router is consistent with the AS ID of the router, an IBGP neighbor relationship is established; if their AS IDs are different, an EBGP neighbor relationship is established.

```
R1(config)#router bgp 1
R1(config-router)#neighbor 192.168.1.2 remote-as 2
R1(config-router)#exit

R2(config)#router bgp 2
R2(config-router)#neighbor 192.168.1.1 remote-as 1
R2(config-router)#exit
```

3. Advertise routes to the BGP process.

```
R1(config)#router bgp 1
R1(config-router)#network 10.1.1.0 mask 255.255.255.0
R1(config-router)#exit

R2(config)#router bgp 2
R2(config-router)#network 10.4.1.0 mask 255.255.255.0
R2(config-router)#exit
```

Notes:

In BGP, the **network** command is used to specify the routes to be advertised to the BGP process rather than specify the interfaces to be enabled with BGP, which is different from the **network** command in RIP and OSPF. Routes advertised to the BGP process using the **network** command must be the routes that are displayed after the **show ip route** command is executed and whose mask is consistent with the value of the **mask** parameter.

V. Verification

1. Check whether a BGP neighbor relationship is established between routers and the neighbor status. If a BGP neighbor relationship is established normally and State is Established, EBGP runs normally.

```
R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 2
BGP table version is 3
2 BGP AS-PATH entries
0 BGP Community entries
2 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.1     4     1      12      12        3    0    0 00:08:46        1
update source address   AS number                      time since BGP secton   number of prefixes that
Total number of neighbors 1                            was established         have been received
```

2. Check routes on EBGP neighbor routers. If routes advertised by the peer end are learnt, EBGP is configured correctly.

```
R2#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    2.2.2.2/32 is local host.
B    10.1.1.0/24 [20/0] via 192.168.1.1, 00:09:34
C    10.4.1.0/24 is directly connected, FastEthernet 0/1
C    10.4.1.1/32 is local host.
C    192.168.1.0/24 is directly connected, FastEthernet 0/0
C    192.168.1.2/32 is local host.
```

4.2.4.3 Route Reflector

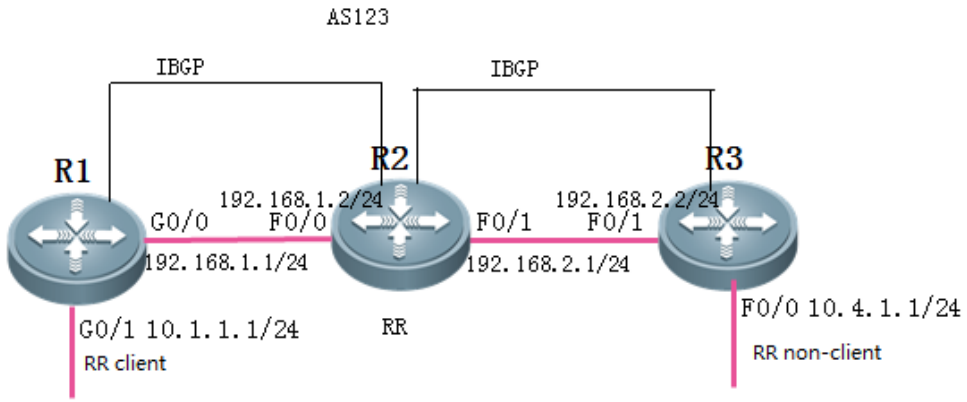
Features

Route reflector solves the split horizon problem of the Internal Border Gateway Protocol (IBGP).

I.Networking Requirements

As shown in the following networking topology, Router R1 and Router R3 fail to learn BGP routes of the peer end due to split horizon of IBGP neighbors. Therefore, the route reflector needs to be configured to solve split horizon problem of IBGP neighbors.

II. Networking Topology



III. Configuration Tips

1. Configure IP addresses and basic IBGP information for routers throughout the network.
2. Configure a route reflector.

III. Configuration Steps

1. Configure IP addresses and basic IBGP information for routers throughout the network.

   For the configuration, see "IBGP Basic Configuration" (choose **Typical Configuration**>**IP Routing**>**BGP**>**IBGP Basic Configuration**).

2. Configure a route reflector.

```
Configure Router R2 as a route reflector and specify Router R1 as a client.
R2(config)#router bgp 123
R2(config-router)#neighbor 1.1.1.1 route-reflector-client          //Specify R1 to be the client of the route reflector on Router R2.
R2(config-router)#exit
```

Notes:

1) When a router is configured as the client of a route reflector, the BGP neighbor relationship with the client will be broken.

2) A route reflector must have learnt IBGP routes so that it can reflect routes.

3) A route reflector can mutually reflect routes between a non-client and a client and between clients but cannot reflect routes learnt from a non-client to other non-clients.

V. Verification

Check routes throughout the network. If Router R1 and Router 3 successfully learn routes from the peer end, the route reflector is configured correctly.

```
R1#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    1.1.1.1/32 is local host.
O    2.2.2.2/32 [110/1] via 192.168.1.2, 16:47:35, GigabitEthernet 0/0
O    3.3.3.3/32 [110/2] via 192.168.1.2, 00:07:13, GigabitEthernet 0/0
C    10.1.1.0/24 is directly connected, GigabitEthernet 0/1
C    10.1.1.1/32 is local host.
B    10.4.1.0/24 [200/0] via 3.3.3.3, 00:04:28
C    192.168.1.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.1.1/32 is local host.
O    192.168.2.0/24 [110/2] via 192.168.1.2, 00:07:23, GigabitEthernet 0/0
```

4.2.5 Route Control

ACL and prefix-list

Similarities:

Both can be used to match the route prefix.

Differences:

ACL can be used to filter IP packets by five elements while prefix-list can be used only to match the route prefix.

Selection:

Either ACL or prefix-list is acceptable when the route prefix needs to be matched. When the route prefix with different mask lengths in a large network segment needs to be matched, prefix-list is preferred.

distribute-list and route-map

Similarities:

Both can be used to filter routes.

Differences:

1) Distribute-list can be used only to filter route entries and does not support route attribute modification. route-map can be used to filter route entries and supports route attribute modification.

2) Route-map can be used to forcibly change the next hop of data packets to implement policy-based routing (PBR).

3) Distribute-list can be applied in routing protocol redistribution, route transfer between distance vector routing protocol neighbors (it can be used to filter routes because routes are transferred between distance vector routing protocol neighbors), and route submission to the routing table by the link state routing protocol (LSAs rather than routes are transferred between link state routing protocol neighbors and therefore it cannot be used to filter LSAs transferred between neighbors).

4) Route-map is applied in routing protocol redistribution and route transfer between BGP neighbors.

Selection:

The selection of distribute-list or route-map depends on the application scenario. If both can be used but the route attribute needs to be modified, route-map is preferred. If the route attribute does not need to be modified, either is acceptable.

4.2.5.1 Distribute-list

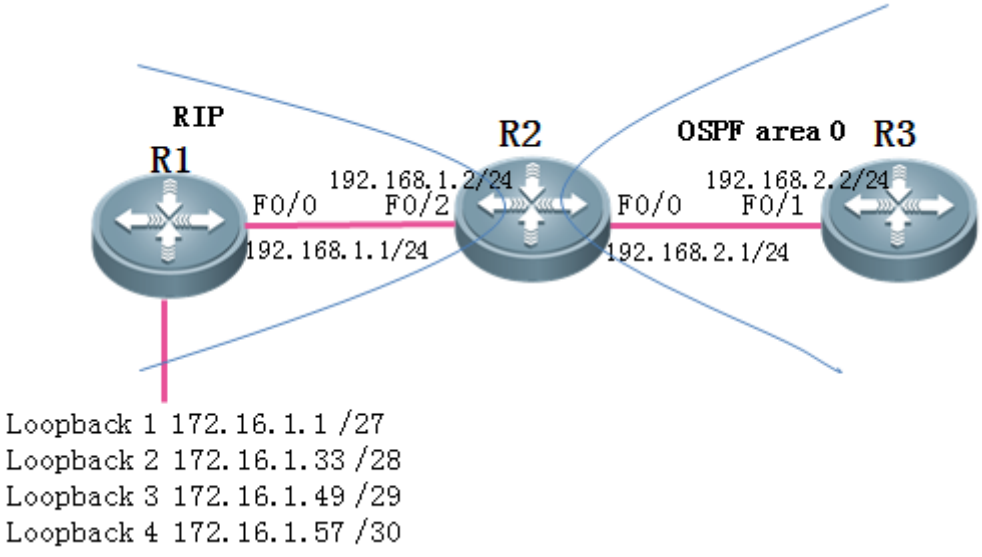
Features

Distribute-list controls route updates and filters route entries. It does not support route attribute modification.

I.Networking Requirements

Redistribute RIP routes to the OSPF domain on Router R2. Route filtering is required during redistribution, and only the routes 172.16.1.32/28, 172.16.1.48/29, and 172.16.1.56/30 are allowed to be redistributed to the OSPF domain.

II. Networking Topology



III. Configuration Tips

1. Configure basic IP addresses.
2. Enable RIP on Router R1 and Router R2 and advertise interfaces to the RIP process.
3. Enable OSPF on Router R2 and Router R3 and advertise interfaces to the OSPF process.
4. Redistribute routes learnt by RIP to the OSPF process on Router R2.
5. Use an ACL or prefix-list to match the routes to be learnt.
6. Redistribute RIP routes to the OSPF process on Router R2 and use distribute-list to filter routes.

IV. Configuration Steps

1. Configure basic IP addresses.

```
Ruijie(config)#hostname R1
R1(config)#interface fastEthernet 0/0
R1(config-if-FastEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
R1(config-if-FastEthernet 0/0)#exit
R1(config)#interface loopback 1
R1(config-if-Loopback 1)#ip address 172.16.1.1 255.255.255.224
R1(config-if-Loopback 1)#exit
R1(config)#interface loopback 2
R1(config-if-Loopback 2)#ip address 172.16.1.33 255.255.255.240
R1(config-if-Loopback 2)#exit
R1(config)#interface loopback 3
R1(config-if-Loopback 3)#ip address 172.16.1.49 255.255.255.248
R1(config-if-Loopback 3)#exit
R1(config)#interface loopback 4
R1(config-if-Loopback 4)#ip address 172.16.1.57 255.255.255.252
R1(config-if-Loopback 4)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface fastEthernet 0/2
R2(config-if-FastEthernet 0/2)#ip address 192.168.1.2 255.255.255.0
R2(config-if-FastEthernet 0/2)#exit
R2(config)#interface fastEthernet 0/0
R2(config-if-FastEthernet 0/0)#ip address 192.168.2.1 255.255.255.0
R2(config-if-FastEthernet 0/0)#exit
```

```
Ruijie(config)#hostname R3
R3(config)#interface fastEthernet 0/1
R3(config-if-FastEthernet 0/1)#ip address 192.168.2.2 255.255.255.0
```

```
R3(config-if-FastEthernet 0/1)#exit
```

2. Enable RIP on Router R1 and Router R2 and advertise interfaces to the RIP process.

```
R1(config)#router rip
R1(config-router)#version 2     //Enable RIPv2.
R1(config-router)#no auto-summary     //Disable automatic summarization.
R1(config-router)#network 172.16.0.0     //Advertise the classful network 172.16.0.0 to the RIP process.
R1(config-router)#network 192.168.1.0
R1(config-router)#exit
```

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.1.0
R2(config-router)#exit
```

3. Enable OSPF on Router R2 and Router R3 and advertise interfaces to the OSPF process.

```
R2(config)#router ospf 1    //Enable OSPF Process 1.
R2(config-router)#network 192.168.2.1 0.0.0.0 area 0    //Advertise the interface with the IP address of 192.168.2.1 to Area 0 of OSPF Process 1.
R2(config-router)#exit
```

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.2.2 0.0.0.0 area 0
R3(config-router)#exit
```

4. Redistribute routes learnt by RIP to the OSPF process on Router R2.

```
R2(config)#router ospf 1
R2(config-router)#redistribute rip subnets    //Redistribute RIP routes to the OSPF process. Subnets must be appended.
R2(config-router)#exit
```

5. Use an ACL or prefix-list to match the routes to be learnt.

Notes:

1) Both ACL and prefix-list can be used to match route entries. Select either of them.

2) When the route prefix with different mask lengths in a large network segment needs to be matched, prefix-list is preferred. You can also use an ACL but you need to enter multiple entries.

In the following example, the route entries 172.16.1.32/27, 172.16.1.48/28, and 172.16.1.56/29 need to be matched, three ACE entries are required in the ACL but only one entry is required in the prefix-list.

1) Use an ACL to match route entries.

Notes:

The ACL is used to match route entries here and the mask is set to 0.0.0.0 to precisely match route entries.

```
R2(config)#ip access-list standard 1
R2(config-std-nacl)#10 permit 172.16.1.32 0.0.0.0
R2(config-std-nacl)#20 permit 172.16.1.48 0.0.0.0
R2(config-std-nacl)#30 permit 172.16.1.56 0.0.0.0
R2(config-std-nacl)#exit
```

2) Use a prefix-list to match route entries.

Notes:

1) The prefix-list can be used only to match route entries. It cannot be used to filter data packets.

2) The prefix-list matches subnets in a network segment, where **ge** indicates the mask length that a mask length must be greater than or equal to while **le** indicates the mask length that a mask length must be smaller than.

3) The prefix-list is also matched from top to bottom and the last entry **deny any** is at the bottom.

```
R2(config)#ip prefix-list ruijie seq 10 permit 172.16.1.0/24 ge 28 le 30   //Define a prefix-list named ruijie to match the route prefix 172.16.1.0/24 with the subnet mask length greater than or equal to 28 and smaller than or equal to 30.
```

6. Redistribute RIP routes to the OSPF process on Router R2 and use distribute-list to filter routes.

Notes:

1) Route entries filtered by distribute-list are matched by the ACL and prefix-list. The route entries to be filtered are determined by ACL and prefix-list.

2) distribute-list can be applied in routing protocol redistribution, route transfer between distance vector routing protocol neighbors (it can be used to filter routes because routes are transferred between distance vector routing protocol neighbors), and route submission to the routing table by the link state routing protocol (LSAs rather than routes are transferred between link state routing protocol neighbors and therefore it cannot be used to filter LSAs transferred between neighbors).

The following examples use the distribute-list to call an ACL and prefix-list to filter routes.

1) Use the distribute-list to apply an ACL to filter routes.

```
R2(config)#router ospf 1
R2(config-router)#distribute-list lout rip     //Filter routes when RIP routes are redistributed to the OSPF process (note that the direction must be out).
R2(config-router)#exit
```

2) Use the distribute-list to call a prefix-list to filter routes.

```
R2(config)#router ospf 1
R2(config-router)#distribute-list prefix ruijie out rip    //Filter routes when RIP routes are redistributed to the OSPF process (note that the direction must be out).
R2(config-router)#exit
```

Supplement:

1) The distance vector protocol uses the distribute-list to filter route entries transmitted between neighbors. The commands are as follows:

```
R2(config)#router rip
R2(config-router)#distribute-list 1infastEthernet 0/2 //1 indicates ACL 1 and the prefix-list can be also used. In indicates routes learnt from neighbors and out indicates routes transferred to neighbors. Specific interfaces can be also appended.
```

2) The link state protocol uses the distribute-list to filter route entries to be submitted to the routing table.

```
R2(config)#router ospf 1
R2(config-router)#distribute-list 1 in //1 indicates ACL 1 and a prefix-list can be also used. The direction must be in.
```

V. Verification

Check route entries on Router R3. If Router R3 successfully learns the route entries 172.16.1.32/28, 172.16.1.48/29, and 172.16.1.56/30, the distribute-list used for route filtering is configured correctly.

```
R3#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
O E2 172.16.1.32/28 [110/20] via 192.168.2.1, 00:02:45, FastEthernet 0/1
O E2 172.16.1.48/29 [110/20] via 192.168.2.1, 00:02:29, FastEthernet 0/1
O E2 172.16.1.56/30 [110/20] via 192.168.2.1, 00:02:21, FastEthernet 0/1
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.2/32 is local host.
```

4.2.5.2 Route-map

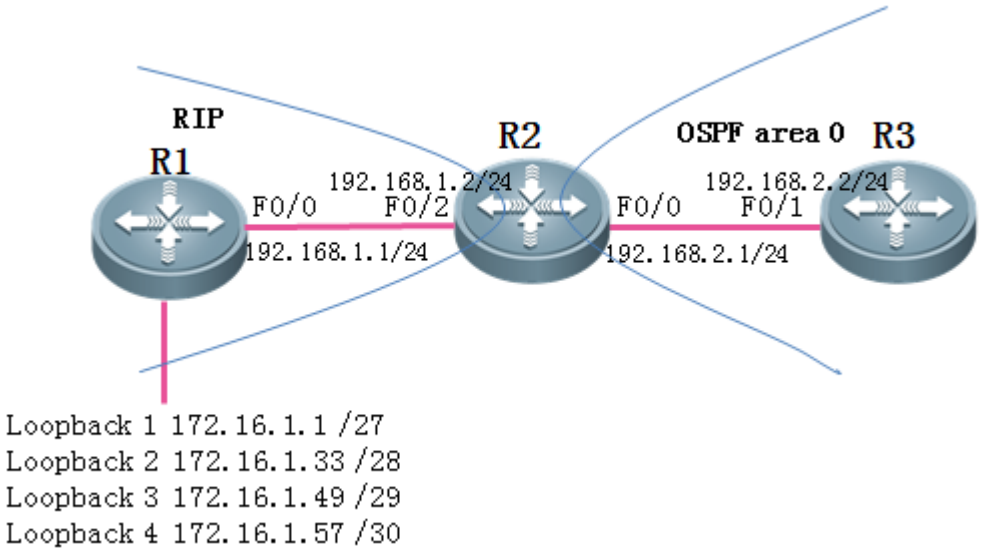
Features

Route-map controls route updates and supports route attribute modification.

I.Networking Requirements

Redistribute RIP routes to the OSPF domain on Router R2. Route filtering is required during redistribution, and only the routes 172.16.1.32/28, 172.16.1.48/29, and 172.16.1.56/30 are allowed to be redistributed to the OSPF domain. The type of the imported external route is OE1 and the metric value is 50.

II. Networking Topology



III. Configuration Tips

1. Configure basic IP addresses.
2. Enable RIP on Router R1 and Router R2 and advertise interfaces to the RIP process.
3. Enable OSPF on Router R2 and Router R3 and advertise interfaces to the OSPF process.
4. Redistribute routes learnt by RIP to the OSPF process on Router R2.
5. Use an ACL or prefix-list to match the routes to be learnt.
6. Configure route-map.
7. Redistribute RIP routes to the OSPF process on Router R2 and call route-map for routing control.

IV. Configuration Steps

1. Configure basic IP addresses.

```
Ruijie(config)#hostname R1
R1(config)#interface fastEthernet 0/0
```

```
R1(config-if-FastEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
R1(config-if-FastEthernet 0/0)#exit
R1(config)#interface loopback 1
R1(config-if-Loopback 1)#ip address 172.16.1.1 255.255.255.224
R1(config-if-Loopback 1)#exit
R1(config)#interface loopback 2
R1(config-if-Loopback 2)#ip address 172.16.1.33 255.255.255.240
R1(config-if-Loopback 2)#exit
R1(config)#interface loopback 3
R1(config-if-Loopback 3)#ip address 172.16.1.49 255.255.255.248
R1(config-if-Loopback 3)#exit
R1(config)#interface loopback 4
R1(config-if-Loopback 4)#ip address 172.16.1.57 255.255.255.252
R1(config-if-Loopback 4)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface fastEthernet 0/2
R2(config-if-FastEthernet 0/2)#ip address 192.168.1.2 255.255.255.0
R2(config-if-FastEthernet 0/2)#exit
R2(config)#interface fastEthernet 0/0
R2(config-if-FastEthernet 0/0)#ip address 192.168.2.1 255.255.255.0
R2(config-if-FastEthernet 0/0)#exit
```

```
Ruijie(config)#hostname R3
R3(config)#interface fastEthernet 0/1
R3(config-if-FastEthernet 0/1)#ip address 192.168.2.2 255.255.255.0
R3(config-if-FastEthernet 0/1)#exit
```

2. Enable RIP on Router R1 and Router R2 and advertise interfaces to the RIP process.

```
R1(config)#router rip
R1(config-router)#version 2     //Enable RIPv2.
R1(config-router)#no auto-summary     //Disable automatic summarization.
R1(config-router)#network 172.16.0.0     //Advertise the classful network 172.16.0.0 to the RIP
process.
R1(config-router)#network 192.168.1.0
R1(config-router)#exit
```

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.1.0
R2(config-router)#exit
```

3. Enable OSPF on Router R2 and Router R3 and advertise interfaces to the OSPF process.

```
R2(config)#router ospf 1    //Enable OSPF Process 1.
R2(config-router)#network 192.168.2.1 0.0.0.0 area 0    //Advertise the interface with the IP address of 192.168.2.1 to Area 0 of OSPF Process 1.
R2(config-router)#exit
```

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.2.2 0.0.0.0 area 0
R3(config-router)#exit
```

4. Redistribute routes learnt by RIP to the OSPF process on Router R2.

```
R2(config)#router ospf 1
R2(config-router)#redistribute rip subnets    //Redistribute RIP routes to the OSPF process. Subnets must be appended.
R2(config-router)#exit
```

5. Use an ACL or prefix-list to match the routes to be learnt.

   Notes:

   1) Both ACL and prefix-list can be used to match route entries. Select either of them.

   2) If several subnet routes in a network segment need to be matched, the prefix-list is preferred. You can also use an ACL but you need to enter multiple entries.

   In the following example, the route entries 172.16.1.32/27, 172.16.1.48/28, and 172.16.1.56/29 need to be matched, three ACE entries are required in the ACL but only one entry is required in the prefix-list.

   1) Use an ACL to match route entries.

   Notes:

   The ACL is used to match route entries here and the mask is set to 0.0.0.0 to precisely match route entries.

```
R2(config)#ip access-list standard 1
R2(config-std-nacl)#10 permit 172.16.1.32 0.0.0.0
R2(config-std-nacl)#20 permit 172.16.1.48 0.0.0.0
R2(config-std-nacl)#30 permit 172.16.1.56 0.0.0.0
R2(config-std-nacl)#exit
```

   2) Use a prefix-list to match route entries.

   Notes:

   1) The prefix-list can be used only to match route entries. It cannot be used to filter data packets.

   2) The prefix-list matches subnets in a network segment, where **ge** indicates the mask length that a mask length must be greater than or equal to while **le** indicates the mask length that a mask length must be smaller than.

   3) The prefix-list is matched from top to bottom, which is the same as the matching sequence and rules of the ACL.

```
R2(config)#ip prefix-list ruijie seq 10 permit 172.16.1.0/24 ge 28 le 30   //Define a prefix-list named ruijie to match the route prefix 172.16.1.0/24 with the subnet mask length greater than or equal to 28 and smaller than or equal to 30.
```

6. Configure route-map.

Notes:

1) route-map can be used to filter routes and modify route attributes.

2) route-map can use multiple matching conditions (including route entries, metric value, and metric type) whereas distribute-list can be used only to match route entries.

3) route-map is matched from top to bottom and there is an implicit deny any at the end of any route-map.

4) The execution logic of route-map is as follows:

route-map *aaa* permit *10*

match x y z //Multiple match conditions are compiled horizontally, which are in the OR relationship. That is, the match statement is matched as long as one condition is met.

match a

set b //Multiple set statements are compiled vertically and multiple set actions will be executed simultaneously.

set c

route-map *aaa*permit*20*

match p

match q //Multiple match conditions are compiled vertically, which are in the AND relationship. That is, the match statement is matched only when all the conditions are met.

set r

route-map *aaa*deny any (hidden in the system)

The execution logic is as follows:

If (x or y or z)

then set (b and c)

else if (p and q)

then set r

else deny

Match ip address of route-map can be used to match an ACL or prefix-list but only either of them can be selected. See the following examples.

1) **Match ip address** uses an ACL for matching.

```
R2(config)#route-map aaa permit 10
R2(config-route-map)#match ip address 1 //Match route entries in ACL 1.
R2(config-route-map)#set metric-type type-1     //Set the type to 1 for imported external routes.
R2(config-route-map)#set metric 50  //Set metric to 50 for imported external routes.
R2(config-route-map)#exit
```

2) **Match ip address** uses a prefix-list for matching.

```
R2(config)#route-map aaa permit 10
R2(config-route-map)#match ip address prefix-list ruijie //Match route entries in the prefix-list named ruijie.
R2(config-route-map)#set metric-type type-1
R2(config-route-map)#set metric 50
R2(config-route-map)#exit
```

7. Redistribute RIP routes to the OSPF process on Router R2 and call route-map for routing control.

Notes:

Route-map can be applied during **route redistribution** or **establishment of a BGP neighbor relationship using the neighbor command.**

```
R2(config)#router ospf 1
R2(config-router)#redistribute rip subnets route-map aaa //Apply route-map aaa when RIP routes are redistributed to the OSPF process.
R2(config-router)#exit
```

Supplement:

The configuration commands of applying route-map for establishment of a BGP neighbor relationship are as follows:

```
R2(config)#router bgp 1
R2(config-router)#neighbor 10.1.1.1 route-map aaa in //in indicates that control is performed on routes learnt from the neighbor and out indicates that control is performed on routes distributed to the neighbor (route-map is used for the BGP neighbor for routing control. After route-map is configured, routes of the BGP neighbor need to be soft reset so that the configuration takes effect. Do not perform this operation in peak hours of services).
```

V. Verification

Check route entries on Router R3. Route-map used for routing control is configured correctly if Router R3 successfully learns route entries 172.16.1.32/28, 172.16.1.48/29, and 172.16.1.56/30, the routes are of OE1 type, and the cost is changed.

```
R3#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
O E1 172.16.1.32/28 [110/51] via 192.168.2.1, 00:03:14, FastEthernet 0/1
```

```
O E1 172.16.1.48/29 [110/51] via 192.168.2.1, 00:03:14, FastEthernet 0/1
O E1 172.16.1.56/30 [110/51] via 192.168.2.1, 00:03:14, FastEthernet 0/1
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.2/32 is local host.
```

4.2.6 Policy-Based Routing

Features

Policy-Based Routing (PBR) provides a data packet routing and forwarding mechanism that is more flexible than destination address-based routing and forwarding. PBR flexibly selects a route based on the source address, destination address, port ID, and packet length of IP/IPv6 packets.

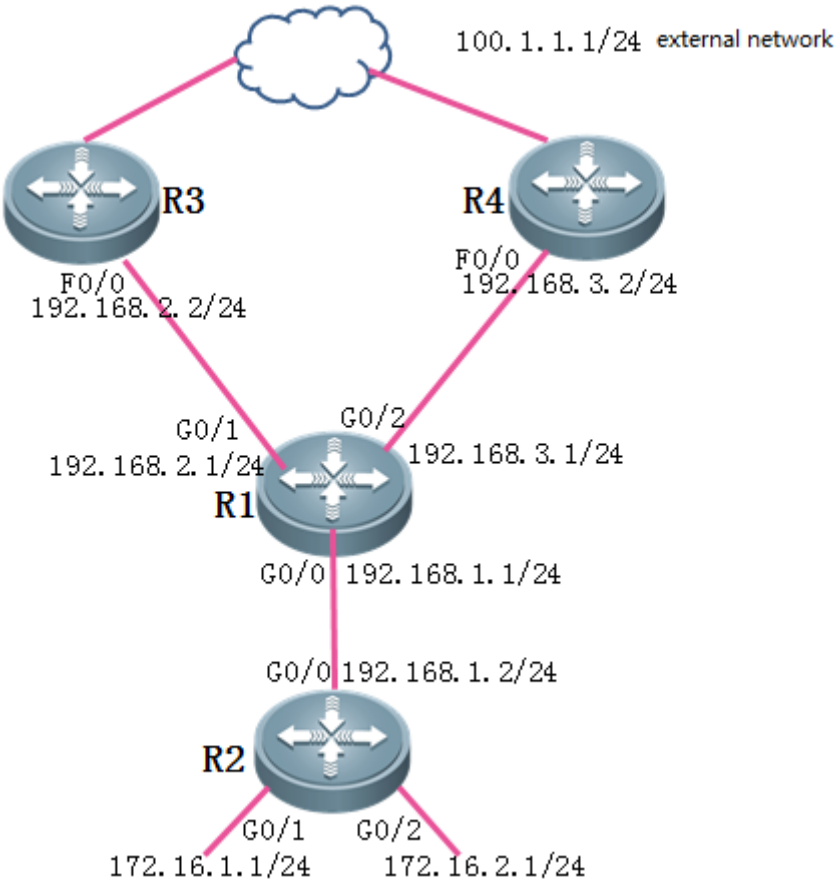
Scenarios

An enterprise has two egress paths, some PCs in the intranet access the Internet through one egress path and the other PCs in the intranet access the Internet through the other egress path. In this case, the PBR function can be enabled on routers.

I.Networking Requirements

As shown in the following networking topology, Router R1 has two egresses to the external network: Router R3 and Router R4. The intranet 172.16.1.0/24 needs to access the external network through Router R3 and the intranet 172.16.2.0/24 needs to access the external network through Router R4.

II. Networking Topology



III. Configuration Tips

1. Configure basic IP addresses.
2. Configure basic IP routes to ensure routes throughout the network are reachable.
3. Configure ACLs on Router R1 to match the traffic of the intranet.
4. Configure PBR.
5. Apply PBR.

IV. Configuration Steps

1. Configure basic IP addresses.

```
Ruijie(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
R1(config-GigabitEthernet 0/0)#exit
R1(config)#interface gigabitEthernet 0/1
```

```
R1(config-GigabitEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
R1(config-GigabitEthernet 0/1)#exit
R1(config)#interface gigabitEthernet 0/2
R1(config-GigabitEthernet 0/2)#ip address 192.168.3.1 255.255.255.0
R1(config-GigabitEthernet 0/2)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface gigabitEthernet 0/0
R2(config-GigabitEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-GigabitEthernet 0/0)#exit
R2(config)#interface gigabitEthernet 0/1
R2(config-GigabitEthernet 0/1)#ip address 172.16.1.1 255.255.255.0
R2(config-GigabitEthernet 0/1)#exit
R2(config)#interface gigabitEthernet 0/2
R2(config-GigabitEthernet 0/2)#ip address 172.16.2.1 255.255.255.0
R2(config-GigabitEthernet 0/2)#exit
```

```
Ruijie(config)#hostname R3
R3(config)#interface fastEthernet 0/0
R3(config-if-FastEthernet 0/0)#ip address 192.168.2.2 255.255.255.0
R3(config-if-FastEthernet 0/0)#exit
```

```
Ruijie(config)#hostname R4
R4(config)#interface fastEthernet 0/0
R4(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
R4(config-if-FastEthernet 0/0)#exit
```

2. Configure basic IP routes to ensure routes throughout the network are reachable.

```
R1(config)#ip route 172.16.0.0 255.255.0.0 192.168.1.2
R2(config)#ip route 100.1.1.0 255.255.255.0 192.168.1.1
R3(config)#ip route 172.16.0.0 255.255.0.0 192.168.2.1
R4(config)#ip route 172.16.0.0 255.255.0.0 192.168.3.1
```

3. Configure ACLs on Router R1 to match the traffic of the intranet.

```
R1(config)#ip access-list standard 10          //Configure ACL 10 to match the traffic of intranet
172.16.1.0/24.
R1(config-std-nacl)#10 permit 172.16.1.0 0.0.0.255
R1(config-std-nacl)#exit
R1(config)#ip access-list standard 20      //Configure ACL 20 to match the traffic of intranet
172.16.2.0/24.
R1(config-std-nacl)#10 permit 172.16.2.0 0.0.0.255
R1(config-std-nacl)#exit
```

4. Configure PBR.

```
R1(config)#route-map ruijiepermit 10        //Configure a route-map named ruijie.
R1(config-route-map)#match ip address 10     //Match traffic of intranet ACL 10.
R1(config-route-map)#set ip next-hop 192.168.2.2 //Set the next-hop address of IP packets to
192.168.2.2.
R1(config-route-map)#exit
R1(config)#route-map ruijie permit 20
R1(config-route-map)#match ip address 20
R1(config-route-map)#set ip next-hop 192.168.3.2
R1(config-route-map)#exit
```

Notes:

1) Route-map matches traffic from top to bottom. When traffic matches the PBR, data is forwarded based on the matched policy and the match stops.

2) There is a deny all statement in the route-map. Intranet traffic that does not match PBR is not discarded but routed and forwarded as normal IP packets.

3) **Set ip next-hop** can be used to set the next-hop IP address or outbound interface of data packets. The next-hop IP address is recommended.

6. Apply PBR.

```
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip policy route-map ruijie //Apply PBR.
R1(config-GigabitEthernet 0/0)#exit
```

Notes:

The PBR must be applied in inbound interfaces of data packets rather than in outbound interfaces of data packets. Actually, PBR forcibly sets the next hop of data packets when data packets are transmitted into a router. In outbound interfaces, a router has conducted IP routing on data packets and sends out the data packets. Therefore, PBR does not take effect in the outbound direction.

V. Verification

Track routes to the external network 100.1.1.0/24 by using the source address on Router R2. If the intranet 172.16.1.0/24 accesses the external network through R3 and the intranet 172.16.2.0/24 accesses the external network through R4, PBR is configured correctly.

```
R2#traceroute 100.1.1.1 source 172.16.1.1
< press Ctrl+C to break >
Tracing the route to 100.1.1.1

 1    192.168.1.1 0 msec 0 msec 0 msec
```

```
2    192.168.2.2 10 msec 0 msec 10 msec     //The intranet 172.16.1.0/24 accesses the external network through Router R3.
Other paths are omitted here.
```

```
R2#traceroute 100.1.1.1 source 172.16.2.1
< press Ctrl+C to break >
Tracing the route to 100.1.1.1

 1    192.168.1.1 0 msec 0 msec 0 msec
2    192.168.3.2 10 msec 0 msec 10 msec     //The intranet 172.16.2.0/24 accesses the external network through Router R4.
Other paths are omitted here.
```

4.2.7 Routing across VRFs

Features:

The VPN Routing and Forwarding table (VRF) is used to solve conflicts between local routes. The connection between a PE and a CE should be correlated with a VRF. Each VRF can be assumed as a "virtual router" and routing between VRFs is isolated.

A VRF consists of:

1. An independent routing table;
2. A set of interfaces belonging to this VRF;
3. A set of routing protocols only applicable to this VRF.

As forwarding between VRFs is isolated, how is route connectivity between VRFs realized? There are two common methods: static routing and policy-based routing to implement routing across VRFs.

Routing across VRFs through Static Routing:

Configuration Template 1:

```
ip route [vrf vrf_name] network mask [interface-type interface-number] [ip-address]
```

Configuration Example 1:

```
ip route vrf vpn1 10.0.0.0 255.0.0.0 GigabitEthernet 3/1/0 12.0.0.1
```

Configuration Explanation 1:

Add a static route to 10.0.0.0/8 segment in the VRF VPN1. Data packets to this segment are forwarded from the GI3/1/0 interface to the next-hop interface 12.0.0.1.

The outbound interface (the GI3/1/0 interface in the example) indicates the VRF to which data packets are transferred, that is, specifies the VRF to which the outbound interface belongs. It indicates that the destination segment will be transferred to this VRF.

//If no VRF is added on an interface, this interface belongs to a global VRF, namely a global routing table.

//As VRF transfer is marked by the outbound interface, configure a static route in the form of outbound interface + next hop IP address. Otherwise, the ARP resolution will fail and data cannot be transferred.

Configuration Template 2:

```
ip route [vrf vrf_name] network mask  ip-address global
```

Configuration Example 2:

```
ip route vrf vpn1 10.0.0.0 255.0.0.0 12.0.0.1 global
```

Configuration Explanation 2:

Global indicates a global routing table.

Add a static route to 10.0.0.0/8 segment in the VRF VPN1. Data packets to this segment are forwarded from the global routing table to the next-hop interface 12.0.0.1.

Difference between Configuration Template 1 and Configuration Template 2:

"Configuration Template 1" supports routing across VRFs between VRFs, and between any VRF and a global routing table.

"Configuration Template 2" supports routing across VRFs between any VRF and a global routing table only and cannot support routing across VRFs between any VRFs.

Routing across VRFs Through Policy-based Routing:

1) Define the ACL interesting traffic.

```
ip access-list extended 100
 10 permit ip 10.0.0.0 0.255.255.255 any
```

2) Define policy-based routing.

```
route-map internet permit 10
 match ip address 100
 set vrf vpn1
```

//set vrf: Routes IP packets through the specified interface using a VRF instance. The priority of policy-based routing is higher than that of common routing. This command cannot not be configured together with **set ip [default] nexthop** or **set [default]interface**. Select routes for IP packets that are received from the interface and match the match rules using

a VRF specified by **set vrf**, no matter whether this VRF and the interface that receives the packets belong to the same VRF.

3) Apply policy-based routing on the interface.

```
interface GigabitEthernet 3/1/0
 ip policy route-map internet
```

I. Actual Networking Requirements

The Multiprotocol Label Switching (MPLS) VPN has been widely used. As known to all, the public network and VPN carried by MPLS cannot access each other because they are across VRFs which isolate the public network from the private network.

The networks have a requirement that some non-VPN services need to be carried by a public network. That is, some services are not included in the VPN can be accessed through a public network. As generally VPN services and non-VPN services have no need for mutual access, the two can be carried by the same public network.

However, some networks have a special requirement that non-VPN services need to access the Internet while the Internet egress belongs to a VRF instance of MPLS VPN. How to realize mutual access between non-VPN services and VPN services becomes an issue.

Requirements:

The department A and office MAN belongs to a non-VPN service and needs to realize mutual access with other non-VPN services.

The department A and office MAN needs to access the Internet.

Non-VPN services other than the department A and office MAN cannot access the Internet.

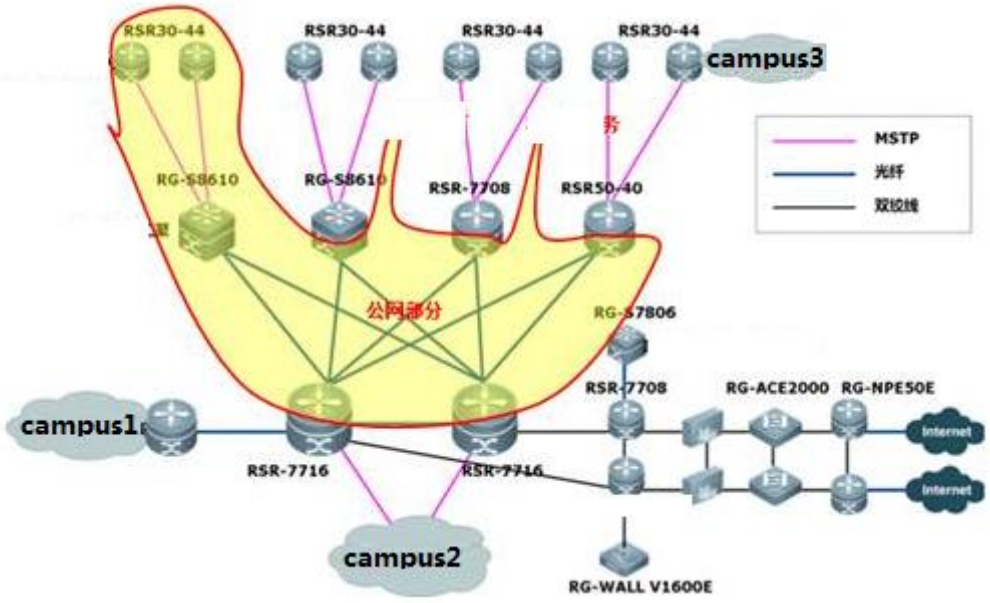
Topology Description:

This topology is the actual topology of a network.

The part with yellow shading refers to the public network and carries VPN services and non-VPN services at the same time.

At the Internet egress, the interface that connects two RSR7716 routers to a RSR7708 router belongs to the VRF Internet.

II. Network Topology



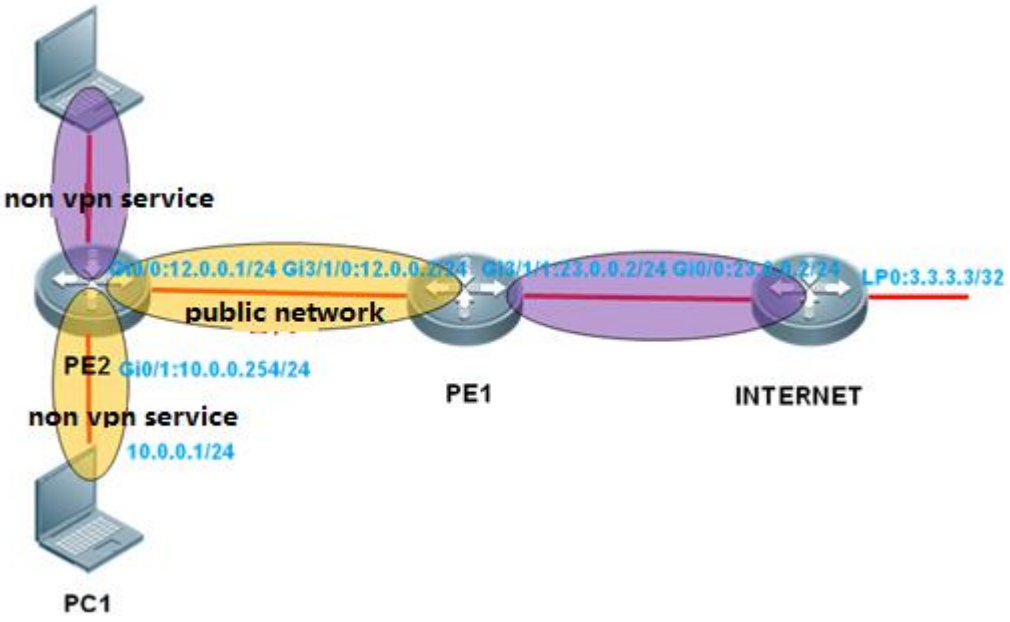
III. Analog Networking Requirements

PC 1 belongs to a non-VPN service and needs to realize mutual access with other non-VPN services.

PC 1 needs to access the Internet.

Non-VPN services other than PC 1 cannot access the Internet.

IV. Network Topology



V. Configuration Tips

Data transmission is bidirectional. Ruijie considers the route connectivity both from PC 1 to the Internet and from the Internet to PC 1.

From PC 1 to the Internet:

Requirement: PC 1 needs to access the Internet, but non-VPN services other than PC 1 cannot access the Internet. Therefore, implement the VRF policy-based routing in the direction of the ingress GI3/1/0 of PE 1. Routing across VRFs is allowed in the PC 1 segment only and blocked in other segments.

Import a default route to the global routing table on PE 1 so that non-VPN services on the public network can learn the default route to the Internet.

From the Internet to PC 1:

PE 1 needs a reverse route. Ruijie uses the static routing across VRFs to reverse to the PC1 segment.

PE 1 needs to redistribute the static route to OSPF in VRF so that the egress router can learn the non-VPN route.

VI. Configuration Steps

Routing across VRFs is generally applied to PEs on the MPLS VPN, but it is VRF transfer in essence and unrelated to the MPLS.Therefore, MPLS VPN configuration is not involved in this example.

PE 1 Configuration:

1. Basic configuration for route connectivity.

```
ip vrf vpn1
interface GigabitEthernet 3/1/0
   ip policy route-map internet
   ip address 12.0.0.2 255.255.255.0
interface GigabitEthernet 3/1/1
   ip vrf forwarding vpn1
   ip address 23.0.0.2 255.255.255.0
interface Loopback 0
   ip address 2.2.2.2 255.255.255.255
router ospf 1
   network 2.2.2.2 0.0.0.0 area 0
   network 12.0.0.2 0.0.0.0 area 0
   default-information originate always
router ospf 10 vrf vpn1
   redistribute static subnets
   network 23.0.0.2 0.0.0.0 area 0
```

2. Routing policy from PC 1 to the Internet (via policy-based routing)

```
route-map internet permit 10
   match ip address 100
   set vrf vpn1
ip access-list extended 100
   10 permit ip 10.0.0.0 0.255.255.255 any
interface GigabitEthernet 3/1/0
   ip policy route-map internet
```

3. Routing policy from the Internet to PC 1 (via static routing)

```
ip route vrf vpn1 10.0.0.0 255.0.0.0 GigabitEthernet 3/1/0 12.0.0.1
```

PE 2 Configuration:

```
interface GigabitEthernet 0/0
   ip ref
   ip address 12.0.0.1 255.255.255.0
interface GigabitEthernet 0/1
   ip ref
   ip address 10.0.0.254 255.255.255.0
interface Loopback 0
   ip ref
   ip address 1.1.1.1 255.255.255.255
router ospf 1
   network 1.1.1.1 0.0.0.0 area 0
   network 10.0.0.0 0.0.0.255 area 0
   network 12.0.0.1 0.0.0.0 area 0
```

Configuration for the Internet egress router

```
interface GigabitEthernet 0/0
   ip ref
   ip address 23.0.0.3 255.255.255.0
interface Loopback 0
   ip ref
   ip address 3.3.3.3 255.255.255.255
router ospf 1
   redistribute static subnets
   network 23.0.0.3 0.0.0.0 area 0
   default-information originate
ip route 0.0.0.0 0.0.0.0 Loopback 0
```

VII. Verification

1. PC 1 can ping the Internet egress router 3.3.3.3.

```
PC1#ping 3.3.3.3
Sending 5, 100-byte ICMP Echoes to 3.3.3.3, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/20 ms
```

4.3 Fixed Switch Modules

Features

The RSR10-02E, RSR20-04E, and RSR20-14E/F routers have fixed switch ports. These routers are designed using a new architecture and therefore, the configuration is different from that of the NMX-24ESW switch module. The fixed switch modules have the following characteristics:

1. You cannot log in to fixed switch modules and they do not need to be managed separately (there is no centralized or distributed management).
2. All configurations of fixed switch modules are completed on the router CLI (integrated routing and switching are implemented).
3. The method for configuring the switching function of fixed switch modules is the same as the configuration method on the switch.

Configuration Examples

(Note: The following configuration is completed on the router CLI.)

1. Create VLAN 10 and VLAN 20.

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exi
Ruijie(config)#vlan 20
```

2. Configure the SVI addresses for VLAN 10 and VLAN 20.

```
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 10.0.0.1 255.255.255.0
Ruijie(config-if-VLAN 10)#exit
```

```
Ruijie(config)#interface vlan 20
Ruijie(config-if-VLAN 20)#ip address 20.0.0.1 255.255.255.0
```

3. Configure attribute of switch ports.

```
Ruijie(config)#interface fastEthernet 1/1
Ruijie(config-if-FastEthernet 1/1)#switchport mode access
Ruijie(config-if-FastEthernet 1/1)#switchport access vlan 10
Ruijie(config-if-FastEthernet 1/1)#exit
Ruijie(config)#interface fastEthernet 1/2
Ruijie(config-if-FastEthernet 1/2)#switchport mode access
Ruijie(config-if-FastEthernet 1/2)#switchport access vlan 20
Ruijie(config-if-FastEthernet 1/2)#exit
Ruijie(config)#interface fastEthernet 1/3
Ruijie(config-if-FastEthernet 1/3)#switchport mode trunk
```

4.4 Security

4.4.1 ACL

4.4.1.1 Standard ACL

Function Introduction

A standard ACL can only match source IP addresses.

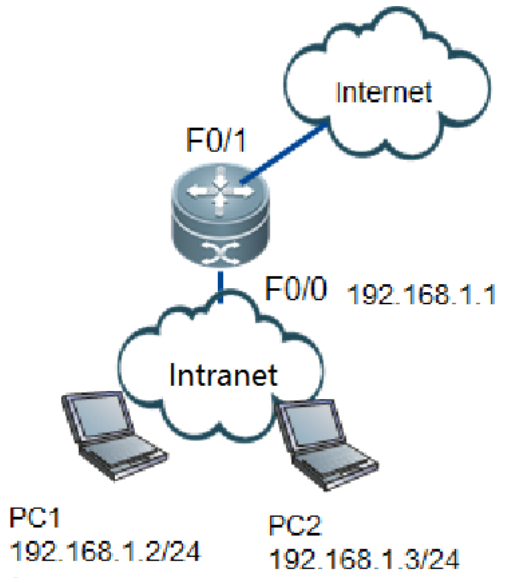
Application Scenario

During security policy setting, a standard ACL can be used to control all traffic from certain IP addresses or a network segment, for example, prohibiting certain IP addresses from accessing all resources. An extended ACL can be used to control partial traffic from certain IP addresses or a network segment, for example, prohibiting certain IP addresses from accessing another network segment.

I.Networking Requirements

The intranet IP address PC1 192.168.1.2 is prohibited from accessing the Internet, but other IP addresses are not prohibited.

II. Network Topology



III. Configurations Tips

1. Configure a standard ACL in global mode.
2. Apply the standard ACL on the intranet interface.
3. Save the configuration.

IV. Configuration Steps

1. Configure a standard ACL in global mode

   Notes:

   (1) The number of a standard ACL ranges from 1 to 99 and from 1300 to 1999. The number of an extended ACL ranges from 100 to 199 and from 2000 to 2699.

   (2) A standard ACL can only match source IP addresses, but an extended ACL can match five elements of the data stream (source IP address, destination IP address, source port, destination port, and protocol number).

   (3) An ACL matches the ACE entries from top to down (according to the ascending order of the sequence numbers of the ACE entries). After finding a match, the ACL executes the action (allow/deny) of the related ACE entry and does not match any other ACE entries.

   (4) An ACL contains an implicit ACE entry (deny any) that denies all traffic.(4) To prohibit a certain network segment while allowing other network segments, after configuring an ACE entry denying the traffic, add an ACE entry "permit any" to allow other traffic.

```
Ruijie(config)#ip access-list standard 1 //Creates a standard ACL 1
```

```
Ruijie(config-std-nacl)#10 deny 192.168.1.2 0.0.0.0 //Configures the ACL entry with a sequence number of 10 to match the IP address 192.168.1.2 (IP address + wildcard mask)
Ruijie(config-std-nacl)#20 permit any      // Configures to permit other traffic
Ruijie(config-std-nacl)#exit
```

2. Call the standard ACL on the intranet interface

```
Ruijie(config)#interface fastEthernet 0/0
Ruijie(config-if-FastEthernet 0/0)#ip access-group 1 in       //Applies the ACL 1 on the intranet interface
```

3. Save the configuration

```
Ruijie(config-if-FastEthernet 0/0)#end
Ruijie#write        //Verifies and saves the configuration
```

V. Verification

Test whether the intranet PCs can access the Internet. If PC1 cannot access the Internet but other PCs can, the configuration is correct.

1. Show configuration of the ACL.

```
Ruijie#show access-lists
ip access-list standard 1
10 deny 192.168.1.2 0.0.0.0
20 permit any
```

2. Show application of the ACL on the interface.

```
Ruijie#show ip access-group
ip access-group 1 in
Applied On interface FastEthernet 0/0.
```

4.4.1.2 Extended ACL

Function Introduction:

An extended ACL can match five elements of the data stream (source IP address, destination IP address, source port, destination port, and protocol number).

Application Scenario:

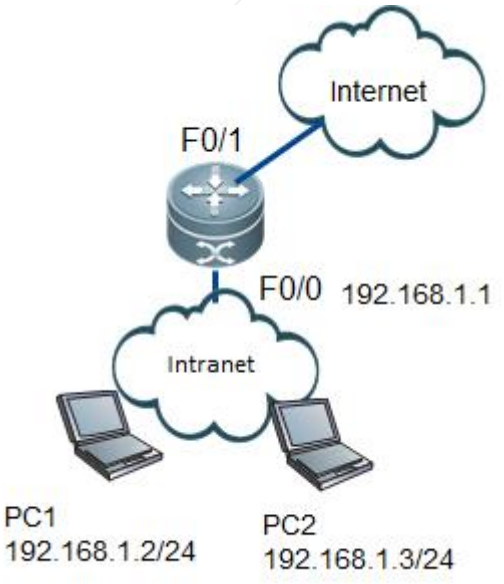
During security policy setting, an extended ACL can be used to control partial traffic from certain IP addresses or a network segment. For example, to prohibit an IP address from accessing websites, an extended ACL can be written with the source IP

address being the aforesaid IP address, the destination IP address being any IP address, and the destination port being 80 (the HHTP port is 80).

I.Networking Requirements

PC1 is prohibited from accessing the Web service of 100.100.100.100 (TCP port80), but other traffic is all permitted.

II. Network Topology



III. Configurations Tips

1. Configure an extended ACL in global mode
2. Apply the extended ACL on the intranet interface
3. Save the configuration

IV. Configuration Steps

1. Configure an extended ACL in global mode

   (1) The number of a standard ACL ranges from 1 to 99 and from 1300 to 1999. The number of an extended ACL ranges from 100 to 199 and from 2000 to 2699.

   (2) A standard ACL can only match source IP addresses, but an extended ACL can match five elements of the data stream (source IP address, destination IP address, source port, destination port, and protocol number).

(3) An ACL matches the ACE entries from top to down (according to the ascending order of the sequence numbers of the ACE entries). After finding a match, the ACL executes the action (allow/deny) of the related ACE entry and does not match any other ACE entries.

(4) An ACL contains an implicit ACE entry (deny any) that denies all traffic.To prohibit a certain network segment while allowing other network segments, after configuring an ACE entry denying the traffic, add an ACE entry "permit any" to allow other traffic.

```
Ruijie(config)#ip access-list extended 100
Ruijie(config-ext-nacl)#10 deny tcp 192.168.1.2 0.0.0.0 100.100.100.100 0.0.0.0 eq 80    //Configures an extended ACL to prohibit the intranet PC1192.168.1.2 fromaccessingPort80 of 100.100.100.100.
Ruijie(config-ext-nacl)#20 permit ip any any    //Configures to permit other traffic (mandatory)
Ruijie(config-ext-nacl)#exit
```

2. Apply the extended ACL on the intranet interface

```
Ruijie(config)#interface fast Ethernet 0/0
Ruijie(config-if-FastEthernet 0/0)#ip access-group 254.00 cm    //Applies the ACL on the interface
```

3. Save the configuration

```
Ruijie(config-if-FastEthernet 0/0)#end
Ruijie#write        //Verifies and saves the configuration
```

V. Verification

1. Test whether theintranet PC1 can access the Web service of 100.100.100.100 and other traffic. If PC1 cannot access the Web service of 100.100.100.100 but can access other traffic, the configuration is correct.
2. Show configuration of the ACL.

```
Ruijie#show access-lists
ip access-list extended 100
10 deny tcp host 192.168.1.2 host 100.100.100.100 eq www
20 permit ip any any
```

3. Show application of the ACL on the interface.

```
Ruijie#show ip access-group
ip access-group 100 in
Applied On interface Fast Ethernet 0/0.
```

4.4.1.3 Reflexive ACL

Function Introduction:

Reflexive ACLs can be used for one-way access. A temporary access list is automatically generated based on the L3 and L4 information of the traffic originated by the intranet. The temporary access list is created according to the following principles: the protocol is not changed, the source IP address and the destination IP address are exchanged, and the source port and the destination port are exchanged. The router allows traffic to enter the intranet only when the L3 and L4 information of the returned traffic exactly matches that of the temporary access list created based on the outbound traffic.

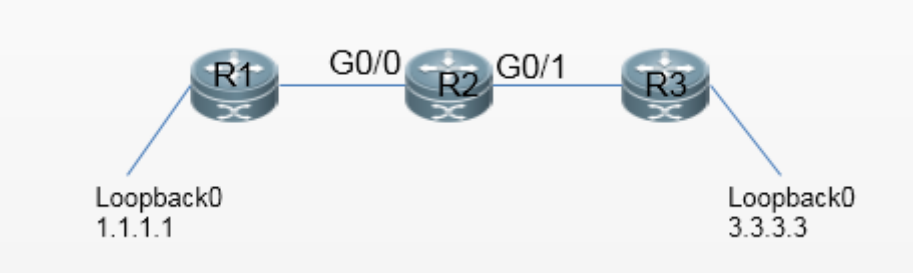
Application Scenario

During security policy setting, standard/extended ACLs can be used to match IP traffic. Besides, reflexive ACLs can also be used to meet one-way access demands. Only when one end actively initiates an access session, the return packets from the peer can be passed. If the peer actively initiates an access session, the access is denied by the ACL.

I.Networking Requirements

The loopback 0 address 1.1.1.1 of R1 can actively access loopback 0 3.3.3.3 of R3, but R3 cannot actively access R1, so as to realize one-way access from R1 to R3.。

II. Network Topology



III. Configurations Tips

1. Complete basic configuration for each device, including the configuration of interface IP addresses and routers.
2. Configure a reflexive ACL on R2.

IV. Configuration Steps

1. Complete basic configuration for each device, including the configuration of interface IP addresses and routers

Omitted.

3. Configure a reflexive ACL

```
R2(config)#ip access-list extended 100
R2(config-ext-nacl)#permit ip host 1.1.1.1 host 3.3.3.3
R2(config)#inter gi0/0
R2(config-if-GigabitEthernet 0/0)#ip access-group 100 in reflect
```

```
R2(config)#ip access-list extended 101
R2(config-ext-nacl)#deny ip any any
R2(config)#inter gi0/1
R2(config-if-GigabitEthernet 0/0)#ip access-group 101 in
```

V. Verification

1. After configuration, the ping from loopback 0 of R1 to loopback 0 of R3 shows to be successful.

```
R1#ping 3.3.3.3 source 1.1.1.1
Sending 5, 100-byte ICMP Echoes to 3.3.3.3, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/20 ms
```

2. The ping from loopback 0 of R3 to loopback 0 of R1 is failed.

```
R3#ping 1.1.1.1 source 3.3.3.3
Sending 5, 100-byte ICMP Echoes to 1.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5)
```

4.4.2 NAT

Features:

NAT: refers to Network Address Translation. During normal data forwarding, the source and destination addresses at the IP header and the port number are not changed. However, when NAT is enabled, the packet header contents are changed, implementing functions such as hiding real addresses of inside and outside hosts, enabling multiple hosts to share a few IP addresses to access inside and outside networks, implementing overlapping of IP addresses, and server load balance.

Port Address Translation (PAT): also known as Network Address Port Translation (NAPT) or port reusing of NAT. It is used to implement network address translation by mapping and distinguishing data streams based on IP addresses and port numbers so that multiple inside hosts can access an outside network using one or a few legal IP addresses.

NAT terms:

Inside local: inside local address (the real address of an inside host, generally a private address).

Inside global: inside global address (the address of an inside host for accessing outside networks after NAT; it is a legal IP address allocated by ISP).

Outside local: outside local address (the address of an outside host after NAT; it is generally a private IP address. When an inside host accesses the outside host, the outside host is considered as an inside host instead of an outside host.)

Outside global: outside global address (the real address of an outside host; it is a legal IP address on the Internet).

4.4.2.1 Source IP Address Translation

4.4.2.2 PPPOE

Function Introduction:

Ruijie products support PPP over Ethernet (PPPOE) for Dial-on-Demand Routing (DDR).Similar to DDR, the products are featured by dialing stimulation upon data communication and automatic disconnection after idle timeout.

The PPPOE implementation of the products is similar to that of senior DDR (DDR Profiles).An Ethernet interface is bound to a logic dialer interface, and the logic dialer interface implements specific negotiation.

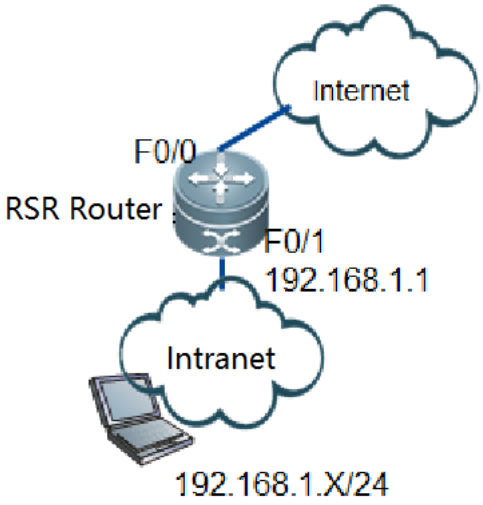
Application Scenario

An enterprise rents the broadband dialing line of a Telecom operator to access Internet resources.

I.Networking Requirements

Intranet users use the RG-RSR router to access Internet, and the Internet line is the ADSL dialing line.

II. Network Topology



III. Configurations Tips

1. Configure dialing.
2. Configure NAT.
3. Configure the default route.

IV. Configuration Steps

1. Enable PPPOE on the physical interface

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface FastEthernet 0/0
Ruijie(config-if-FastEthernet 0/0)#pppoe enable                                    //Enables PPPOE
Ruijie(config-if-FastEthernet 0/0)# pppoe-client dial-pool-number 5 no-ddr  //Binds the Ethernet interface to the dialer pool 5
Ruijie(config-if-FastEthernet 0/0)# ip ref                                                  //Enable Ruijie Express Forwarding (REF). If the command is not identified, REF is enabled by default.
Ruijie(config-if-FastEthernet 0/0)#exit
```

2. Configure the logic dialer interface

```
Ruijie(config)#interface dialer 0
Ruijie(config-if-dialer 0)# ip ref                          //Enables REF. If the command is not identified, ref is enabled by default.
Ruijie(config-if-dialer 0)#encapsulation ppp            //Encapsulates PPP
Ruijie(config-if-dialer 0)#ppp chap hostname pppoe      //Configures the CHAP-encrypted user name: pppoe
Ruijie(config-if-dialer 0)#ppp chap password  pppoe     /Configures the CHAP-encrypted password: pppoe
```

```
Ruijie(config-if-dialer 0)#ppp pap sent-username pppoe password pppoe          //Configures PAP-encrypted user name and password
Ruijie(config-if-dialer 0)#ip address negotiate              //Negotiates to obtain the IP address
Ruijie(config-if-dialer 0)#dialer pool 5                     //Associates the dialer pool 5
Ruijie(config-if-dialer 0)#dialer-group 1                 //Rules stimulating dialing
Ruijie(config-if-dialer 0)#dialer idle-timeout 300  //The dialer is disconnected when the idle time of 300s times out
Ruijie(config-if-dialer 0)#mtu 1492
Ruijie(config-if-dialer 0)#exit
Ruijie(config)#access-list 1 permit any
Ruijie(config)#dialer-list 1 protocol ip permit          //Global dialer list
```

3. Configure NAT

```
Ruijie(config)#access-list 100 permit ip any any         //Defines the data stream to execute NAT. The parameter is set to "any" here.
Ruijie(config)#ip nat pool ruijie prefix-length 24           //Configures the NAT address pool to "ruijie" and match 24bits mask.
Ruijie(config-ipnat-pool)#address interface dialer 0 match interface dialer 0    //Configures IP NAT translation. To forward data from dialer 0, use the address of dialer 0 for NAT.
 Ruijie(config-nat-pool)#exit
Ruijie(config)#ip nat inside source list 100 pool ruijie overload  // Configures the NAT policy. "100" indicates access-list 100 and "ruijie" indicates the address pool of NAT.
 Ruijie(config)#interface dialer 0
Ruijie(config-if-dialer 0)#ip nat outside                       //Indicates an Internet NAT interface
 Ruijie(config-if-dialer 0)#interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)#ip nat inside           //Indicates an intranet NAT interface
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.1.1 255.255.255.0         //Configures an intranet IP address as the intranet gateway
 Ruijie(config-if-FastEthernet 0/1)#ip ref
```

4. Configure the default route

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0  dialer 0
```

V. Verification

1. Check whether dialing is successful

```
Ruijie#show ip interface brief
Interface                        IP-Address(Pri)         OK?      Status
FastEthernet 0/0                 no address            YES       DOWN
FastEthernet 0/1                192.168.1.1/24          YES       UP
dialer 0                          222.168.1.2            YES       UP
```

Note: If the configuration is correct, the IP address is displayed after "dialer 0".

2. After the IP address, mask and gateway of an intranet computer are configured to 192.168.1.x, 255.255.255.0 and 192.168.1.1 respectively, and the DNS is correctly configured, the computer can access Internet.

4.4.2.3 Basic Network Access Configuration for Router without Switching Interface

Introduction:

This section introduces basic network access configurations for routers without switching interfaces. The router models include RSR1002, RSR20-04, RSR20-14, RSR20-18, RSR20-24, RSR30-44 (without NMX-24ESW card), RSR30-X, RSR50 series, and RSR77 series. It is common that the routers have routing interfaces but do not have switching interfaces. If multiple PCs need to access the Internet, a switch is needed in the inside network. This section introduces how to access Internet through NAT and how to map the inside network server to the Internet.

Features:

Port Address Translation (PAT): also known as Network Address Port Translation (NAPT).It is used to implement network address translation by mapping and distinguishing data streams based on IP addresses and port numbers of outside interfaces so that multiple inside hosts can access an outside network using IP addresses of the outside interfaces. It is often used when there is only one public network address.

Address pool translation: It is used to implement network address translation by mapping and distinguishing data streams based on IP addresses and port numbers of the public address pool so that multiple inside hosts can access the outside network using a few public IP addresses. It is often used when one outbound interface has multiple public IP addresses.

Static NAT: It is used to map IP addresses of inside hosts to public IP addresses in the one to one manner, or map IP addresses and port numbers of inside hosts to public IP addresses and port numbers in the one to one manner. It is often used to map an IP address of an inside host to a public IP address, or map a port of an inside server to a port of a public address so that the inside server can be accessed through the public IP address or public IP address + port number.

Scenarios

An enterprise can rent a private line of an operator for network access. The following describes three scenarios for relevant functions:

Scenario 1: When there is only one public IP address, the IP addresses of all inside network users need to be translated into the IP address of the outside network interface, so that all inside network users can access the outside network.

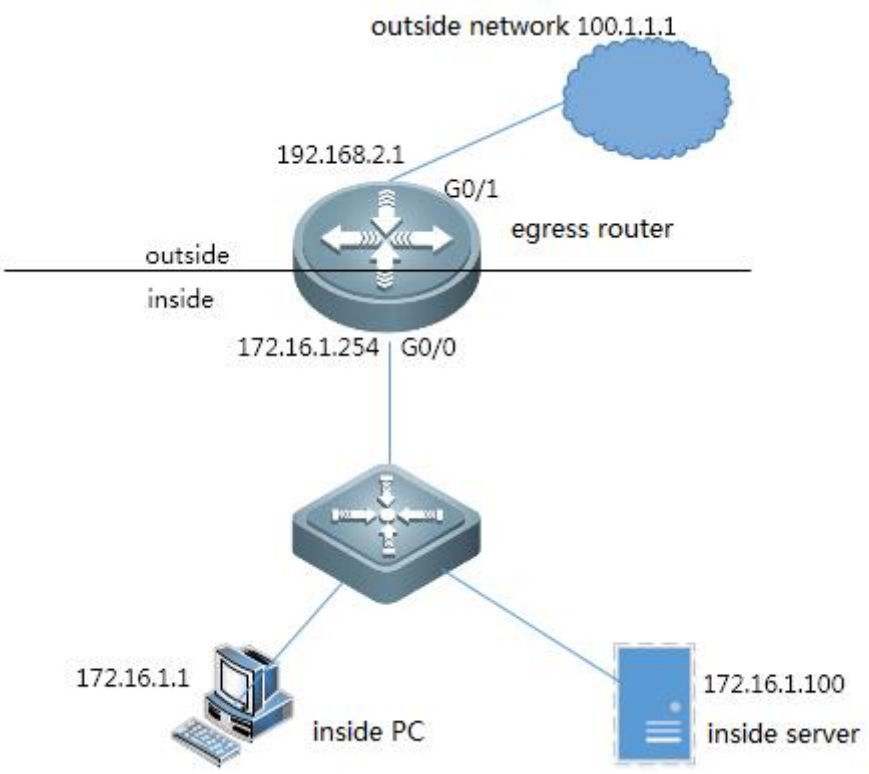
Scenario 2: When there is a public IP address segment, the IP addresses of all inside network users need to be translated into the IP addresses in the public IP address segment, so that the inside network users can access the outside network.

Scenario 3: The inside network server is mapped to a public IP address so that outside network users can access the resources on the inside network server through the public IP address.

I.Networking Requirements

An RSR router is used as the Internet egress, and all inside PC gateways are on this router. The router is used to access the outside network, the IP address (port number) of the inside network server is mapped to a public IP address (port number), so as to provide services for outside users.

II. Network Topology



III. Configurations Steps

1. Configure basic IP addresses.
2. Configure basic IP routes.
3. Configure the DHCP server.
4. Define the inside network port and outside network port for NAT.
5. Configure ACLs on R1, and match the inside network traffic for NAT.

6. Configure a NAT policy for scenario 1.
7. Configure a NAT policy for scenario 2.
8. Configure a NAT policy for scenario 3.

IV. Configuration Steps

1. Configure basic IP addresses.

```
Ruijie(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip address 172.168.1.254 255.255.255.0
R1(config-GigabitEthernet 0/0)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
R1(config-GigabitEthernet 0/1)#exit
```

3. Configure basic IP routes.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2      // Configures the outbound route to the default route of the Internet.
```

4. Configure the DHCP server.

```
Ruijie(conf)#service dhcp //Enables the DHCP service.
Ruijie(conf)#ip  dhcp pool ruijie //ruijie refers to the name of the DHCP address pool, and can be named at random.
Ruijie(dhcp-config)#netw 172.16.1.0 255.255.255.0 //Indicates the network segment of the IP addresses from which a computer will obtain an IP address.
Ruijie(dhcp-config)#default-router 172.16.1.254 //Indicates the gateway address of the f0/1 interface connected to the computer, that is, the IP address of the f0/1 interface.
Ruijie(dhcp-config)#dns-server 202.96.113.34 202.96.13.35  //Indicates the computer's DNS. The former one is the active DNS, and the latter one is the standby DNS.
```

5. Define the inside network port and outside network port for NAT.

```
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip nat outside      //Configures the outside network port for NAT.
R1(config-GigabitEthernet 0/1)#exit
R1(config)#int gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip nat inside //Configures the inside network port for NAT.
R1(config-GigabitEthernet 0/0)#exit
```

5. Configure ACLs on R1, and match the inside network traffic for NAP.

```
R1(config)#ip access-list standard 10
R1(config-std-nacl)#10 permit 172.16.1.0 0.0.0.255
R1(config-std-nacl)#exit
```

6. Configure a NAT policy for scenario 1.

```
R1(config)#ip nat inside source list 10 interface gigabitEthernet 0/1 overload     //Performs NAT for traffic matched by ACL 10, and translates the traffic into the address of the gigabitEthernet 0/1 interface.
```

7. Configure a NAT policy for scenario 2.

(1) Configure the Internet address pool.

```
R1(config)#ip nat pool ruijie netmask 255.255.255.0         //Configures a public address pool named ruijie.
R1(config-ipnat-pool)#address 192.168.2.10 192.168.2.11  //Indicates the start and end IP addresses of a public address.
R1(config-ipnat-pool)#address 192.168.2.15 192.168.2.15 //If there are multiple discontinuous public addresses, multiple public address segments can be configured.
R1(config-ipnat-pool)#exit
```

Notes:

a. The IP addresses in the public address pool may not be in the same network segment as the IP addresses of outside network ports, as long as they are available IP addresses allocated by the outside network.

b. The start and end IP addresses of the public addresses can be discontinuous.

(2) Configure a NAT policy.

```
R1(config)#ip nat inside source list 10 pool ruijie overload      //Performs NAT for traffic matched to ACL 10, and translates the traffic into address in the address pool named ruijie.
```

Notes:

The parameter overload is used to perform NAT overload. If the parameter overload is not added, it indicates that dynamic one-to-one IP mapping is performed, instead of port translation. However, this cannot solve the problem of insufficient public addresses. The purpose of performing NAT at the network egress is to solve the problem of insufficient public addresses, and thus the parameter overload must be added.

8. Configure a NAT policy for scenario 3.

Map the IP address 172.16.1.100 of the inside network server to a public IP address 192.168.2.168; or map the TCP Port 80 of inside network 172.16.1.100 to Port 10 of public network 192.168.2.168.

The following are examples of one-to-one mapping based on IP addresses and port mapping based on TCP and UDP:

(1) One-to-one mapping based on IP addresses

```
R1(config)#ip nat inside source static 172.16.1.100 192.168.2.168 permit-inside      //Maps inside network 172.16.1.100 to public network 192.168.2.168.
```

(2) Port mapping based on TCP and UDP

```
R1(config)#ip nat inside source static tcp 172.16.1.100 80 192.168.2.168 80  permit-inside      //Maps the TCP port 23 of inside network 172.16.1.100 to port 23 of public network 192.168.2.168.
```

Notes:

(1) Static NAT can be used for one-to-one mapping of IP addresses and port mapping based on TCP and UDP.

(2) The permit-inside function: When an inside network server is statically mapped to a public address, if an inside network PC needs to access the server through the public address, the parameter permit-inside must be configured. The parameter permit-inside is recommended when static NAT is configured.

V. Verification

Verification for scenario 1: test whether the inside network can access the outside network. If an inside network PC can access the outside network, the NAT configuration is correct. The NAT translation entries on the outbound router are displayed as follows:

```
R1#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp192.168.2.1:133    172.16.1.1:133     100.1.1.1          100.1.1.1
icmp192.168.2.1:130    172.16.1.1:130     100.1.1.1          100.1.1.1
icmp192.168.2.1:129    172.16.1.1:129     100.1.1.1          100.1.1.1
icmp192.168.2.1:131    172.16.1.1:131     100.1.1.1          100.1.1.1
icmp192.168.2.1:132    172.16.1.1:132     100.1.1.1          100.1.1.1
```

inside global address (public IP address)

Inside local address (private IP address)

Verification for scenario 2: test whether the inside network can access the outside network. If an inside network PC can access the outside network, the NAT configuration is correct. The NAT translation entries on the outbound router are displayed as follows:

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp192.168.2.11:134   172.16.1.1:134     100.1.1.1          100.1.1.1
icmp192.168.2.11:138   172.16.1.1:138     100.1.1.1          100.1.1.1
icmp192.168.2.11:136   172.16.1.1:136     100.1.1.1          100.1.1.1
icmp192.168.2.11:137   172.16.1.1:137     100.1.1.1          100.1.1.1
icmp192.168.2.11:135   172.16.1.1:135     100.1.1.1          100.1.1.1
```

inside global address (public IP address)

inside local address (private IP address)

4.4.2.4 Multiple Egresses NAT and Permit-inside function

Features:

If an outside network has multiple egresses, when data packets are forwarded through different outside interfaces, the inside and outside data streams are translated into different IP addresses + port numbers. In addition, the permit-inside function enables an inside host to access an inside server through a public network address.

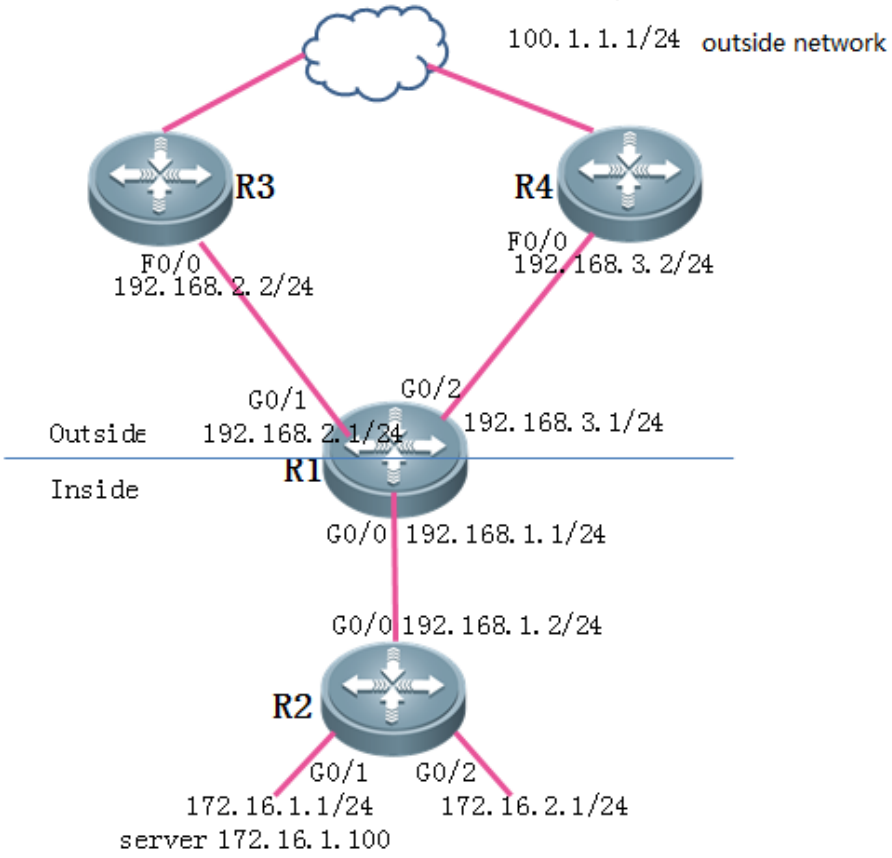
Scenario

An enterprise rents private lines of multiple operators for network access. An inside server needs to be mapped to two outside interfaces so that outside users can access the resources on the server. To enable inside users to access the inside server through the IP addresses of the outside interfaces (sometimes a domain name is needed to access the server, but the resolved domain name maps to the public IP address), you can use the permit-inside function of NAT to enable both inside and outside users to access the server through the public address.

I.Networking Requirements

As shown in the network topology below, R1 has two egresses to an outside network: R3 and R4. The required implementation is as follows: inside users in the network segment of access the outside network through R3 and that the inside addresses are translated into the public address of the egress; inside users in the network segment of access the outside network through R4 and the inside addresses are translated into the public address of the egress. The address 172.16.1.100 of an inside server needs to be translated into the public address192.168.2.168, and both inside and outside PCs need to access the server through the public address.

II. Network Topology



III. Configurations Tips

1. Configure basic IP addresses.
2. Configure basic IP routes.
3. Define the inside port and outside port for NAT.
4. Configure an ACL on R1, and match the inside traffic for NAT.
5. Configure the public address pool.
6. Configure an NAT policy.
7. Configure static NAT.
8. Configure an ACL on R1 and match the inside traffic.
9. Configure a policy route.
10. Apply the policy route.

IV. Configuration Steps

1. Configure basic IP addresses.

```
Ruijie(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
R1(config-GigabitEthernet 0/0)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
R1(config-GigabitEthernet 0/1)#exit
R1(config)#interface gigabitEthernet 0/2
R1(config-GigabitEthernet 0/2)#ip address 192.168.3.1 255.255.255.0
R1(config-GigabitEthernet 0/2)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface gigabitEthernet 0/0
R2(config-GigabitEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-GigabitEthernet 0/0)#exit
R2(config)#interface gigabitEthernet 0/1
R2(config-GigabitEthernet 0/1)#ip address 172.16.1.1 255.255.255.0
R2(config-GigabitEthernet 0/1)#exit
R2(config)#interface gigabitEthernet 0/2
R2(config-GigabitEthernet 0/2)#ip address 172.16.2.1 255.255.255.0
R2(config-GigabitEthernet 0/2)#exit
```

```
Ruijie(config)#hostname R3
R3(config)#interface fastEthernet 0/0
R3(config-if-FastEthernet 0/0)#ip address 192.168.2.2 255.255.255.0
R3(config-if-FastEthernet 0/0)#exit
```

```
Ruijie(config)#hostname R4
R4(config)#interface fastEthernet 0/0
R4(config-if-FastEthernet 0/0)#ip address 192.168.3.2 255.255.255.0
R4(config-if-FastEthernet 0/0)#exit
```

2. Configure basic IP routes so that the entire network is accessible.

```
R1(config)#ip route 172.16.0.0 255.255.0.0 192.168.1.2
R2(config)#ip route 100.1.1.0 255.255.255.0 192.168.1.1
R2(config)#ip route 192.168.0.0 255.255.0.0 192.168.1.1
```

3. Define the inside port and outside port for NAT.

```
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip nat outside      //Configures the outside interface for the first NAT.
R1(config-GigabitEthernet 0/1)#exit
R1(config)#interface gigabitEthernet 0/2
```

```
R1(config-GigabitEthernet 0/1)#ip nat outside      //Configures the outside interface for the second NAT.
R1(config-GigabitEthernet 0/1)#exit
R1(config)#int gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip nat inside   //Configures the inside interface for NAT.
R1(config-GigabitEthernet 0/0)#exit
```

4. Configure an ACL on R1, and match the inside traffic for NAT.

```
R1(config)#ip access-list standard 10
R1(config-std-nacl)#10 permit 172.16.1.0 0.0.0.255
R1(config-std-nacl)#20 permit 172.16.2.0 0.0.0.255
R1(config-std-nacl)#exit
```

5. Configure the public address pool.

Notes:

If multiple public egresses are available and data packets are forwarded from different egresses, NAT needs to be performed to match the available public address of a corresponding egress. Ruijie devices use the parameter **match interface** in the NAT address pool to match the outbound interface for sending data packets. The source addresses of the data packets are translated into the available public address of the outbound interface through NAT.

```
R1(config)#ip nat pool nat_ruijie netmask 255.255.255.0     //Configures the public address pool
nat_ruijie for NAT.
R1(config-ipnat-pool)#address 192.168.2.10 192.168.2.11 match interface GigabitEthernet 0/1   //When data
packets are forwarded through the GigabitEthernet 0/1 interface, the addresses are translated into
192.168.2.10 - 192.168.2.11through NAT.
R1(config-ipnat-pool)#address 192.168.3.10 192.168.3.11 match interface GigabitEthernet 0/2    //When data
packets are forwarded through the GigabitEthernet 0/2 interface, the addresses are translated into
192.168.3.10 - 192.168.3.11through NAT.
R1(config-ipnat-pool)#exit
```

6. Configure the source address translation through NAT.

```
R1(config)#ip nat inside source list 10 pool nat_ruijie overload  //Translates the traffic matched to ACL
10 into addresses in the nat_ruijie address pool, and performs NAT overload.
```

Notes:

The parameter **overload** is used to perform NAT overload. If the parameter **overload** is not added, dynamic one-to-one IP mapping will be performed and port number port translation will not be performed. This cannot solve the problem of insufficient public addresses. If NAT is performed at the network egress to solve the problem of insufficient public addresses, the parameter **overload** must be added.

7. Configuring static NAT

Notes:

Static NAT can be used for one-to-one translation of IP addresses and port number translation based on TCP and UDP.

1) permit-inside: When an inside server is statically mapped to a public address, if an inside PC needs to access the

server through the public address, the parameter permit-inside must be configured. The parameter permit-inside is recommended when static NAT is configured.

The following describes the examples of one-to-one IP address mapping and port number mapping based on TCP and UDP:

One-to-one IP address mapping

```
R1(config)#ip nat inside source static 172.16.1.100 192.168.2.168 permit-inside  //Maps the inside address 172.16.1.100 to the public address 192.168.2.168.
```

2) Port number mapping based on TCP and UDP

```
R1(config)#ip nat inside source static tcp 172.16.1.100 23 192.168.2.168 23  permit-inside  //Maps inside 172.16.1.100 TCP port 23 to public 192.168.2.168 TCP port 23.
```

8. Configure an ACL on R1 and match the inside traffic

Notes:

Restricted by the flow table processing mechanism of Ruijie, the permit-inside function and the policy-based routing of NAT are conflicting with each other. Therefore, it is necessary to deny the traffic in the network segment from inside users to the server in the ACL of a policy route. The policy route is not executed when inside users accesses the server. The configuration is as follows:

```
R1(config)#ip access-list extended 110        //Configures ACL 110 to match the access traffic from the inside network segment 172.16.1.0/24 to the outside network.
R1(config-ext-nacl)#10 deny ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
R1(config-ext-nacl)#20 permit ip 172.16.1.0 0.0.0.255 any
R1(config)#ip access-list extended 120      //Configures ACL 120 to match the access traffic from the inside network segment 172.16.1.0/24 to the outside network.
R1(config-ext-nacl)#10 deny ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
R1(config-ext-nacl)#20 permit ip 172.16.2.0 0.0.0.255 any
R1(config-ext-nacl)#exit
```

If the deny rule is not configured for the traffic between inside servers and users the data translation analysis is as follows:

If an inside PC 172.16.2.10 accesses the server through 192.168.2.168, the translation process is as follows:

	Source IP address	Destination IP address
Before translation	172.16.2.10	192.168.2.168
After translation	192.168.2.168	172.16.1.100

Based on the flow table processing mechanism of Ruijie, the data flow is deemed as a data flow with the source IP address of 172.16.2.10 and the destination IP address of172.16.1.100 after the translation. Therefore, when configuring a policy route ACL, such traffic must be discarded first (that is, all the traffic from the inside network segment to the network segment where the server resides); otherwise, such traffic will be redirected by policy-based routing to the next hop of the specified outside interface. In addition, since the network segment 172.16.1.0 where the server resides is also configured with policy-based routing, the above problem also exists on the server.

9. Configure a policy route.

```
R1(config)#route-map ruijiepermit 10        //Configures route-map ruijie.
R1(config-route-map)#match ip address 110    //Matches the traffic of inside network ACL 110.
R1(config-route-map)#set ip next-hop 192.168.2.2  //Forcibly sets the next hop of IP packets to
192.168.2.2 and sets the egress to R3.
R1(config-route-map)#exit
R1(config)#route-map ruijie permit 20
R1(config-route-map)#match ip address 120
R1(config-route-map)#set ip next-hop 192.168.3.2
R1(config-route-map)#exit
```

10. Apply the policy route.

```
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip policy route-map ruijie //Applies the policy route.
R1(config-GigabitEthernet 0/0)#exit
```

V. Verification

1. Test whether an inside PC can access an outside network, and check whether the policy route is selected. If 172.16.1.0/24 can access the outside network through R3, and 172.16.2.0/24 can access the outside network through R4, the configurations of the multi-egress NAT and policy route are correct.

```
R2#traceroute 100.1.1.1 source 172.16.1.1
< press Ctrl+C to break >
Tracing the route to 100.1.1.1

 1    192.168.1.1 0 msec 0 msec 0 msec
2    192.168.2.2 10 msec 0 msec 10 msec     //172.16.1.0/24 accesses the outside network through R3.
Other routes are omitted.
```

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp192.168.2.11:134   172.16.1.1:134     100.1.1.1          100.1.1.1
icmp192.168.2.11:138   172.16.1.1:138     100.1.1.1          100.1.1.1
icmp192.168.2.11:136   172.16.1.1:136     100.1.1.1          100.1.1.1
icmp192.168.2.11:137   172.16.1.1:137     100.1.1.1          100.1.1.1
icmp192.168.2.11:135   172.16.1.1:135     100.1.1.1          100.1.1.1
```

Inside global address (public IP address)

Inside local address (private IP address)

2. Test whether inside and outside PCs can access the server through the public IP address. If all inside PCs can access the server through the public IP address, the configuration of static NAT is correct. When the inside PCs access the server through the public address, and the NAT mapping table is as follows:

```
Ruijie#telnet 192.168.2.168
Trying 192.168.2.168, 23...

server>

R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 192.168.2.168:1046 172.16.2.10:1046   192.168.2.168:23   172.16.1.100:23
```

Inside global address (server's public address)

Inside local address (PC's private address)

Outside local address (server's public address)

Outside global address (server's private address)

2.4.2.2 Outside Source IP Address Translation

Features:

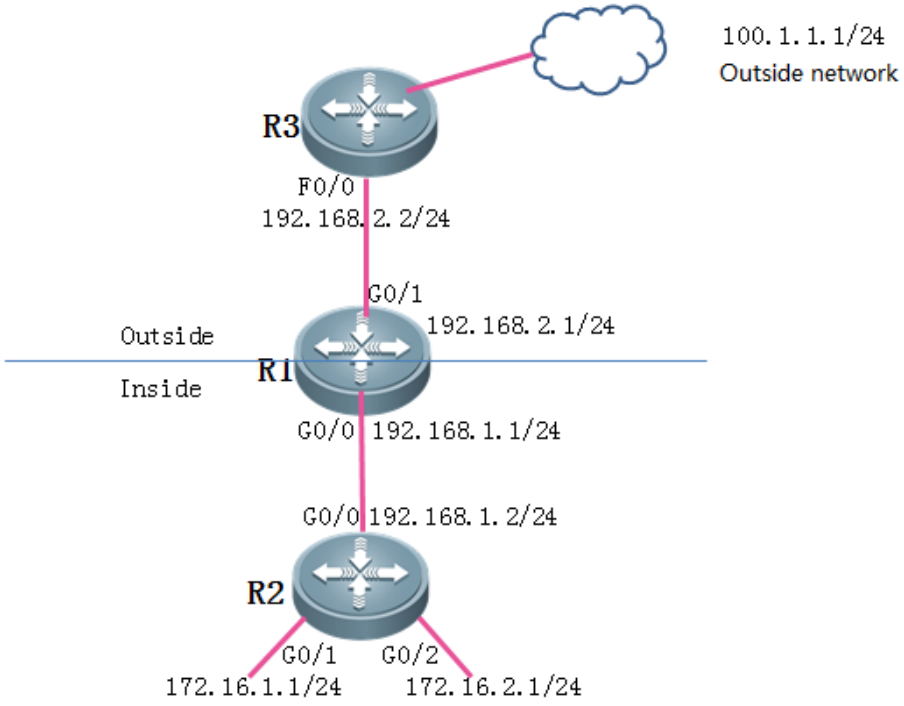
When an inside host needs to access an outside network without introducing an outside route, the IP address + port number of the outside host can be translated into the IP address + port number of the inside network through outside source IP address translation.

I.Networking Requirements

Due to the security policy for the inside network, only mutual access between inside PCs is allowed.

When inside PCs need to access an outside server, the outside source IP address translation function of NAT can be used to translate the public address of the outside server into an inside address so that the inside users do not know that they have accessed the outside network.

II. Network Topology



III. Configurations

1. Configure basic IP addresses.
2. Configure basic IP routes.
3. Define the inside port and outside port for NAT.
4. Configure the outside source address translation of NAT.

IV. Steps

1. Configure basic IP addresses.

```
Ruijie(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
R1(config-GigabitEthernet 0/0)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip address 192.168.2.1 255.255.255.0
R1(config-GigabitEthernet 0/1)#exit
```

```
Ruijie(config)#hostname R2
R2(config)#interface gigabitEthernet 0/0
R2(config-GigabitEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
R2(config-GigabitEthernet 0/0)#exit
```

```
R2(config)#interface gigabitEthernet 0/1
R2(config-GigabitEthernet 0/1)#ip address 172.16.1.1 255.255.255.0
R2(config-GigabitEthernet 0/1)#exit
R2(config)#interface gigabitEthernet 0/2
R2(config-GigabitEthernet 0/2)#ip address 172.16.2.1 255.255.255.0
R2(config-GigabitEthernet 0/2)#exit
```

```
Ruijie(config)#hostname R3
R3(config)#interface fastEthernet 0/0
R3(config-if-FastEthernet 0/0)#ip address 192.168.2.2 255.255.255.0
R3(config-if-FastEthernet 0/0)#exit
```

2. Configure the IP route.

```
R1(config)#ip route 172.16.0.0 255.255.0.0 192.168.1.2
R1(config)#ip route 100.1.1.0 255.255.255.0 192.168.2.2
R2(config)#ip route 192.168.0.0 255.255.0.0 192.168.1.1
R3(config)#ip route 172.16.0.0 255.255.0.0 192.168.2.1      //Configures the return route from the outside network to inside network (If the outside network has no return route to the inside network, the inside source IP address translation needs to be performed on the egress router).
```

3. Define the inside port and outside port for NAT.

```
R1(config)#interface gigabitEthernet 0/1
R1(config-GigabitEthernet 0/1)#ip nat outside      //Configures the outside interface for NAT.
R1(config-GigabitEthernet 0/1)#exit
R1(config)#int gigabitEthernet 0/0
R1(config-GigabitEthernet 0/0)#ip nat inside//Configures the inside interface for NAT.
R1(config-GigabitEthernet 0/0)#exit
```

4. Configure the outside source address translation of NAT.

Notes:

(1) The outside source IP address translation can be used for one-to-one IP address translation and port number translation based on TCP and UDP.

(2) During the outside source IP address translation, the inside local address of the outside server may not be in the network segment on the egress router. The inside local address is only required to be reached by the inside route and be able to route packets of inside PCs accessing the server to the egress router.

The following describes the examples of one-to-one IP address mapping and port number mapping based on TCP and UDP:

1) One-to-one IP address mapping

```
R1(config)#ip nat outside source static 100.1.1.1 192.168.1.168       //When the inside network accesses 192.168.1.168, translates the destination IP address into 100.1.1.1.1
```

2) Port mapping based on TC P and UDP

```
R1(config)#ip nat outside source static tcp 100.1.1.1 23 192.168.1.168 23     //When the inside network accesses TCP Port 23 of 192.168.1.168, translates the destination IP address into Port 23 of 100.1.1.1.
```

V. Verification

Test whether the inside network can be accessed by a private IP addresses visible on the local network through the outside server. If the outside server can be normally accessed, the NAT configuration of the outside source IP address translation is correct. The NAT translation entries on the egress router are displayed as follows:

```
R2#telnet 192.168.1.168 /source interface gi
R2#telnet 192.168.1.168 /source interface gigabitEthernet 0/1
Trying 192.168.1.168, 23...

server>

R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.1.1:1032    172.16.1.1:1032    192.168.1.168:23   100.1.1.1:23
                                          ouside host's inside   outside host's real
                                          private IP address     IP address
```

4.4.3 IPSEC

4.4.3.1 IPSEC Debug

Description of IPSec Debugging

Notes: To debug IPSec, you need to enable "debug crypto isakmp" and "debug crypto ipsec". The customer business may be affected due to IPSec debugging. Therefore, customer permission must be obtained before debugging, and IPSec debugging must be performed during non-peak hours.

```
R1#ping 3.3.3.3 sou 1.1.1.1
Sending 5, 100-byte ICMP Echoes to 3.3.3.3, timeout is 2 seconds:
< press Ctrl+C to break >
*Oct 18 12:26:54: %7: Get acquire: 1.1.1.1/0.0.0.0 -> 3.3.3.3/0.0.0.0  //Triggers interesting traffic, from 1.1.1.1 to 3.3.3.3.
*Oct 18 12:26:54: %7: Get acquire: negotiate source 10.1.1.1 -> dest 202.100.1.100  //Negotiates with the peer 202.100.1.100.
```

```
*Oct 18 12:26:54: %7:  set acquire!
*Oct 18 12:26:54: %7: receve sa acquire
*Oct 18 12:26:54: %7: Acqurire negociate with 202.100.1.100
*Oct 18 12:26:54: %7: (33) sending packet to 202.100.1.100 (I) MM_SI1_WR1, MM_SA_SETUP  // Sends the first packet of Phase 1 to negotiate with the IKE policy parameter.
*Oct 18 12:26:54: %7: sendout main I1, and wait R1
*Oct 18 12:26:54: %7: IKE recvmsg 124 bytes.
*Oct 18 12:26:54: %7: IKE:recvmsg for 10.1.1.1 of interface GigabitEthernet 0/0.
*Oct 18 12:26:54: %7: Not IKE NAT negotiate pkt.
*Oct 18 12:26:54: %7: (33) received packet from 202.100.1.100, (I) MM_SI1_WR1, MM_SA_SETUP  // Receives the second packet of Phase 1.
*Oct 18 12:26:54: %7:   Exchange type : 0x2<sa><vendor ID><vendor ID>
*Oct 18 12:26:54: %7:  extract_payload done!
*Oct 18 12:26:54: %7: main mode r1 process
*Oct 18 12:26:54: %7: (33) Checking ISAKMP transform 1 against priority 10 policy
*Oct 18 12:26:54: %7:     encryption DES-CBC
*Oct 18 12:26:54: %7:     hash SHA
*Oct 18 12:26:54: %7:     auth pre-share
*Oct 18 12:26:54: %7:     default group 1
*Oct 18 12:26:54: %7:     life type in seconds
*Oct 18 12:26:54: %7: life duration 86400 orginal:86400
*Oct 18 12:26:54: %7: (33) atts are acceptable                              // Receives from the peer end the policy field matched with this end.
*Oct 18 12:26:54: %7: vendor_id=0x4a 0x13 0x1c 0x81 0x7 0x3 0x58 0x45 0x5c 0x57 0x28 0xf2 0xe 0x95 0x45 0x2f
*Oct 18 12:26:54: %7:  nat_t's vendor id is detected, nat_vid_t_index=0.//The detection result shows that the peer end supports NAT-T.
*Oct 18 12:26:54: %7: vendor_id=0x4a 0x13 0x1c 0x81 0x7 0x3 0x58 0x45 0x5c 0x57 0x28 0xf2 0xe 0x95 0x45 0x2f //Indicates the vendor_id in RFC3947 used to detect whether the packet passes through the NAT device.
*Oct 18 12:26:54: %7: vendor_id=0xaf 0xca 0xd7 0x13 0x68 0xa1 0xf1 0xc9 0x6b 0x86 0x96 0xfc 0x77 0x57 0x1 0x0
*Oct 18 12:26:54: %7:  dpd's vendor id is detected.
*Oct 18 12:26:54: %7: (33) sending packet to 202.100.1.100 (I) MM_SI2_WR2, MM_KEY_EXCH   //Sends the third packet of Phase 1.
*Oct 18 12:26:54: %7: IKE message packet process over.
*Oct 18 12:26:54: %7: IKE recvmsg 200 bytes.
*Oct 18 12:26:54: %7: IKE:recvmsg for 10.1.1.1 of interface GigabitEthernet 0/0.
*Oct 18 12:26:54: %7: Not IKE NAT negotiate pkt.
*Oct 18 12:26:54: %7: (33) received packet from 202.100.1.100, (I) MM_SI2_WR2, MM_KEY_EXCH //Receives the fourth packet of Phase 1.
```

```
*Oct 18 12:26:54: %7:   Exchange type : 0x2<key><nonce><NAT-D><NAT-D>
*Oct 18 12:26:54: %7:  extract_payload done!
*Oct 18 12:26:54: %7: main mode process R2:(33) processing NONCE payload.
*Oct 18 12:26:54: %7: (33)main mode process R2:SKEYID state generated
*Oct 18 12:26:54: %7: Local has been NAT.  //Indicates that the IP address of the local end has been translated through NAT.
*Oct 18 12:26:54: %7:  Local machine IP is 10.1.1.1, port is 500.
*Oct 18 12:26:54: %7: Local IP NAT-D hash:, len=20
*Oct 18 12:26:54: %7: 0xe3,0x9f,0x02,0x7f,0x11,0x14,0x2a,0xc6,0xe8,0x5d,0x03,0x3d,0xbf,0x41,0x69,0x20,
*Oct 18 12:26:54: %7: 0x46,0xa7,0x1a,0xb7,
*Oct 18 12:26:54: %7: Peer recv local IP NAT-D hash:, len=20
*Oct 18 12:26:54: %7: 0x28,0xea,0x92,0x1d,0x40,0x68,0x5b,0xd5,0xb3,0x88,0x5c,0x5b,0x18,0xd6,0x63,0xcd,
//Checks whether hash of local NAT-D is consistent with hash of received NAT-D. If not, it can be determined that the IP address of the peer has been translated through NAT.
*Oct 18 12:26:54: %7: 0x3c,0xcf,0xe2,0xb7,
*Oct 18 12:26:54: %7: Local record peer NAT-D hash:, len=20
*Oct 18 12:26:54: %7: 0xf8,0x61,0x67,0x99,0x1b,0xbb,0xe0,0xc3,0xa1,0xad,0xec,0xac,0x5f,0x0c,0xb5,0x1e,
*Oct 18 12:26:54: %7: 0xae,0x48,0xf5,0x1b,
*Oct 18 12:26:54: %7: Peer recv NAT-D hash:, len=20
*Oct 18 12:26:54: %7: 0xf8,0x61,0x67,0x99,0x1b,0xbb,0xe0,0xc3,0xa1,0xad,0xec,0xac,0x5f,0x0c,0xb5,0x1e,
*Oct 18 12:26:54: %7: 0xae,0x48,0xf5,0x1b,
*Oct 18 12:26:54: %7:  Peer hasn't been NAT. //Checks whether hash of NAT-D of the peer recorded locally is consistent with hash of NAT-D received from the peer. If yes, it can be determined that the IP address of the peer hasn't been translated through NAT.
*Oct 18 12:26:54: %7: (33) sending packet to 202.100.1.100 (I) MM_SI3_WR3, MM_VERIFY   //Sends the fifth packet of Phase 1 used for identity verification.
*Oct 18 12:26:54: %7: IKE message packet process over.
*Oct 18 12:26:54: %7: IKE recvmsg 72 bytes.
*Oct 18 12:26:54: %7: IKE:recvmsg for 10.1.1.1 of interface GigabitEthernet 0/0.
*Oct 18 12:26:54: %7: IKE NAT negotiate pkt.
*Oct 18 12:26:54: %7: (33) received packet from 202.100.1.100, (I) MM_SI3_WR3, MM_VERIFY
//Receives the sixth packet of Phase 1 used for identity verification.
*Oct 18 12:26:54: %7:   Exchange type : 0x2<id><hash>
*Oct 18 12:26:54: %7:  extract_payload done!
*Oct 18 12:26:54: %7: (33) (auth pre-share) processing ID payload. message ID = 0
*Oct 18 12:26:54: %7: (33) (auth pre-share) processing HASH payload. message ID = 0
*Oct 18 12:26:54: %7: (33) (auth pre-share) SA has been authenticated with 202.100.1.100
*Oct 18 12:26:54: %7: (main mode)(33) (I)Phase_1 negotiate complete!               // Indicates that the negotiation of Phase 1 is completed and the negotiation enters Phase 2.
*Oct 18 12:26:54: %7: +++++++++++++++Fill quick sa's dpd_mode(0).
*Oct 18 12:26:54: %7: (33) Beginning Quick Mode exchange, M-ID of 1336559833
```

```
*Oct 18 12:26:54: %7:   life seconds 3600
*Oct 18 12:26:54: %7:   life kilobytes 4608000
*Oct 18 12:26:54: %7:   mode 3
*Oct 18 12:26:54: %7:   hash 1
*Oct 18 12:26:54: %7: 0 0 0 34 1 3 4 1 10 10 b7 6c 0 0 0 28 1 2 0 0 80 1 0 1 0 2 0 4 0 0 e 10 80 1 0 2
0 2 0 4 0 46 50 0 80 4 0 3 80 5 0 1
*Oct 18 12:26:54: %7: (33)(quick mode) sending packet to 202.100.1.100 (I) QM_SI1_WR1   // Sends the
first packet of Phase 2.
*Oct 18 12:26:54: %7: IKE message packet process over.
*Oct 18 12:26:54: %7: IKE recvmsg 176 bytes.
*Oct 18 12:26:54: %7: IKE:recvmsg for 10.1.1.1 of interface GigabitEthernet 0/0.
*Oct 18 12:26:54: %7: IKE NAT negotiate pkt.
*Oct 18 12:26:54: %7: find phase 2 quick sa!
*Oct 18 12:26:54: %7: (33) (1336559833)received packet from 202.100.1.100, (I) QM_SI1_WR1  //Receives
the second packet of Phase 2.
*Oct 18 12:26:54: %7:   Exchange type : 0x20<hash><sa><nonce><id>
*Oct 18 12:26:54: %7:  extract_payload done!
*Oct 18 12:26:54: %7: (quick mode)(isakmp_id---33) process r1:processing SA payload. message ID =
1336559833a 0 0 40 0 0 0 1 0 0 0 1 0 0 0 34 1 3 4 1 7b 72 b2 44 0 0 0 28 1 2 0 0 80 1 0 1 0 2 0 4 0 0 e
10 80 1 0 2 0 2 0 4 0 46 50 0 80 4 0 3 80 5 0 1
*Oct 18 12:26:54: %7:  set->lifebak_sec=3600
*Oct 18 12:26:54: %7:  Check Attr successful!
*Oct 18 12:26:54: %7: (quick_mode)(I)phase 2 sa established,begining to update sab!
//Indicates that the SA of Phase 2 is generated and it starts to upgrade SAB.
*Oct 18 12:26:54: %7: (33) Creating IPSec SAs-esp.
*Oct 18 12:26:54: %7:     inbound SA has spi 269530988
*Oct 18 12:26:54: %7:     protocol esp, DES_CBC
*Oct 18 12:26:54: %7:     auth MD5
*Oct 18 12:26:54: %7:  fill esp in success!
*Oct 18 12:26:54: %7:     outbound SA has spi 2071114308
*Oct 18 12:26:54: %7:     protocol esp, DES_CBC
*Oct 18 12:26:54: %7:     auth MD5
*Oct 18 12:26:54: %7:  fill esp out success!
*Oct 18 12:26:54: %7:    lifetime of 3600 seconds, soft 3555 seconds
*Oct 18 12:26:54: %7:    lifetime of 4607000 kilobytes, soft 256 kilobytes
*Oct 18 12:26:54: %7: ++++++++++++Fill sab' dpd_mode(0)
*Oct 18 12:26:54: %7: add first sab into salink.
*Oct 18 12:26:54: %7:  life_seconds=3600
*Oct 18 12:26:54: %7:  life_back_seconds=3600
*Oct 18 12:26:54: %7: (quick mode)(isakmp_id---33) sending packet to 202.100.1.100 (I) QM_IDLE  //Sends
the third packet of Phase 2.
```

```
*Oct 18 12:26:54: %7: (quick mode)(isakmp_id---33)process r1:Phase_2 negotiate complete!
*Oct 18 12:26:54: %7: ike's tunnel (number=1)established.
*Oct 18 12:26:54: %7: IKE message packet process over.
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

4.4.3.2 Basic Configuration

4.4.3.3 IPSEC Static Tunnel

Features

When IPSec static tunnels are used for networking, you need to manually configure the two ends of each IPSec tunnel, but dynamic negotiation is not needed. However, with the increase of encrypted points and tunnels, it is more difficult to configure and maintain IPSec tunnels. Therefore, the static tunnel technology is generally used in scenarios with fewer encrypted points.

Scenario

If the headquarters of a company and its branches need to mutually share data through their inside networks and hope that the data are not easily intercepted, cracked or stolen by hackers during transmission, you can create an IPSec VPN on the network devices of the headquarters and branches. The IPSec VPN not only enables the headquarters and branches to directly access the resources of each other, but also encrypts the data during transmission, so as to ensure data security. If both the headquarters and branches use static IP addresses, a static IPSec VPN can be used.

Working Principle

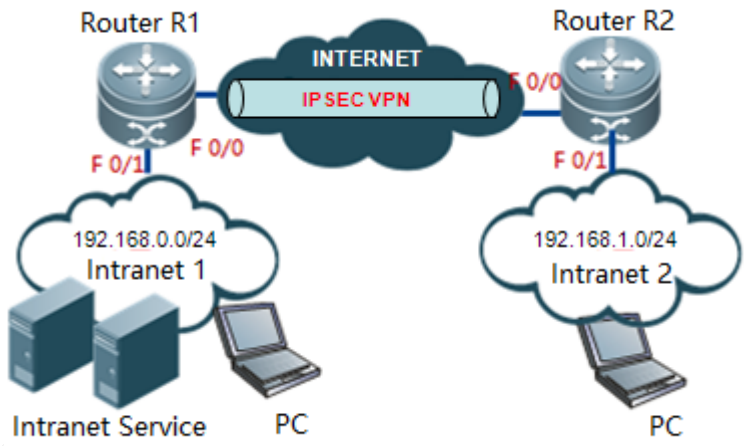
The IPSec VPN has two negotiation stages: ISAKMP and IPSec. At the ISAKMP stage, the protection policies of the two ends are negotiated to verify the validity of the peers, generate the encryption key, and protect the negotiation of the IPSec SA at the second stage. At the IPSec stage, the protection policies for IPSec SA are determined, including whether to use AH or ESP, transmission mode or tunnel mode, and what the protected data is. The negotiation purpose of the second stage is to generate the IPSec SA for protecting IP data. The IPSec communication peers must reach an agreement on the security policies at the first and second stages; otherwise, the IPSec negotiation fails.

I.Networking Requirements

Two LANs access the Internet (or a private network) through two RSR routers respectively. In addition, the network segments 192.168.0.0/24 and 192.168.1.0/24 of the two LANs need to communicate with each other, and the communication traffic must be encrypted.

In this scenario, a static IPSec VPN is deployed on the two RSR routers to implement communication between the LANs and meet the data encryption requirements.

II. Network Topology



III. Configurations

1. Configure routers R1 and R2 so that R1 and R2 can access the Internet and can be successfully pinged by each other.
2. Configure a static IPSec VPN tunnel on R1.
   (1) Configure the interesting traffic of IPSec.
   (2) Configure the ISAKMP policy.
   (3) Configure the pre-shared key.
   (4) Configure the IPSec transform set.
   (5) Configure the IPSec crypto map.
   (6) Apply the crypto map to an interface.
3. Configure a route on R1 to direct the traffic to LAN 2 to the egress.
4. Configure a static IPSec VP tunnel on R2.
   (1) Configure the interesting traffic of IPSec.
   (2) Configure the ISAKMP policy.
   (3) Configure the pre-shared key.
   (4) Configure the IPSec transform set.
   (5) Configure the IPSec crypto map.
   (6) Apply the crypto map to an interface.

5. Configure a route on R2 to direct the network segment route of LAN 1 to the egress.

Notes:

The IP network segments of LAN1 and LAN2 to be mutually accessed shall not be overlapped.

Since RSR50 and RSR50E involve the IPSec function, they must be configured with AIM-VPN encryption cards (For details about how to check whether RSR50 and RSR50E have been configured with AIM-VPN encryption cards, see the appendix at the end of this document).

IV. Configuration Steps

1. Configure routers R1 and R2 so that R1 and R2 can access the Internet and can be successfully pinged by each other.
2. Configure a static IPSec VPN tunnel onR1.

(1) Configure the interesting traffic of IPSec.

```
access-list 101 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255  //Specifies the traffic with source address 192.168.0.0/24 and destination network 192.168.1.0/24 as interesting traffic.
```

(2) Configure the ISAKMP policy.

```
crypto isakmp keepalive 5 periodic  //Configures the IPSec DPD detection function.
crypto isakmp policy 1//Creates a new ISAKMP policy.
authentication pre-share      //Specifies "pre-shared key" as the authentication method. Configures "authentication rsa-sig" in case of digital certificates, and "authentication digital-email" in case of digital envelopes.
group 2    //
encryption 3des      //Specifies 3DES for encryption.
```

(3) Configure the pre-shared key.

```
crypto isakmp key 0 ruijie address 10.0.0.2  //Specifies "ruijie" as the pre-shared key of peer 10.0.0.2. The same key should be used at the peer end. The key does not need to be configured when digital certificates/envelopes are used for authentication.
```

(4) Configure the IPSec transform set.

```
crypto ipsec transform-set myset  esp-des esp-md5-hmac //Specifies that ESP encapsulation, DES encryption and MD5 verification are used for IPsec.
```

(5) Configure the IPSec encryption map.

```
crypto map mymap 5 ipsec-isakmp //Creates a crypto map named "mymap".
set peer 10.0.0.2//Specifies the peer address.
set transform-set myset//Specifies "myset" as the IPsec transform set.
match address 101//Specifies ACL 101 as the interesting address.
```

(6) Apply the encryption map to an interface.

```
interface GigabitEthernet0/0
ip add 10.0.0.1 255.255.255.0
```

```
crypto map mymap
```

3. Configure a route on R1 to direct the traffic to LAN 2 to the egress.

```
    ip route 192.168.1.0 255.255.255.0 10.0.0.2
```

4. Configure a static IPSec VPN tunnel on R2.

(1) Configure the interesting traffic of IPSec.

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255  //Specifies the traffic with source address 192.168.1.0/24 and destination network 192.168.0.0/24 as interesting traffic.
```

(2) Configure the ISAKMP policy.

```
crypto isakmp policy 1  //Creates a new ISAKMP policy.
authentication pre-share      //Specifies "pre-shared key" as the authentication method. Configures "authentication rsa-sig" in case of digital certificates, and "authentication digital-email" in case of digital envelops.
encryption 3des      //Specifies 3DES for encryption.
group 2
```

(3) Configure the pre-shared key.

```
crypto isakmp key 0 ruijie address 10.0.0.1  //Specifies "ruijie" as the pre-shared key of peer 10.0.0.1. The same key should be used at the peer end. The key does not need to be configured in case of digital certificates/envelopes.
```

(4) Configure the IPSec transformation set.

```
crypto ipsec transform-set myset  esp-des esp-md5-hmac //Specifies ESP encapsulation, DES encryption and MD5 Verification for IPSec.
```

(5) Configure the crypto map.

```
crypto map mymap 5 ipsec-isakmp     //Creates a crypto map named "mymap".
set peer 10.0.0.1      //Specifies the peer address.
set transform-set myset    //Specifies "myset" as the transform set.
match address 101     //Specifies ACL 101 as the interesting traffic
```

(6) Apply the crypto map to an interface

```
interface GigabitEthernet0/0
ip add 10.0.0.2 255.255.255.0
crypto map mymap
```

5. Configure a route on R2 to direct the traffic to Lan 1 to the egress.

```
    ip route 192.168.0.0 255.255.255.0 10.0.0.1
```

V. Verification

1. In R1, ping 192.168.1.1 with source IP address 192.168.0.1 The communication is normal.

```
R1#ping 192.168.1.1 source 192.168.0.1
Sending 5, 100-byte ICMP Echoes to 192.168.1.1, timeout is 2 seconds:
< press Ctrl+C to break >
.!!!!
```

2. Check whether the negotiation about the ISAKMP and IPSec SA have been successful on R1.

```
Ruijie#show crypto isakmp sa  //Shows the result of ISAKMP SA negotiation.
destinationsourcestateconn-idlifetime(second)
10.0.0.210.0.0.1IKE_IDLE084129//The ISAKMP negotiation is successful and the status is IKE_IDLE.
Ruijie#show crypto ipsec sa //Shows the result of IPSec SA negotiation.
Interface: GigabitEthernet 0/0
Crypto map tag:mymap    //Indicates the name of the crypto map applied to the interface.
local ipv4 addr 10.0.0.1    //Indicates the IP address used during ISAKMP/IPSec negotiation.
media mtu 1500
================================
sub_map type:static, seqno:5, id=0
local  ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))    //Indicates the source IP addresses of the interesting traffic.
remote  ident (addr/mask/prot/port):(192.168.1.0/0.0.0.255/0/0)) //Indicates the destination IP addresses of the interesting traffic.
PERMIT
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4    //Indicates the number of packets successfully encapsulated, encrypted and digested.
#pkts decaps:4, #pkts decrypt:4, #pkts verify 4//Indicates the number of packets successfully decapsulated, decrypted and verified. When data is encrypted through IPSec for communication, you can see constant increasing of the preceding statistic counts when you repeatedly run the command show crypto ipsec sa.
#send errors 0, #recv errors 0  //Indicates the number of packets that are incorrectly sent and received. Normally, the counts do not increase.
Inbound esp sas:
spi:0x2ecca8e (49072782)    //Indicates the inbound SPI of the IPSec SA.
transform:esp-des esp-md5-hmac    //Indicates that the IPSec encryption transform set is esp-des esp-md5-hmac.
in use settings={Tunnel Encaps,}   //Indicates that the tunnel mode is used.
crypto map mymap 5
sa timing: remaining key lifetime (k/sec): (4606998/1324)  //Indicates that the remaining lifetime of the SA is: 4606998 kilobytes/1324 seconds.
IV size:8 bytes   //Indicates that the length of IV vector is 8 bytes.
Replay detection support: Y   //Indicates the anti-replay processing.
Outbound esp sas:
spi:0x5730dd4b (1462820171)//Indicates the outbound SPI of the IPSec SA. When the inbound SPI and outbound SPI are displayed, it indicates that the IPSec SA negotiation is successful.
```

```
transform: esp-des esp-md5-hmac
 in use settings={Tunnel Encaps,}
crypto map mymap 5
sa timing: remaining key lifetime (k/sec): (4606998/1324)
IV size: 8 bytes
Replay detection support: Y
```

VI. Appendix

1. How to check whether RSR50 and RSR50E have been configured with AIM-VPN encryption cards?

RSR50 and RSR50E have no embedded VPN encryption cards. IPSec is processed through processes, and therefore its performance is very low. For packets of 500pps 60Byte, 50 packets are lost and the packet loss rate is 10%. For packets of larger than 2Kpps, the packet loss rate is 100%.

If IPSec is used when there is no AIM-VPN encryption card, function failures related to IPSec may occur. For example: even when data streams are encrypted with small traffic, the CPU usage is about 100%; or large packets cannot be successfully pinged.

An AIM-VPN card is a pluggable card with a size similar to that of a RAM card. It is inserted inside the management board.

You can use the following method to check whether the management board is configured with an AIM-VPN card:

```
RSR50#debug su
RSR50(support)#pci show
RSR50(support)#
*Jan 29 13:41:23: %7: ==================BEGIN====================
*Jan 29 13:41:23: %7: PCI Bus 0 slot 1/0: PCI device 0x166D:0x0002
*Jan 29 13:41:23: %7: PCI Bus 0 slot 6/0: PCI device 0x104C:0xAC28
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/0: PCI device 0x14D9:0x0020
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 3/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 3/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 4/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 4/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 5/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 5/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 14 slot 1/0: PCI device 0x1131:0x1561
*Jan 29 13:41:23: %7: PCI Bus 14 slot 1/1: PCI device 0x1131:0x1562
*Jan 29 13:41:23: %7: ==================_^_====================
As long as 0x0020 is shown, the management card has the AIM-VPN card.
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/0: PCI device 0x14D9:0x0020
```

Notes:

If the log function is disabled (), the output information of the **pci show** command is empty. If you log in to the device through the vty line, the corresponding information will be output only when the terminal monitor is enabled.

4.4.3.4 IPSEC Dynamic Tunnel

Features

A dynamic IPSec tunnel is generally used in a topology with multiple branches. The dynamic tunnel is configured at the central point to receive IPSec VPN dial-in data from the branches. The central point is easy for configuration and maintenance, and has high expansibility.

Scenario

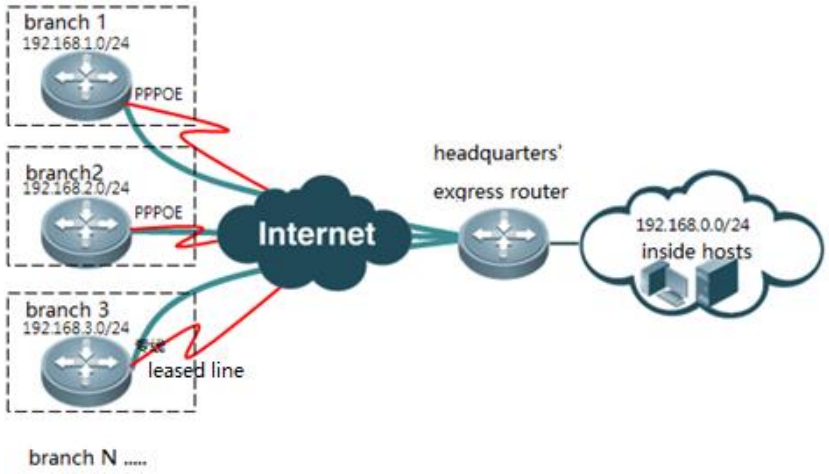
If the headquarters of a company and its branches need to mutually share data through their intranets and hope that the data will not be easily intercepted or cracked by hackers during transmission, you can create an IPSec VPN between the network devices of the headquarters and branches. The IPSec VPN not only enables the headquarters and branches to directly access the resources of each other, but also encrypts the data during transmission, so as to ensure data security. If static IP addresses are used in the headquarters while the dial-up mode is used in the branches (the IP addresses are not permanent, a dynamic IPSec VPN can be used.

I.Networking Requirements

Due to business development, a company sets up multiple branches all over the country. The egress router in the headquarters is connected to the Internet through a dedicated line of a Telecom operator, while the branches are connected to the Internet through a dedicated line or ADSL. The branches need to access the business server in the headquarters, and communication data between the branches and the headquarters needs to be encrypted to ensure business security.

A dynamic IPSec VPN can be deployed on the egress router in the headquarters to receive dial-in data from the branches, so as to enable mutual business access between the headquarters and the branches, and encrypt relevant data.

II. Network Topology



III. Configuration Tips

1. Configure routers in the headquarters and its branches, so that the routers can access the Internet.
2. Configure a dynamic IPSec VPN tunnel on the egress router in the headquarters.
   (1) Configure the ISAKMP policy.
   (2) Configure the pre-shared key.
   (3) Configure the IPSec transform set.
   (4) Configure the dynamic crypto map.
   (5) Map the dynamic IPSec encryption map to the static IPSec encryption map.
   (6) Apply the encryption map to an interface.
3. Configure the route on the router of the headquarters, and direct the branches to the egress.
4. Configure a static IPSec VPN tunnel on the routers of the branches.
   (1) Configure the interesting traffic of IPSec.
   (2) Configure the ISAKMP policy.
   (3) Configure the pre-shared key.
   (4) Configure the IPSec transform set.
   (5) Configure the crypto map.
   (6) Apply the encryption map to an interface.
6. Configure the routes on the routers of the branches, and direct the traffic to the headquarters to the egress.

Notes:

- The IP network segments of LAN 1 and LAN 2 to be mutually accessed must not be overlapped.
- Since RSR50 and RSR50E involve the IPSec function, they must be configured with AIM-VPN encryption cards (For details about how to check whether RSR50 and RSR50E have been configured with AIM-VPN encryption cards, see the appendix at the end of this section).

IV. Configuration Steps

1. Configure routers in the headquarters and its branches, so that the routers can access the Internet

   It must be ensure that the ping from branches to the headquarters' public IP address is successful.

2. Configure a dynamic IPSec VPN tunnel on the egress router of the headquarters.

   (1) Configure the ISAKMP policy.

```
crypto isakmp policy 1   //Creates a new ISAKMP policy.
encryption 3des        //Specifies to use 3DES for encryption.
authentication pre-share            //Specifies the authentication method is "pre-shared key".
Configures "authentication rsa-sig" in case of digital certificates, and "authentication digital-email"
in case of digital envelopes.
```

   (2) Configure the pre-shared key.

```
crypto isakmp key 0 ruijie address 0.0.0.0 0.0.0.0                  //Configures the pre-shared key to
"ruijie". The same key shall be configured for the IPSec client. Because the IP address at the peer end
is dynamic, the address 0.0.0.0 0.0.0.0 is used to represent all IPSec clients.
```

   (3) Configure the IPSec transform set.

```
crypto ipsec transform-set myset esp-des esp-md5-hmac   //Specifies IPSec to use ESP for encapsulation,
DES for encryption and MD5 for verification.
```

   (4) Configure the IPSec crypto map.

```
crypto dynamic-map dymymap 5             //Creates a dynamic IPSec crypto map named "dymymap".
set transform-set myset                            //Specifies the transform set to "myset".
```

   (5) Map the dynamic crypto map to the static crypto map.

```
crypto map mymap 10 ipsec-isakmp dynamic dymymap   //Maps the dynamic crypto map "dymymap" to the
static crypto map "mymap".
```

   (6) Apply the crypto map to an interface.

```
interface GigabitEthernet 0/0
 crypto map mymap
```

3. Configure the route on the router of the headquarters, and direct the traffic to the branches to the egress.

```
  ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 192.168.2.0 255.255.255.0 10.0.0.2
ip route 192.168.3.0 255.255.255.0 10.0.0.2
......
```

4. Configure the static IPSec VPN tunnel on the routers of the branches(taking branch1 as an example).

   (1) Configure the interesting traffic of IPSec.

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255  //Specifies the traffic with
source address 192.168.1.0/24 and destination network 192.168.0.0/24 as interesting traffic.
```

(2) Configure the ISAKMP policy.

```
crypto isakmp keepalive 5 periodic //Configures the IPSec DPD detection function.
crypto isakmp policy 1            //Creates a new ISAKMP policy.
authentication pre-share          //Specifies the authentication method is "pre-shared key". Configures "authentication rsa-sig" in case of digital certificates, and "authentication digital-email" in case of digital envelopes.
encryption 3des                  //Specifies to use 3DES for encryption.
```

(3) Configure the pre-shared key.

```
crypto isakmp key 0 ruijie address 10.0.0.1  //Specifies "ruijie" as the pre-shared key of the peer 10.0.0.1. The same key shall be used on the egress router of the headquarters. The key does not need to be configured in case of digital certificates/envelopes.
```

(4) Configure the IPSec transform set.

```
crypto ipsec transform-set myset  esp-des esp-md5-hmac //Specifies IPSec to use ESP for encapsulation, DES for encryption and MD5 for verification.
```

(5) Configure the crypto map

```
crypto map mymap 5 ipsec-isakmp //Creates a crypto map named "mymap"
set peer 10.0.0.1                //Specifies the peer address.
set transform-set myset          //Specifies the transform set as "myset".
match address 101               //Specifies ACL 101 as the interesting traffic .
```

(6) Apply the encryption map to an interface.

```
interface dialer 0
crypto map mymap
```

5. Configure the routes on the routers of the branches, and direct the traffic to the headquarters to the egress.

```
  ip route 192.168.0.0 255.255.255.0 dialer 0
```

V. Verification

1. Ping 192.168.0.1 from the router of branch 1 with source IP address 192.168.1.1. The communication is normal.

```
R1#ping 192.168.0.1 source 192.168.1.1
Sending 5, 100-byte ICMP Echoes to 192.168.1.1, timeout is 2 seconds:
< press Ctrl+C to break >
.!!!!
```

2. On the router of branch1, check whether ISAKMP and IPSec SA negotiations are successful.

```
Ruijie#show crypto isakmp sa                                    //Shows the result of ISAKMP SA negotiation.
 destination       source           state                  conn-id          lifetime(second)
```

```
10.0.0.2          10.0.0.1          IKE_IDLE                0                84129
//The ISAKMP negotiation is successful and the status is IKE_IDLE.
Ruijie#show crypto ipsec sa                                          //Shows the result of IPSec
SA negotiation.
Interface: GigabitEthernet 0/0
Crypto map tag:mymap    //Indicates the name of the crypto map applied to the interface.
local ipv4 addr 10.0.0.1                  //Indicates the IP address used during ISAKMP/IPSec
negotiation.
        media mtu 1500
        ================================
        sub_map type:static, seqno:5, id=0
        local  ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))  //Indicates the source IP
address of the interesting traffic.
remote  ident (addr/mask/prot/port): (192.168.1.0/0.0.0.255/0/0))//Indicates the destination IP
address of the interesting traffic.
        PERMIT
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4    //Indicates the number of packets successfully
encapsulated, encrypted and digested.
#pkts decaps:4, #pkts decrypt:4, #pkts verify 4    //Indicates the number of packets successfully
decapsulated, decrypted and verified. When data is encrypted through IPSec for communication, you can
see constant increasing of the preceding statistic counts when you repeatedly run the command show
crypto ipsec sa.
#send errors 0, #recv errors 0    //Indicates the number of packets that are incorrectly sent and
received. Normally, the counts do not increase.
 Inbound esp sas:
spi:0x2ecca8e (49072782)                  //Indicates the inbound SPI of IPSec SA.
              transform: esp-des esp-md5-hmac  //Indicates that the IPSec encryption transform set
is esp-des esp-md5-hmac.
in use settings={Tunnel Encaps,}         //Indicates that the tunnel mode is used.
              crypto map mymap 5
              sa timing: remaining key lifetime (k/sec): (4606998/1324)  //Indicates that the
remaining lifetime of the SA is: 4,606,998 kilobytes/1,324 seconds.
              IV size: 8 bytes   //Indicates that the length of IV vector is 8 bytes.
Replay detection support: Y   //Indicates the anti-replay processing.
 Outbound esp sas:
spi:0x5730dd4b (1462820171)//Indicates the outbound SPI of IPSec SA. Only when the inbound SPI and
outbound SPI are both displayed, the IPSec SA negotiation is successful.
              transform: esp-des esp-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map mymap 5
              sa timing: remaining key lifetime (k/sec): (4606998/1324)
```

```
IV size: 8 bytes
Replay detection support:Y
```

VI. Appendix

1. How to check whether RSR50 and RSR50E have been configured with AIM-VPN encryption cards?

RSR50 and RSR50E have no embedded VPN encryption cards. IPSec is processed through processes, and therefore its performance is poor. For packets of 500pps 60Byte, 50 packets are lost and the packet loss rate is 10%. For packets of larger than 2Kpps, the packet loss rate is 100%.

If IPSec is used when there is no AIM-VPN encryption card, function failures related to IPSec may occur. For example, the CPU utilization is constantly at 100%, even though the encrypted data traffic is light. , or the ping with large packets size would fail.

An AIM-VPN card is a pluggable card with a size similar to that of a memory bank. It is inserted inside the management board.

You can use the following method to check whether the management board is configured with an AIM-VPN card:

```
RSR50#debug su
RSR50(support)#pci show
RSR50(support)#
*Jan 29 13:41:23: %7: ================BEGIN==================
*Jan 29 13:41:23: %7: PCI Bus 0 slot 1/0: PCI device 0x166D:0x0002
*Jan 29 13:41:23: %7: PCI Bus 0 slot 6/0: PCI device 0x104C:0xAC28
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/0: PCI device 0x14D9:0x0020
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 3/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 3/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 4/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 4/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 5/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 5/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 14 slot 1/0: PCI device 0x1131:0x1561
*Jan 29 13:41:23: %7: PCI Bus 14 slot 1/1: PCI device 0x1131:0x1562
*Jan 29 13:41:23: %7: ================_^_==================
As long as 0x0020 is displayed, the management board has the AIM-VPN card.
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/0: PCI device 0x14D9:0x0020
```

Notes:

If the logging function is disabled (), the output data of the **pci show** command is empty. If you log in to the device through the VTY line, the corresponding data will be output only when the terminal monitor is enabled.

4.4.3.5 IPSEC Dynamic Tunnel with Domain Name Authentication

Features

A dynamic IPSec tunnel is generally used in a topology with multiple branches. The dynamic tunnel is configured at the central point to receive IPSec VPN dial-in information from the branches. The central point is easy for configuration and maintenance, and has high expansibility.

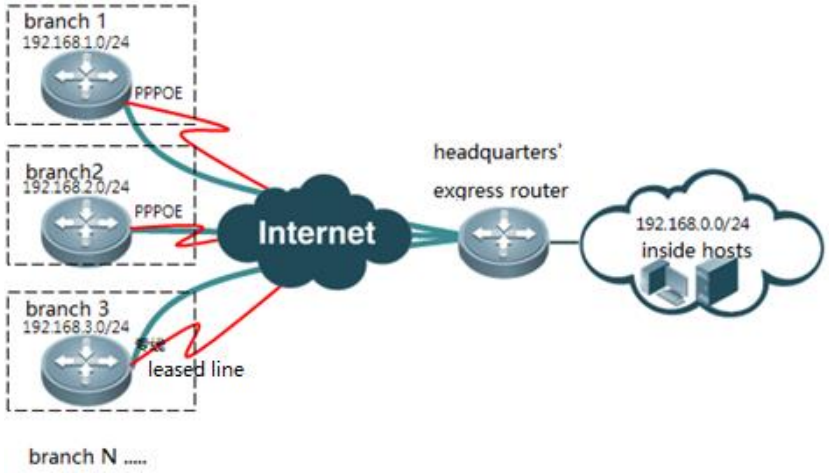
Because IP addresses in the branches are not static, it is unable to use the IP addresses to specify different pre-shared keys. If the same pre-shared key is used in all branches, the key is easily leaked, and thus network security is under threat. This problem can be solved through domain name authentication. Different domain names are allocated to different branches and different keys are specified to different domain names. In this way, key security is guaranteed.

I.Networking Requirements

Due to business development, a company sets up multiple branches all over the country. The egress router in the headquarters is connected to the Internet through a dedicated line of a Telecom operator, while the branches are connected to the Internet through a dedicated line or ADSL. The branches need to access the business server in the headquarters, and communication data between the branches and the headquarters needs to be encrypted to ensure business security.

A dynamic IPSec VPN can be deployed on the egress router in the headquarters to receive dial-in information from the branches, so as to enable mutual business access between the headquarters and the branches, and encrypt relevant data. When the branches use the IPSec VPN to access the Internet in dial-up mode, the key of each branch is authenticated separately.

II. Network Topology



III. Configuration Tips

1. Configure routers in the headquarters and its branches, so that the routers can access the Internet.
2. Configure a dynamic IPSec VPN tunnel on the egress router in the headquarters.

(1) Configure the ISAKMP policy.

(2) Configure the pre-shared key.

(3) Configure the ISAKMP mode as automatic identification.

(4) Configure the IPSec transform set.

(5) Configure the dynamic IPSec crypto map.

(6) Map the dynamic IPSec encryption map to the static IPSec encryption map.

(7) Apply the encryption map to an interface.

3. Configure the route on the router of the headquarters, and direct the traffic to the branches to the egress.

4. Configure the static IPSec VPN tunnel on the routers of the branches.

(1) Configure the self-identity.

(2) Configure interesting traffic of IPSec.

(3) Configure the ISAKMP policy.

(4) Configure the pre-shared key.

(5) Configure the IPSec transform set.

(6) Configure the crypto map.

(7) Apply the encryption map to an interface.

5. Configure the routes on the routers of the branches, and direct the traffic to headquarters to the egress.

Notes:

- The IP network segments of LAN 1 and LAN 2 to be mutually accessed must not be overlapped.
- Since RSR50 and RSR50E involve the IPSec function, they must be configured with AIM-VPN encryption cards (For details about how to check whether RSR50 and RSR50E have been configured with AIM-VPN encryption cards, see the appendix at the end of this section).

IV. Configuration Steps

1. Configure routers in the headquarters and its branches, so that the routers can access the Internet.

   It must be ensure that the ping from branches to the headquarters' public IP address is successful.

2. Configure a dynamic IPSec VPN tunnel on the egress router of the headquarters.

(1) Configure the ISAKMP policy.

```
crypto isakmp policy 1     //Creates a new ISAKMP policy.
encryption 3des        //Specifies to use 3DES for encryption.
authentication pre-share            //Specifies the authentication method is "pre-shared key".
Configures "authentication rsa-sig" in case of digital certificates, and "authentication digital-
email" in case of digital envelopes.
```

(3) Configure the pre-shared key.

```
crypto isakmp key 0 password3 hostname site3.ruijie.com.cn
crypto isakmp key 0 password2 hostname site2.ruijie.com.cn
crypto isakmp key 0 password1 hostname site1.ruijie.com.cn     //Configures the pre-shared key of each branch separately, and uses hostname to specify the name of each branch.
```

(4) Configure the ISAKMP mode as automatic identification.

```
crypto isakmp mode-detect       //Configures the ISAKMP mode as automatic identification, so that negotiations can be received from the branches in IKE aggressive mode.
```

(5) Configure the IPSec encryption transform set.

```
crypto ipsec transform-set myset esp-des esp-md5-hmac      //Specifies IPSec to use ESP for encapsulation, DES for encryption and MD5 for verification.
```

(5) Configure the dynamic IPSec crypto map

```
crypto dynamic-map dymymap 5            //Creates a dynamic IPSec crypto map named "dymymap".
set transform-set myset                    //Specifies the transform set to "myset".
```

(6) Map the dynamic crypto map to the static crypto map.

```
crypto map mymap 10 ipsec-isakmp dynamic dymymap   //Maps the dynamic crypto map "dymymap" to the static crypto map "mymap".
```

(7) Apply the encryption map to an interface.

```
interface GigabitEthernet 0/0
   crypto map mymap
```

3. Configure the router on the router of the headquarters, and direct the traffic to the branches to the egress.

```
    ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 192.168.2.0 255.255.255.0 10.0.0.2
ip route 192.168.3.0 255.255.255.0 10.0.0.2
......
```

4. Configure the static IPSec VPN tunnel on the routers of the branches (taking branch1 as an example).

(1) Configure the self-identity.

```
self-identity fqdn site1.ruijie.com.cn  //Configures the self-identity to "site1.ruijie.com".
```

(2) Configure the interesting traffic of IPSec

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255  //Specifies the traffic with source address 192.168.1.0/24 and destination network 192.168.0.0/24 as interesting traffic.
```

(3) Configure the ISAKMP policy

```
crypto isakmp keepalive 5 periodic //Configures the IPSec DPD detection function.
crypto isakmp policy 1            //Creates a new ISAKMP policy.
authentication pre-share         //Specifies the authentication method is "pre-shared key". Configures "authentication rsa-sig" in case of digital certificates, and "authentication digital-email" in case of digital envelopes.
```

```
encryption 3des                 //Specifies to use 3DES for encryption.
```

(4) Configure the pre-shared key.

```
crypto isakmp key 0 password1 address 10.0.0.2  //Specifies "password1" as the pre-shared key of the
peer 10.0.0.1. The key must be the same as that specified by the headquarters for the branch. The key
does not need to be configured in case of digital certificates/envelopes.
```

(3) Configure the IPSec transform set.

```
crypto ipsec transform-set myset  esp-des esp-md5-hmac //Specifies IPSec to use ESP for
encapsulation, DES for encryption and MD5 for verification.
```

(6) Configure the crypto map.

```
crypto map mymap 5 ipsec-isakmp //Creates a crypto map named "mymap".
set peer 10.0.0.2                 //Specifies the peer address.
set transform-set myset           //Specifies the transform set to "myset".
set exchange-mode aggressive   //Specifies to use the aggressive mode to initiate IKE negotiations.
match address 101                //Specifies ACL 101 as the interesting traffic.
```

(7) Apply the encryption map to an interface.

```
interface dialer 0
    crypto map mymap
```

5. Configure the routes on the routers of the branches, and direct the traffic to the headquarters to the egress.

```
ip route 192.168.0.0 255.255.255.0 dialer 0
```

V. Verification

1. Pint 192.168.0.1 from the router of branch 1 with source IP address 192.168.1.1. The communication is normal.

```
R1#ping 192.168.0.1 source 192.168.1.1
Sending 5, 100-byte ICMP Echoes to 192.168.1.1, timeout is 2 seconds:
< press Ctrl+C to break >
.!!!!
```

2. On the router of branch1, check whether ISAKMP and IPSec SA negotiations are successful.

```
Ruijie#show crypto isakmp sa                                  //Shows the result of ISAKMP SA
negotiation.
 destination       source            state                   conn-id          lifetime(second)
10.0.0.2          10.0.0.1          IKE_IDLE                0                84129                //The
ISAKMP negotiation is successful and the status is IKE_IDLE.
Ruijie#show crypto ipsec sa                                          //Shows the result of IPSec SA
negotiation.
Interface: GigabitEthernet 0/0
Crypto map tag:mymap    //Indicates the name of the crypto map applied to the interface.
```

```
local ipv4 addr 10.0.0.1                  //Indicates the IP address used during ISAKMP/IPSec negotiation.
        media mtu 1500
        ================================
        sub_map type:static, seqno:5, id=0
        local  ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))   //Indicates the source IP
address of the interesting traffic.
remote  ident (addr/mask/prot/port): (192.168.1.0/0.0.0.255/0/0))//Indicates the destination IP address of
the interesting traffic.
        PERMIT
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4//Indicates the number of packets successfully
encapsulated, encrypted and digested.
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4//Indicates the number of packets successfully
decapsulated, decrypted and verified. When data is encrypted through IPSec for communication, you can see
constant increasing of the preceding statistic counts when you repeatedly run the command show crypto
ipsec sa.
#send errors 0, #recv errors 0//Indicates the number of packets that are incorrectly sent and received.
Normally, the counts do not increase.
 Inbound esp sas:
spi:0x2ecca8e (49072782)               //Indicates the inbound SPI of IPSec SA.
              transform: esp-des esp-md5-hmac    //Indicates that the IPSec encryption transform set is
esp-des esp-md5-hmac.
in use settings={Tunnel Encaps,}         //Indicates that the tunnel mode is used.
              crypto map mymap 5
              sa timing: remaining key lifetime (k/sec): (4606998/1324)  //Indicates that the remaining
lifetime of the SA is: 4,606,998 kilobytes/1,324 seconds.
              IV size: 8 bytes   //Indicates that the length of IV vector is 8 bytes.
Replay detection support: Y   //Indicates the anti-replay processing.
 Outbound esp sas:
spi:0x5730dd4b (1462820171)//Indicates the outbound SPI of IPSec SA. Only when the inbound SPI and
outbound SPI are both displayed, the IPSec SA negotiation is successful.
              transform: esp-des esp-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map mymap 5
              sa timing: remaining key lifetime (k/sec): (4606998/1324)
              IV size: 8 bytes
              Replay detection support: Y
```

VI. Appendix

1. How to check whether RSR50 and RSR50E have been configured with AIM-VPN encryption cards?

RSR50 and RSR50E have no embedded VPN encryption cards. IPSec is processed through processes, and therefore its performance is poor. For packets of 500pps 60Byte, 50 packets are lost and the packet loss rate is 10%. For packets of larger than 2Kpps, the packet loss rate is 100%.

If IPSec is used when there is no AIM-VPN encryption card, function failures related to IPSec may occur. For example, the CPU utilization is constantly at 100%, even though the encrypted data traffic is light. , or the ping with large packets size would fail.

An AIM-VPN card is a pluggable card with a size similar to that of a memory bank. It is inserted inside the management board.

You can use the following method to check whether the management board is configured with an AIM-VPN card:

```
RSR50#debug su
RSR50(support)#pci show
RSR50(support)#
*Jan 29 13:41:23: %7: ==================BEGIN====================
*Jan 29 13:41:23: %7: PCI Bus 0 slot 1/0: PCI device 0x166D:0x0002
*Jan 29 13:41:23: %7: PCI Bus 0 slot 6/0: PCI device 0x104C:0xAC28
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/0: PCI device 0x14D9:0x0020
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 3/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 3/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 4/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 4/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 5/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 5/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 14 slot 1/0: PCI device 0x1131:0x1561
*Jan 29 13:41:23: %7: PCI Bus 14 slot 1/1: PCI device 0x1131:0x1562
*Jan 29 13:41:23: %7: ==================_^_====================
As long as 0x0020 is displayed, the management board has the AIM-VPN card.
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/0: PCI device 0x14D9:0x0020
```

Notes:

If the logging function is disabled (), the output information of the **pci show** command is empty. If you log in to the device through the VTY line, the corresponding information will be output only when the terminal monitor is enabled.

4.4.3.6 IPSEC Dynamic Tunnel Based on Digital Certificate

Features

A dynamic IPSec tunnel is generally used in a topology with multiple branches. The dynamic tunnel is configured at the central point to receive IPSec VPN dial-in information from the branches. The central point is easy for configuration and maintenance, and has high expansibility.

When the pre-shared key is used for authentication, the key is easily leaked. If digital certificates are used for authentication, the security of identity authentication can be effectively guaranteed.

Scenario

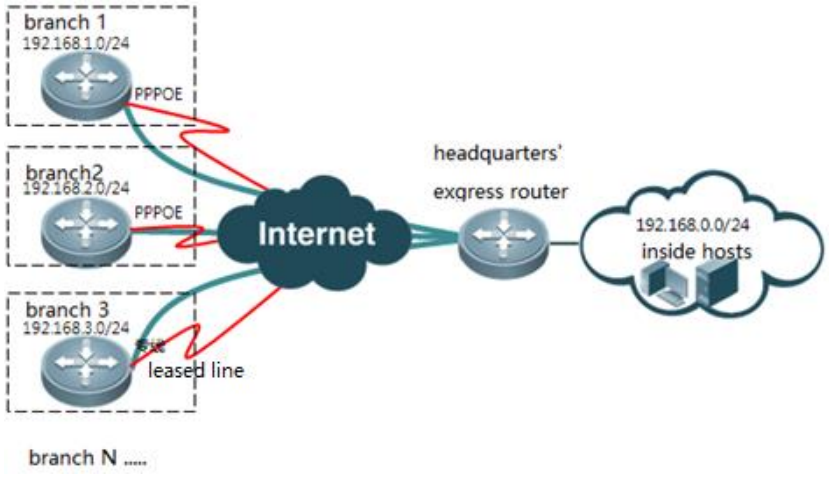
The headquarters of a company and its branches need to mutually share data through their intranets and hope that the data will not be easily intercepted or cracked by hackers during transmission. The branches are connected to the Internet through ADSL in the dial-up mode (that is, the IP addresses accessing the Internet are not permanent). The headquarters and the branches use a digital certificate to verify validity of each other. For this purpose, you can deploy a dynamic IPSec VPN based on the digital certificate on the network devices in the headquarters, and deploy a static IPSec VPN based on the digital certificate on the network devices in the branches.

I.Networking Requirements

Due to business development, a company sets up multiple branches all over the country. The egress router in the headquarters is connected to the Internet through a dedicated line of a telecom operator, while the branches are connected to the Internet through a dedicated line or ADSL. The branches need to access the business server in the headquarters, and communication data between the branches and the headquarters needs to be encrypted to ensure business security.

A dynamic IPSec VPN can be deployed on the egress router in the headquarters to receive dial-in information from the branches, so as to enable mutual business access between the headquarters and the branches, and encrypt relevant data. The branches and the headquarters use a digital certificate to verify the identity of each other.

II. Network Topology



III. Configuration

1. Configure routers in the headquarters and branches, so that the routers can access the Internet.
2. Import the digital certificate on the egress router of the headquarters and routers of the branches.

3. Configure a dynamic IPSec VPN tunnel on the egress router of the headquarters.
4. Configure the route on the router of the headquarters, and direct the traffic to the branches to the egress.
5. Configure a static IPSec VPN tunnel on the routers of the branches.
6. Configure the routes on the routers of the subsidiaries, and direct the traffic to the headquarters to the egress.

Notes:

- The IP network segments of LAN 1 and LAN 2 to be mutually accessed must not be overlapped.
- Since RSR50 and RSR50E involve the IPSec function, they must be configured with AIM-VPN encryption cards (For details about how to check whether RSR50 and RSR50E have been configured with AIM-VPN encryption cards, see the appendix at the end of this section).

IV. Configuration Steps

1. Configure routers in the headquarters and its branches, so that the routers can access the Internet.

   It must be ensured that the ping from branches to the headquarters' public IP address is successful.

2. Import the digital certificate on the egress router of the headquarters and routers of the branches

   Based on on-site environment and customer demands, select an appropriate method to import the digital certificate. For detailed operations of digital certificate import, refer to the section CA Digital Certificate Configuration (Typical Configuration--->Security--->CA Digital Certificate Configuration).

3. Configure a dynamic IPSec VPN tunnel on the egress router of the headquarters.

   (1) Configure the ISAKMP policy.

```
crypto isakmp policy 1//Creates a new ISAKMP policy.
encryption 3des        //Specifies to use 3DES for encryption.
authentication rsa-sig                //Specifies the authentication method is "digital certificate".
The default authentication method is digital certificate.
```

   (2) Configure the IPSec transform set.

```
crypto ipsec transform-set myset esp-des esp-md5-hmac//Specifies IPSec to use ESP for encapsulation,
DES for encryption and MD5 for verification.
```

   (3) Configure the dynamic IPSec encryption map.

```
crypto dynamic-map dymymap 5            //Creates a dynamic IPSec Crypto map named "dymymap".
set transform-set myset                          //Specifies the transform set to "myset".
```

   (4) Map the dynamic IPSec Crypto map to the static IPSec Crypto map.

```
crypto map mymap 10 ipsec-isakmp dynamic dymymap   //Maps the dynamic IPSec Crypto map "dymymap" to the
static IPSec Crypto map "mymap".
```

   (5) Apply the encryption map to an interface.

```
interface GigabitEthernet 0/0
    crypto map mymap
```

   (6) Disable the certificate time and validity check.

```
crypto pki trustpoint center                //Enters the corresponding trust point of the certificate.
time-check none                               //Disables the certificate time check.
revocation-check none                       //Indicates not to check whether the certificate is revoked.
```

Notes: It is recommended to disable the certificate time check and revocation list check; otherwise, the IPSec negotiation may fail.

4. Configure the route on the router of the headquarters, and direct the traffic to the branches to the egress.

```
  ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 192.168.2.0 255.255.255.0 10.0.0.2
ip route 192.168.3.0 255.255.255.0 10.0.0.2
......
```

5. Configure the static IPSec VPN tunnel on the routers of the branches(taking branch1 as an example).

(1) Configure the interesting traffic of IPSec.

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255  //Specifies the traffic with
source address 192.168.1.0/24 and destination network 192.168.0.0/24 as interesting traffic.
```

(2) Configure the ISAKMP policy.

```
crypto isakmp keepalive 5 periodic  //Configures the IPSec DPD detection function.
crypto isakmp policy 1            //Creates a new ISAKMP policy.
encryption 3des                      //Specifies to use 3DES for encryption.
authentication rsa-sig                //Specifies the authentication method is "digital certificate".
The default authentication method is digital certificate.
```

(3) Configure the IPSec encryption transform set.

```
crypto ipsec transform-set myset  esp-des esp-md5-hmac //Specifies IPSec to use ESP for encapsulation,
DES for encryption and MD5 for verification.
```

(4) Configure the IPSec encryption map.

```
crypto map mymap 5 ipsec-isakmp //Creates an crypto map named "mymap".
set peer 10.0.0.2                              //Specifies the peer address.
set transform-set myset                 //Specifies the transform set to "myset".
interesting traffic 101                        //Specifies ACL 101 as the interesting traffic.
```

(5) Apply the crypto map to an interface.

```
interface dialer 0
    crypto map mymap
```

(6) Disable the certificate time and validity check.

```
crypto pki trustpoint center                //Enters the corresponding trustpoint of the certificate.
time-check none                               //Disables the certificate time check.
revocation-check none                       //Indicates not to check whether the certificate is revoked.
```

Notes: It is recommended to disable the certificate time check and revocation list check; otherwise, the IPSec negotiation may fail.

6. Configure the routes on the routers of the branches, and direct the traffic to the headquarters to the egress.

```
ip route 192.168.0.0 255.255.255.0 dialer 0
```

V. Verification

1. Ping192.168.0.1 from the router of branch 1 with source IP address 192.168.1.1. The communication is normal.

```
R1#ping 192.168.0.1 source 192.168.1.1
Sending 5, 100-byte ICMP Echoes to 192.168.1.1, timeout is 2 seconds:
<press Ctrl+C to break >
.!!!!
```

2. On the router of branch1, check whether ISAKMP and IPSec SA negotiations are successful.

```
Ruijie#show crypto isakmp sa                                    //Shows the result of ISAKMP SA
negotiation.
 destination       source            state          conn-id          lifetime(second)
10.0.0.2          10.0.0.1          IKE_IDLE         0                84129                //The
ISAKMP negotiation is successful and the status is IKE_IDLE.
Ruijie#show crypto ipsec sa                                      //Shows the result of IPSec
SA negotiation.
Interface: GigabitEthernet 0/0
Crypto map tag:mymap    //Indicates the name of the crypto map applied to the interface.
local ipv4 addr 10.0.0.1                 //Indicates the IP address used during ISAKMP/IPSec
negotiation.
         media mtu 1500
         ================================
sub_map type:static, seqno:5, id=0
         local  ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))   //Indicates the source IP
address of the interesting traffic.
remote  ident (addr/mask/prot/port): (192.168.1.0/0.0.0.255/0/0))//Indicates the destination IP
address of the interesting traffic.
         PERMIT
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4  //Indicates the number of packets successfully
encapsulated, encrypted and digested.
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4     //Indicates the number of packets successfully
decapsulated, decrypted and verified. When data is encrypted through IPSec for communication, you can
see constant increasing of the preceding statistic counts when you repeatedly run the command show
crypto ipsec sa.
#send errors 0, #recv errors 0    //Indicates the number of packets that are incorrectly sent and
received. Normally, the counts do not increase.
 Inbound esp sas:
spi:0x2ecca8e (49072782)                  //Indicates the inbound SPI of IPSec SA.
```

```
                transform: esp-des esp-md5-hmac    //Indicates that the IPSec encryption transform set
is esp-des esp-md5-hmac.
in use settings={Tunnel Encaps,}          //Indicates that the tunnel mode is used.
                crypto map mymap 5
                sa timing: remaining key lifetime (k/sec): (4606998/1324)  //Indicates that the
remaining lifetime of the SA is: 4,606,998 kilobytes/1,324 seconds.
                IV size: 8 bytes   //Indicates that the length of IV vector is 8 bytes.
Replay detection support: Y   //Indicates the anti-replay processing.
 Outbound esp sas:
spi:0x5730dd4b (1462820171)   //Indicates the outbound SPI of IPSec SA. Only when the inbound SPI and
outbound SPI are both displayed, the IPSec SA negotiation is successful.
                transform: esp-des esp-md5-hmac
                in use settings={Tunnel Encaps,}
                crypto map mymap 5
                sa timing: remaining key lifetime (k/sec): (4606998/1324)
                IV size: 8 bytes
                Replay detection support: Y
```

VI. Appendix

1. How to check whether RSR50 and RSR50E have been configured with AIM-VPN encryption cards?

RSR50 and RSR50E have no embedded VPN encryption cards. IPSec is processed through processes, and therefore its performance is poor. For packets of 500pps 60Byte, 50 packets are lost and the packet loss rate is 10%. For packets of larger than 2Kpps, the packet loss rate is 100%.

If IPSec is used when there is no AIM-VPN encryption card, function failures related to IPSec may occur. For example, the CPU utilization is constantly at 100%, even though the encrypted data traffic is light. , or the ping with large packets size would fail.

An AIM-VPN card is a pluggable card with a size similar to that of a memory bank. It is inserted inside the management board.

You can use the following method to check whether the management board is configured with an AIM-VPN card:

```
RSR50#debug su
RSR50(support)#pci show
RSR50(support)#
*Jan 29 13:41:23: %7: ================BEGIN==================
*Jan 29 13:41:23: %7: PCI Bus 0 slot 1/0: PCI device 0x166D:0x0002
*Jan 29 13:41:23: %7: PCI Bus 0 slot 6/0: PCI device 0x104C:0xAC28
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/0: PCI device 0x14D9:0x0020
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 3/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 3/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 4/0: PCI device 0x14D9:0x9000
```

```
*Jan 29 13:41:23: %7: PCI Bus 1 slot 4/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 1 slot 5/0: PCI device 0x14D9:0x9000
*Jan 29 13:41:23: %7: PCI Bus 1 slot 5/1: PCI device 0x1142:0x9001
*Jan 29 13:41:23: %7: PCI Bus 14 slot 1/0: PCI device 0x1131:0x1561
*Jan 29 13:41:23: %7: PCI Bus 14 slot 1/1: PCI device 0x1131:0x1562
*Jan 29 13:41:23: %7: ================_^_==================
As long as 0x0020 is displayed, the management board has the AIM-VPN card.
*Jan 29 13:41:23: %7: PCI Bus 1 slot 2/0: PCI device 0x14D9:0x0020
```

Notes:

If the logging function is disabled (), the output information of the **pci show** command is empty. If you log in to the device through the VTY line, the corresponding information will be output only when the terminal monitor is enabled.

4.4.3.7 Extended Configuration

4.4.3.8 IPSEC DPD Configuration

Features

Dead Peer Detection (DPD) is a mechanism in the IPSec protocol that detects the liveness of peers so as to avoid interruption of data communication needing to be encrypted when the communication between two peers is interrupted or the other peer still uses IPSec to send the data encapsulation to a peer when the IPSec SA at the peer is disabled.

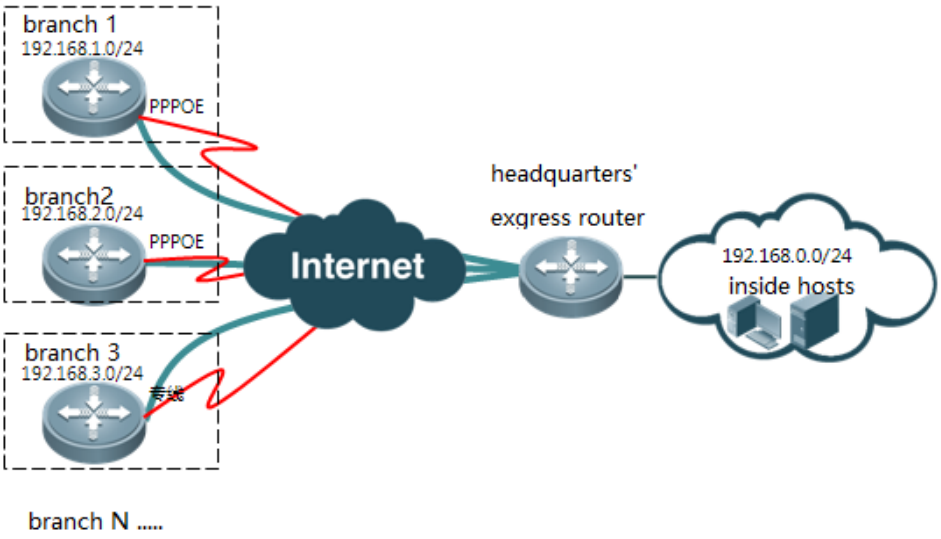
When a peer detects the other peer is dead through DPD, the local peer will clear the corresponding ISAKMP and IPSec SA. At the same time, if there is a new match address (or the Auto Up is enabled), the ISAKMP and IPSec SA negotiations are initiated again.

It does not need to configure DPD on both IPSec peers. Generally, DPD only need to be configured on the peer initiating data transmission. For example, in a headquarters-branch topology, if all the business data transmission is firstly initiated by a branch to communicate with the headquarters while the headquarters has no demand of accessing the branch, DPD only needs to be configured in the branch.

I.Networking Requirements:

DPD is configured in a branch to detect the liveness of the IPSec peers between the branch and the headquarters, so as to avoid interruption of data communication between the branch and the headquarters, which may be caused by the failure of data decryption at the headquarter—the branch sends encrypted data to the headquarters after the IPSec SA of the branch is abnormally deleted in the headquarters' router.

II. Network Topology:



III. Configuration Tips

1. Configure basic IPSec functions.
2. Configure DPD on branch1.

IV. Configuration Steps

1. Configure basic IPSec functions.

Based on field environment and customer demands, select an appropriate IPSec deployment scheme. For detailed configurations, refer to the section Basic Configuration (Typical Configuration--->Security--->IPSec--->Basic Configuration).

2. Configure DPD on branch 1.

```
crypto isakmp keepalive 10 on-demand          //Configures the DPD detection period as 10 seconds and the detection mode as on-demand.
```

Notes: DPD has two detection modes: periodical detection and on-demand detection. The on-demand detection mode is generally used.

Periodical detection: When the configured time expires, the system will actively and periodically send DPD detection messages. The maximum number of retransmission times is 5 by default.

On-demand detection: ADPD detection message is sent only when the idle time of the tunnel exceeds the configured time and a packet is sent.

V. Verification

1. Initiate a match address on the branch to the headquarters, so as to create ISAKMP SA and IPSec SA between the branch and the headquarters.
2. Disconnect the cable of the egress port of the router in the headquarters. After detecting that the peer is unreachable, the branch clears ISAKMP and IPSec SA, and initiates a negotiation again.

```
sitel#show crypto isakmp sa
destination       source            state                    conn-id          lifetime(second)
//Indicates that there is no successful ISAKMP SA negotiation.
sitel#show crypto ipsec sa
Interface: FastEthernet 0/0
        Crypto map tag:mymap
local ipv4 addr 10.0.0.2
        media mtu 1500
        ================================
        sub_map type:static, seqno:10, id=0
        local  ident (addr/mask/prot/port): (192.168.1.0/0.0.0.255/0/0))
        remote  ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))
        PERMIT
        #pkts encaps: 8, #pkts encrypt: 8, #pkts digest 0
        #pkts decaps: 8, #pkts decrypt: 8, #pkts verify 0
        #send errors 2, #recv errors 0
```

```
No sa is created now.     //Indicates that there is no successful IPSec SA negotiation.
```

4.4.3.9 IPSEC Reverse Route Injection

Features

IPSec Reverse Route Injection is generally applied in the router of the headquarters in a headquarters-branch IPSec VPN. Through this function, when the IPSec negotiation between a branch and its headquarters is successful, the router of the headquarters will automatically inject the network segment of the branch into the route table, so that the headquarters can correctly forward data to the branch.

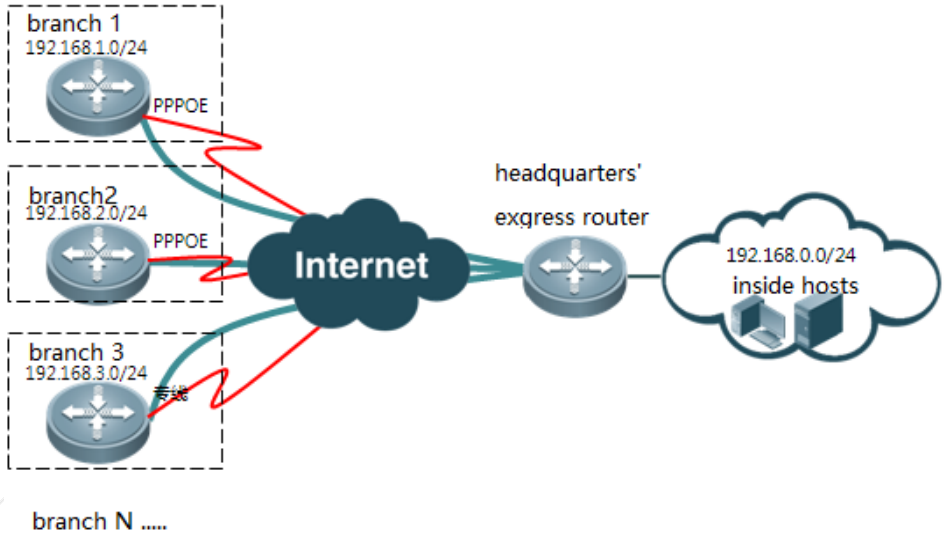
The working principle of IPSec Reverse Route Injection is that: when the IPSec negotiation between a branch and its headquarters is successful, the router of the headquarters will check the match address of the successful IPSec SA negotiation to learn about the network segment information of the branch, add the network segment information into the route table, and use the IP address of the branch as the next hop.

For example, the IPSec match address of branch1 is: branch network segment 192.168.1.0/24——>headquarters network segment 192.168.0.0/24. After successful IPSec negotiation, the IPSec match address of the headquarters router corresponding to the branch is: headquarters network segment 192.168.0.0/24——>branch network segment 192.168.1.0/24. The match address shows that the network segment of the branch needing to communicate with the headquarters is "192.168.1.0/24". At this time, the headquarters router adds the network segment 192.168.1.0/24 into the route table through Reverse Route Injection, and uses the IP address of branch1 as the next hop.

I.Networking Requirements:

Use IPSec Reverse Route Injection to dynamically inject the route information of a branch into the headquarters router, so as to enable communication between the headquarters and the branch.

II. Network Topology:



III. Configuration Tips

1. Configure basic IPSec functions.
2. Configure Reverse Route Injection on the headquarters router.
3. Re-distribute the reversely injected route to the dynamic routing protocol (optional, taking OSPF as an example).

IV. Configuration Steps

1. Configure basic IPSec functions.

Based on on-site environment and customer demands, select an appropriate IPSec deployment scheme. For detailed configurations, refer to the section Basic Configuration (Typical Configuration--->Security--->IPSec--->Basic Configuration).

2. Configure Reverse Route Injection on the headquarters router.

```
crypto dynamic-map dymymap 5
reverse-route                                    //Configures Reverse Route Injection.
```

Notes:

- Similar to a static route, the injected route thereby has an administrative distance of 1 and a weight of xxx by default. The expansion parameter can be used to modify the administrative distance and metric value of the injected route, or mark the injected route.
- The remote-peer parameter can only be used to perform reverse route injection for a specific peer.
- The route injected thereby can be associated with BFD or TRACK.

```
Ruijie(config-crypto-map)#reverse-route ?
<1-255>      Distance
```

```
  bfd           Configure bfd
  remote-peer   Match address of packets to encrypt
  tag           Set tag for this route
  track         Install route depending on tracked item
  weight        Route weight
<cr>
```

3. Re-distribute the reversely injected route to the dynamic routing protocol (optional, taking OSPF as an example).

```
router ospf 1
    redistribute static subnets
```

V. Verification

1. After the IPSec negotiation between branch 1 and the headquarters is successful, a route directed to branch 1 is dynamically generated in the headquarters router:

```
Ruijie(config)#show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C    10.0.0.0/24 is directly connected, GigabitEthernet 0/0
C    10.0.0.1/32 is local host.
C    192.168.0.0/24 is directly connected, Loopback 0
C    192.168.0.1/32 is local host.
S    192.168.1.0/24 [1/0] via 10.0.0.2                  //Indicates the route reversely injected by the headquarters after the IPSec VPN of branch 1 is successfully dialed. It should be noted that, if the next hop address of a static route is reached through the default route, because the default route is not recursive, Reverse Route Injection may fail.
```

2. After the corresponding IPSec SA is cleared on branch1, the corresponding route entry disappears from the headquarters router:

```
center#show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
   O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
```

```
C    10.0.0.0/24 is directly connected, GigabitEthernet 0/0
C    10.0.0.1/32 is local host.
C    192.168.0.0/24 is directly connected, Loopback 0
C    192.168.0.1/32 is local host.
```

4.4.3.10 IPSEC Multi-Peer Mutual Backup

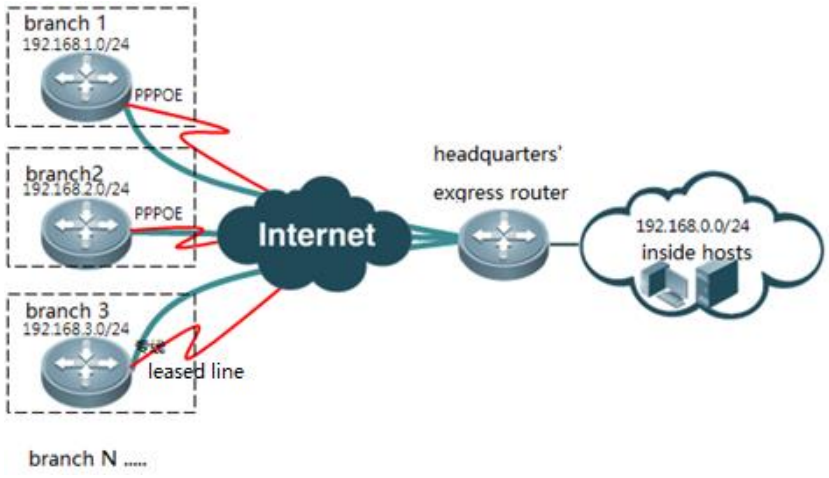
Features

The IPSec multi-peer mutual backup function enables the router to automatically switch to the backup peer (multiple backup peers can be configured) for IPSec VPN negotiation when the IPSec VPN negotiation with the master peer is failed, so as to realize redundant backup of an IPSec VPN.

I.Networking Requirements:

The headquarters router is connected to the Internet through two egresses: one is China Telecom and the other is China Unicom. When the line of China Telecom is interrupted, a branch can establish an IPSec VPN with the headquarters router through the line of Chine Unicom, so as to ensure normal communication between the branch and the headquarters.

II. Network Topology:



III. Configuration:

1. Configure basic IPSec functions.
2. Configure the IPSec multi-peer mutual backup function on the branch router.
3. Configure IPSec DPD on the branch router.

IV. Configuration Steps

1. Configure basic IPSec functions.

   Based on site environment and customer demands, select an appropriate IPSec deployment scheme. For detailed configurations, refer to the section "Basic Configuration" (Typical Configuration--->Security--->IPSec--->Basic Configuration).

   (1) Apply the IPSec encryption map to the two egresses of the headquarters router.

```
interface GigabitEthernet 0/0
crypto map mymap                        //Applies the crypto map to the egress of China Telecom.
interface GigabitEthernet 0/1
crypto map mymap                        //Applies the crypto map to the egress of China Unicom.
```

   (2) If the pre-shared key is used for authentication, specify the pre-shared keys for the corresponding IP addresses of the two egresses on the branch router.

```
crypto isakmp key 0 ruijie address x.x.x.x
crypto isakmp key 0 ruijie address y.y.y.y   //Specifies the pre-shared keys corresponding to the IP address of Chine Telecom and the IP address of Chine Unicom, respectively.
```

2. Configure the IPSec multi-peer mutual backup function on the branch router.

```
crypto map mymap 5 ipsec-isakmp
set peer x.x.x.x                          //Specifies the public IP address of China Telecom as the master peer.
set peer y.y.y.y                          //Specifies the public IP address of China Unicom as the backup peer.
```

3. Configure IPSec DPD on the branch router.

   For the configuration method of IPSec DPD, refer to the section "IPSec DPD Configuration" (Typical Configuration->Security--->IPSec--->Extension Configuration --->IPSEC DPD Configuration).

   Notes:

   To use the IPSec multi-peer mutual backup function, you need to enable IPSec DPD on the branch router, so that the branch router can detect the peer faults and automatically switch to the backup peer.

V. Verification

1. Initiate a data connection on the branch router to access the headquarters so as to create an IPSec VPN.

```
It can be seen that, an IPSec VPN is successfully created between the branch and the headquarters using the public IP address of China Telecom.
Ruijie#show crypto isakmp sa
 destination       source            state                    conn-id          lifetime(second)
x.x.x.x    10.0.0.1IKE_IDLE                0                84129           //x.x.x.x is the public IP address of China Telecom.
```

2. Disconnect the egress cable of China Telecom on the headquarters router, and continue to initiate a data connection on the branch router to access the headquarters.

```
It can be seen that, an IPSec VPN is successfully created between the branch and the headquarters
using the public IP address of China Unicom.
Ruijie#show crypto isakmp sa
 destination       source            state                  conn-id          lifetime(second)
y.y.y.y    10.0.0.1IKE_IDLE                0                84129          //y.y.y.y is the public
IP address of China Unicom.
```

4.4.3.11 IPSEC Automatic Tunnel Connection (autoup)

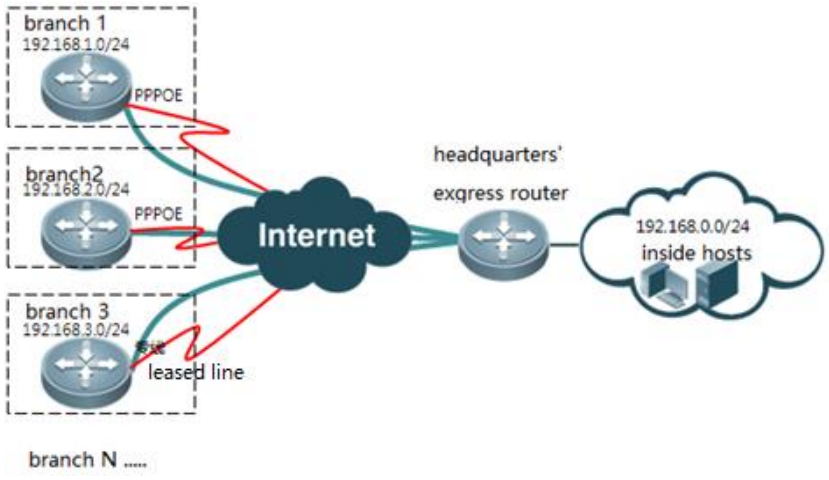
Features

Generally, an IPSec tunnel is created through negotiation after data streams are triggered. When automatic tunnel connection (autoup) is enabled, the tunnel is automatically triggered inside the IPSec module, which means that, as long as IPSec is configured, no matter whether data streams are triggered, the device will automatically initiate an IPSec negotiation.

I.Networking Requirements:

The branch and the headquarters need to use a dynamic IPSec VPN to encrypt business data exchanged mutually. Because the headquarters needs to access the application server of branch 1 from time to time, no matter whether branch 1 needs to access the headquarters or not, the IPSec VPN between branch 1 and the headquarters needs to be enabled permanently.

II. Network Topology:



III. Configuration:

1. Configure basic IPSec functions.

2. Enable IPSec automatic tunnel connection on branch 1.

IV. Steps

1. Configure basic IPSec functions.

   Based on site environment and customer demands, select an appropriate IPSec deployment scheme. For detailed configurations, refer to the section "Basic Configuration" (Typical Configuration--->Security--->IPSec--->Basic Configuration).

2. Enable IPSec automatic tunnel connection on branch 1.

```
R1(config)#crypto map mymap 10 ipsec-isakmp
R1(config-crypto-map)#set autoup                                    //Enables IPSec automatic tunnel
connection.
```

Notes: The "set autoup" command is ineffective under a dynamic map.

V. Verification

When IPSec automatic tunnel connection is enabled on the router of branch 1, no matter whether branch 1 triggers data streams to access the headquarters, an IPSec tunnel will be created through automatic negotiation.

```
Ruijie#show crypto isakmp sa                                    //Shows the result of ISAKMP SA
negotiation.
 destination       source        state             conn-id        lifetime(second)
10.0.0.2          10.0.0.1       IKE_IDLE          0               84129               //The ISAKMP
negotiation is successful and the status is IKE_IDLE.
Ruijie#show crypto ipsec sa                                         //Shows the result of IPSec
SA negotiation.
Interface: GigabitEthernet 0/0
Crypto map tag:mymap    //Indicates the name of the encryption map applied to the interface.
local ipv4 addr 10.0.0.1                //Indicates the IP address used during ISAKMP/IPSec
negotiation.
         media mtu 1500
         ================================
         sub_map type:static, seqno:5, id=0
         local  ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))    //Indicates the source
IP addresses of the interesting traffic.
remote  ident (addr/mask/prot/port): (192.168.1.0/0.0.0.255/0/0))//Indicates the destination IP
addresses of the interesting traffic.
         PERMIT
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4//Indicates the number of packets successfully
encapsulated, encrypted and digested.
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4//Indicates the number of packets successfully
decapsulated, decrypted and verified. When data is encrypted through IPSec for communication, you can
```

```
see constant increasing of the preceding statistic counts when you repeatedly run the command show
crypto ipsec sa.
#send errors 0, #recv errors 0//Indicates the number of packets that are incorrectly sent and
received. Normally, the counts do not increase.
 Inbound esp sas:
spi:0x2ecca8e (49072782)                    //Indicates the inbound SPI of IPSec SA.
               transform: esp-des esp-md5-hmac    //Indicates that the IPSec transform set is esp-des
esp-md5-hmac.
in use settings={Tunnel Encaps,}          //Indicates that the tunnel mode is used.
               crypto map mymap 5
               sa timing: remaining key lifetime (k/sec): (4606998/1324)  //Indicates that the
remaining lifetime of the SA is: 4,606,998 kilobytes/1,324 seconds.
               IV size: 8 bytes   //Indicates that the length of IV vector is 8 bytes.
Replay detection support: Y   //Indicates the anti-replay processing
 Outbound esp sas:
spi:0x5730dd4b (1462820171)//Indicates the outbound SPI of IPSec SA. When the inbound SPI and
outbound SPI are displayed, it indicates that the IPSec SA negotiation is successful.
               transform: esp-des esp-md5-hmac
            in use settings={Tunnel Encaps,}
               crypto map mymap 5
               sa timing: remaining key lifetime (k/sec): (4606998/1324)
               IV size: 8 bytes
               Replay detection support: Y
```

4.4.4 GRE

Features

Generic Routing Encapsulation (GRE) is a protocol used to encapsulate data packets of certain network layer protocols (for example, IP and IPX), so that the encapsulated data packets can be transmitted in another network layer protocol (for example, IP).GRE uses the tunnel technology, and is a Layer 3 tunnel protocol for Virtual Private Networks (VPNs).

A tunnel is a virtual point-to-point connection. It provides a channel so that encapsulated data packets can be transmitted over the channel, and data packets can be encapsulated and decapsulated at two ends of the tunnel respectively.

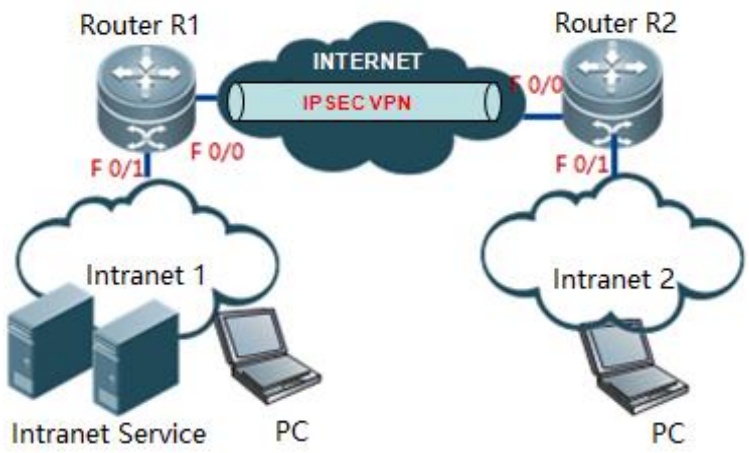
Scenario

When the headquarters of a company and its branches need to mutually share information through their inside networks and the data security is not highly emphasized, a GRE VPN can be employed on the network devices of the headquarters and branches to enable the headquarters and branches to mutual access resources of each other.

I.Networking Requirements

The two LANs access the Internet through the egress routers respectively. Besides, the two egress routers use a GRE tunnel to enable users of the two LANs to mutually access each other.

II. Network Topology



III. Configuration Tips

1. Configure routers R1 and R2 so that R1 and R2 can access the Internet and can be successfully pinged by each other.
2. Configure a GRE tunnel on R1.
3. Configure a route on R1 to direct the network segment route of LAN 2 to the GRE tunnel.
4. Configure a GRE tunnel on R2.
5. Configure a route on R2 to direct the traffic to LAN 1 to the GRE tunnel.

Notes: The IP network segments of LAN 1 and LAN 2 to be mutually accessed must not be overlapped.

IV. Configuration Steps

1. Configure routers R1 and R2 so that R1 and R2 can access the Internet and can be successfully pinged by each other.

   R1:

```
interface Fastethernet 0/0
ip ref
ip address 222.100.100.1 255.255.255.252
ip route 0.0.0.0 0.0.0.0 222.100.100.2
```

R2:

```
interface Fastethernet 0/0
ip ref
ip address 222.200.200.1 255.255.255.252
ip route 0.0.0.0 0.0.0.0 222.200.200.2
```

2. Configure a GRE tunnel on R1.

```
Ruijie>enable                          //Enters the privileged mode.
Ruijie#configure terminal               //Enters the global configuration mode.
Ruijie(config)#interface tunnel 1
Ruijie(config-if-Tunnel 1)# ip address 172.16.100.1 255.255.255.0    //Configures the IP address of the GRE tunnel.
Ruijie(config-if-Tunnel 1)#tunnel source 222.100.100.1              //Configures the source IP address of the GRE tunnel (the IP address of the outbound interface of R1).
Ruijie(config-if-Tunnel 1)#tunnel source 222.100.100.1              //Configures the destination IP address of the GRE tunnel (the IP address of the outbound interface of R2).
Ruijie(config-if-Tunnel 1)#exit
```

3. Configure a route on R1 to direct the network segment route of LAN 2 to the GRE tunnel.

```
Ruijie(config)#ip route 192.168.2.0 255.255.255.0 Tunnel 1 172.16.100.2
//Accesses 192.168.2.0/24, and sends the packet through tunnel 1 to 172.16.100.2 (IP address of the peer GRE tunnel).
```

4. Configure a GRE tunnel on R2.

```
Ruijie>enable                          //Enters the privileged mode.
Ruijie#configure terminal               //Enters the global configuration mode.
Ruijie(config)#interface tunnel 1
Ruijie(config-if-Tunnel 1)# ip address 172.16.100.2 255.255.255.0    //Configures the IP address of the GRE tunnel.
Ruijie(config-if-Tunnel 1)#tunnel source 222.200.200.1              //Configures the source IP address of the GRE tunnel (the IP address of the outbound interface of R2).
Ruijie(config-if-Tunnel 1)#tunnel source 222.100.100.1              //Configures the destination IP address of the GRE tunnel (the IP address of the outbound interface of R1).
```

6. Configure a route on R2 to direct the network segment route of LAN 1 to the GRE tunnel.

```
Ruijie(config)#ip route 192.168.1.0 255.255.255.0 Tunnel 1 172.16.100.1   //Accesses 192.168.1.0/24, and sends the packet from tunnel 1 to 172.16.100.1 (the IP address of the peer VPN tunnel).
```

V. Verification

1. Ping the address of LAN 2 on a PC of LAN 1.

```
C:\Users\Administrator>ping 192.168.2.1
```

```
Pinging 32-byte data in 192.168.2.1:
Reply from 192.168.2.1:byte=32 time=2ms TTL=248
Reply from 192.168.2.1:byte=32 time=1ms TTL=248
Reply from 192.168.2.1:byte=32 time=1ms TTL=248
Reply from 192.168.2.1:byte=32 time=2ms TTL=248

Ping statistics information of 192.168.2.1:
Data packet:sent = 4, received = 4, lost = 0 (0% lost),
Estimated round-trip time (in milliseconds):
Shortest = 1ms, longest = 2ms, average = 1ms
```

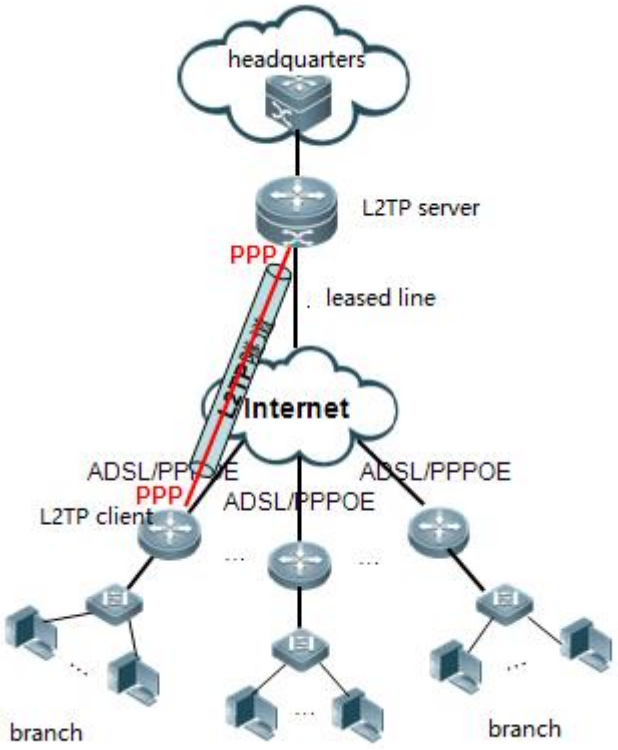
2. Show the GRE tunnel status on the router.

```
Ruijie#show interfaces tunnel 1
Index(dec):11 (hex):b
Tunnel 1 is UP, line protocol is UP
Hardware is Tunnel
Interface address is: 172.16.100.2/24
  MTU 1480 bytes, BW 9 Kbit
  Encapsulation protocol is Tunnel, loopback not set
Keepalive interval is no set
  Carrier delay is 0 sec
  RXload is 1 ,Txload is 1
  Tunnel source 222.200.200.1 (FastEthernet 0/0), destination 222.100.100.1
  Tunnel TTL 255
  Tunnel protocol/transport IPIP
  Queueing strategy: FIFO
  Output queue 0/40, 0 drops;
   Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
5 packets input, 500 bytes, 0 no buffer, 0 dropped         //Indicates that there are data packets
inputted from the GRE tunnel.
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
5 packets input, 600 bytes, 0 no buffer, 0 dropped         //Indicates that there are data packets
outputted from the GRE tunnel.
0 output errors, 0 collisions, 0 interface resets
```

4.4.5 L2TP VPN

Features

In the voluntary tunnel mode: A remote access client runs the L2TP software and functions as an LAC in the L2TP connection model. The remote client/LAC (called as "LAC customer" in RFC 2661) is connected to LNS, and PPP frames are directly forwarded through the L2TP tunnel between the customer and LNS. It is generally used for mutual connection between the headquarters and branches of a company.



Scenarios

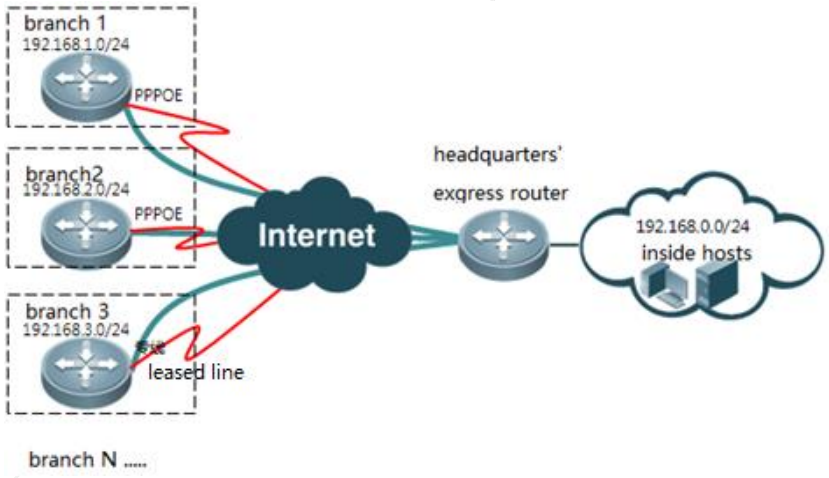
The headquarters of a company and its branches need to mutually share data through their inside networks, the data security is not highly emphasized, and the headquarters uses local user names and passwords to verify routers of branches. For this purpose, you can forcibly enable L2TP VPN on the network devices of the headquarters and branches and configure the PPP authentication mode as local authentication.

I.Networking Requirements

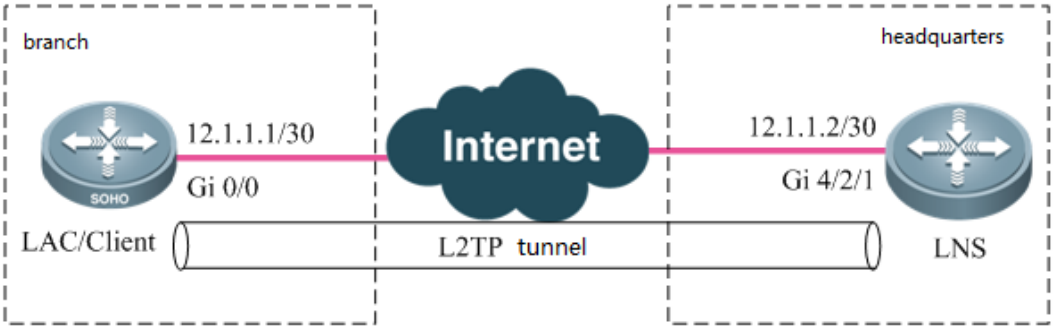
Due to business development, a company creates multiple branches all over the country. The egress router of the headquarters is connected to the Internet through a dedicated line of a Telecom operator, while the branches are connected to the Internet through a dedicated line or ADSL. The branches need to access the business server in the headquarters, and communication data between the branches and the headquarters needs to be encrypted to ensure business security.

For this purpose, you can create an L2TP VPN between egress routers of the headquarters and the branches, so as to realize mutual access between them.

II. Network Topology



Simulated topology:



III. Configuration Tips

The major difference between configurations of L2TP VPN 2.0 and 1.0 lies in the configuration of LNS: 1. A virtual-vpdn 2.0 interface must be created firstly; 2. The vpdn-group of LNS must be specified as source-ip 3, and the virtual-vpdn interface must be configured with a static IP address; 4. A new command must be used to configure and call the address pool. Notes: The virtual-vpdn interface automatically adjusts MSS (the length of header encapsulated by LETP is deducted). However, when the interface is used together with other VPNs, the MSS must be modified manually.

The configuration steps are as follows:

1. Configure LNS VPDN.
2. Configure the LNS address pool and user information.
3. Configure the LNS virtual-vpdn interface.

4. Configure the PPP dial-up of the branch router.
5. Configure the L2TP Class of the branch router.
6. Configure the L2TP pseudowire-class interface of the branch router.
7. Configure the Virtual-ppp interface of the branch router.

IV. Configuration Steps

1. Configure LNS VPDN.

```
vpdn enable
interface virtual-vpdn 1    //Creates a virtual-vpdn interface first. The interface must be created in advance.
vpdn-group 1
    accept-dialin
source-ip 12.1.1.2    //It must be configured. The IP address is the destination address of the LAC dial-in request packet, and is generally the egress address of the dedicated line.
        protocol l2tp
virtual-vpdn 1         //It requires that the protocol is set to L2TP; otherwise, this command is not displayed during configuration.
l2tp tunnel authentication                    //Enables L2TP tunnel authentication based on demands.
l2tp tunnel password ruijie                   //Configures the L2TP tunnel authentication password as "ruijie" based on demands.
```

Notes:

(1) After enabling tunnel authentication and configuring the password on LNS, you must enable tunnel authentication and configure the same password on the L2TP client; otherwise, L2TP negotiation will fail.

(2) If the destination IP address of the LAC dial-in request packet is the loopback address of LNS, the **source-ip** command is ineffective and must be replaced with the **bind slot-id** command. The "slot-id" indicates the card slot number of the dedicated line egress. The command is supported in the 10.4(3b31)p1 version or latter versions.

2. Configure the LNS address pool and user information.

```
vpdn pool test 100.1.1.1 100.1.1.100     //Configures the address pool of the L2TP user. The command used is different from the one used for configuring L2TP.
username test password test            //Adds the account and password information of the L2TP client needing local authentication.
```

3. Configure the LNS virtual-vpdn interface.

```
interface Virtual-vpdn 1
 ppp authentication chap
ip address 10.1.1.1 255.255.255.0 //The virtual-vpdn interface must be configured with a static IP address.
vpdn intf_pool test              //Calls the address pool configured for VPDN on the interface. The command used is different from the one used for configuring L2TP.
```

```
======Configurations of the branch router (client/LAC) remain the same, and are exactly the same as the configurations of the client of L2TP VPN 1.0 in the voluntary tunnel mode.=======
```

4. Configure the PPP dial-up of the branch router.

   You need to ensure that the branch router has been correctly connected to the Internet and can communicate with LNS.

   In case of ADSL dial-up, refer to "Typical Configuration"--->"WAN interface Configuration"--->"ADSL Dial-up".

5. Configure the L2TP Class of the branch router.

```
l2tp-class l2x
hostname site1            //It is optional.
authentication            //Enables L2TP tunnel authentication.
password ruijie           //Configures the L2TP tunnel authentication password as "ruijie".
```

Notes: The tunnel authentication password configured on the L2TP client must be the same with that on LNS; otherwise, L2TP negotiation will fail.

7. Configure the L2TP pseudowire-class interface of the branch router.

```
pseudowire-class pw
encapsulation l2tpv2        //Specifies to use L2TP V2 for encapsulation.
protocol l2tpv2 l2x           //Specifies L2TP V3 as the tunnel protocol and "l2x" as the L2TP class.
ip local interface gi 0/0    //Specifies the source IP address for L2TP tunnel negotiation. The address is the address of the extranet port.
```

8. Configure the Virtual-ppp interface of the branch router.

```
interface Virtual-ppp 1
    ip ref
ppp chap hostname test                //Configures the hostname of the CHAP test
ppp chap password test                //Configures the password of CHAP test
ip address negotiate                      //Configures the IP address to be automatically allocated.
pseudowire 12.1.1.2 1 pw-class pw    //Specifies the LNS address, and specifies to use pseudowire-class of "pw".
```

V. Verification

1. Show the status information of L2TP client.

   (1) After configuration, the branch router automatically initiates L2TP dial-up. If the dial-up is successfully, run the show ip interface brief command on the branch router, and the result shows that the status of the interface is "UP" and the correct IP address is obtained.

```
50#sh ip int b
Interface                      IP-Address(Pri)      OK?       Status
GigabitEthernet 0/0            12.1.1.1/24          YES       UP
GigabitEthernet 0/1            no address           YES       DOWN
GigabitEthernet 0/2            no address           YES       DOWN
GigabitEthernet 0/3            no address           YES       DOWN
Virtual-ppp 1                  100.1.1.1/32         YES       UP
50#
```

(2) In the route table, already generated is a host route of the virtual-vpdn interface address of LNS that is directly connected to the virtual-ppp interface.

```
50#sh ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.1.1/32 is directly connected, Virtual-ppp 1
C    12.1.1.0/24 is directly connected, GigabitEthernet 0/0
C    12.1.1.1/32 is local host.
C    100.1.1.1/32 is local host.
50#
```

(3)The L2TP client can be pinged to the virtual-vpdn interface address of LNS.

```
50#ping 10.1.1.1
Sending 5, 100-byte ICMP Echoes to 10.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
50#
50#
```

2. Show the status information on LNS.

   (1) Run the show vpdn command on LNS to show the user information successfully dialed in:

```
77#show vpdn

VPDN ID : 1. DEVID 1. SessionLimit 10240,Server SessionCnt 2

L2TP Tunnel and Session Information Total tunnels 2 sessions 2

LocID RemID Remote Name          State  Remote Address  Port  Sessions L2TP Class/
                                                                VPDN Group

57378 4     50                   est    12.1.1.1        1701  1        1
57379 1     3044                 est    12.1.1.3        1701  1        1

LocID       RemID       TunID       Username, Intf/      State    Last Chg
                                    Vcid, Circuit
3           1           57378       test,vpdn1           est      00:31:29
4           1           57379       test1,vpdn1          est      00:12:50

%No active PPTP tunnels
```

Two users have been dialed in.

(2) Show the corresponding vpdn interface on LNS.

```
77#show ip int b | inc up
GigabitEthernet 4/2/1          12.1.1.2/24         no address          up                  up
Virtual-vpdn 1                 10.1.1.1/24         no address          up                  up
Mgmt 0                         no address          no address          up                  down
77#
```

Only one virtual-vpdn interface is generated.

(3) Confirm the route table of a corresponding client.

```
77#sh ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C     10.1.1.0/24 is directly connected, Virtual-vpdn 1
C     10.1.1.1/32 is local host.
C     12.1.1.0/24 is directly connected, GigabitEthernet 4/2/1
C     12.1.1.2/32 is local host.
C     100.1.1.1/32 is directly connected, Virtual-vpdn 1
C     100.1.1.2/32 is directly connected, Virtual-vpdn 1
```

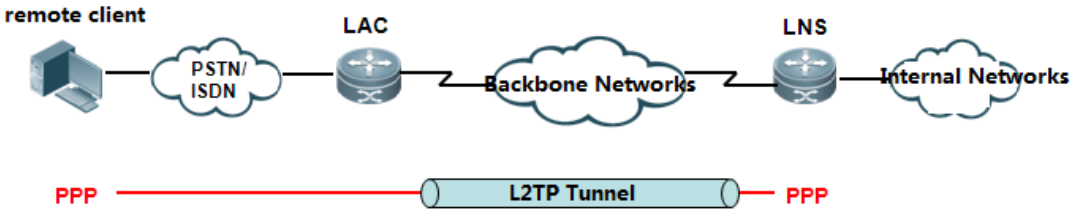
The host routes of two dialed-in clients are generated.

4.4.6 VPDN 2.0

L2TP 2.0 Compulsory Tunnel Mode – Local User Authentication

Features

In L2TP Compulsory Tunnel Mode, the L2TP Access Concentrator (LAC) ends calls from remote access clients, and then extends PPP sessions to the L2TP Network Server (LNS) in tunnel mode via an intermediate network. In this mode, the remote access clients are not required to know L2TP and only have to dial in to the LAC via PPP. 3G solutions adopt this mode.



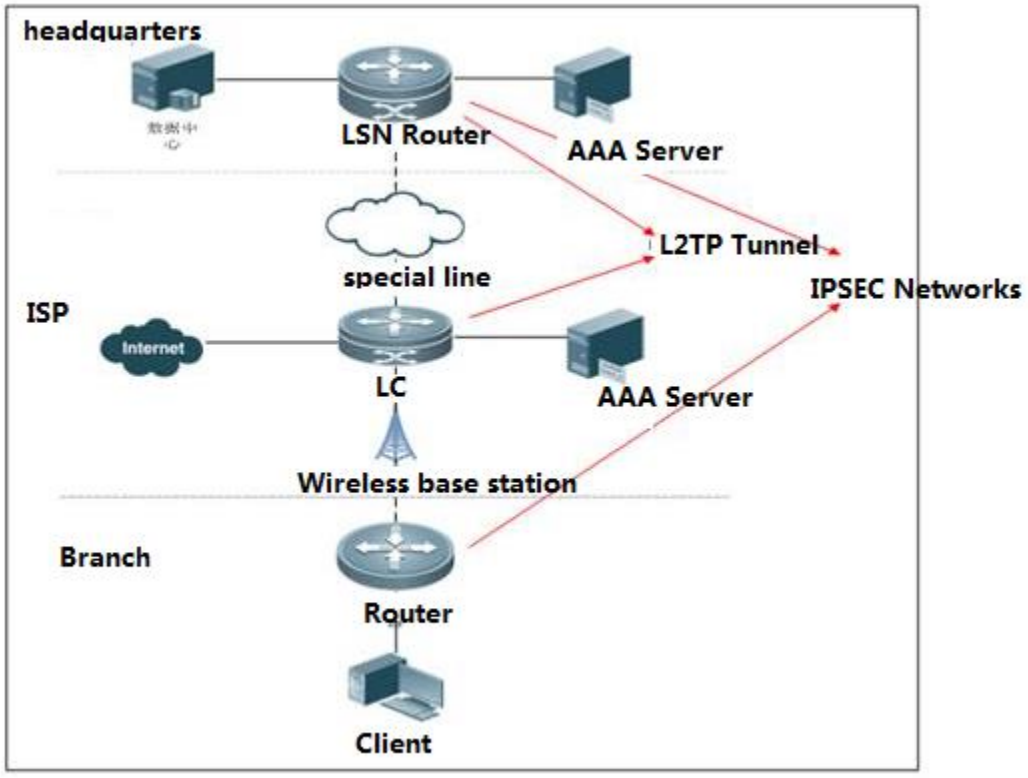
Scenario

A company rents a 3G network from an Internet service provider (ISP). Its branch routers need to dial in to the intranet of the headquarters via the 3G network. The headquarters authenticates branch routers by the local user names and passwords. For this purpose, you can set the compulsory L2TP tunnel mode between the ISP network and the headquarters intranet, and configure local authentication for PPP authentication.

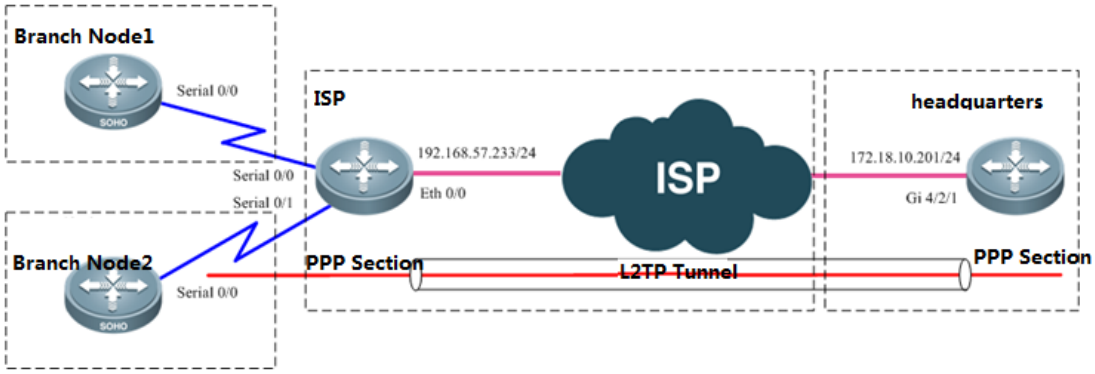
I.Networking Requirements

Take a 3G scenario for example: RSR series routers are used as the LNS and converge L2TP sessions of all clients. Perform CHAP authentication and assign IP addresses for all users on the local LNS.

II. Network Topology



Anolog Topology:



III. Configuration Tips

The major difference between configurations of L2TP VPN 2.0 and 1.0 is LNS configuration: 1. A virtual-vpdn 2.0 interface must be created first; 2. The source IP address of the VPDN-Group of the LNS must be specified; 3. The virtual-vpdn interface must be configured with a static IP address; 4. A new command must be used to configure and call the address pool. Note: The virtual-vpdn interface automatically adjusts the MSS (the length of the header encapsulated by the L2TP is deducted). However, when the interface is used together with other VPNs, the MSS must be modified manually.

Configuration Steps:

1. Configure the LNS VPDN.
2. Configure the LNS address pool and user information.
3. Configure the LNS virtual-vpdn interface.
4. Configure PPP dial-up for branch routers.

IV. Configuration Steps

1. Configure the LNS VPDN.

```
vpdn enable
interface virtual-vpdn 1   //Creates a virtual-vpdn 2.0 interface first. The interface must be created in advance.
vpdn-group 1
    accept-dialin
        source-ip 172.18.10.201    //(Mandatory) It indicates the destination address of the LAC dial-in request packet and is generally the egress address of the dedicated line.
protocol l2tp
        virtual-vpdn 1             //It requires that the protocol is set to L2TP. Otherwise, this command is not displayed during configuration.
l2tp tunnel authentication                      //Enables L2TP tunnel authentication as required.
l2tp tunnel password ruijie                //Sets the L2TP tunnel authentication password to ruijie.
```

Note:

1) After configuring tunnel authentication and password on the LNS, configure the same on the L2TP client. Otherwise, L2TP negation fails.

2) If the destination address of the LAC dial-in request packet is the loopback address of the LNS, the **source-ip** command will not take effect and must be replaced with the **bind slot-id** command. The slot-id indicates the line card slot number of the dedicated line egress. This command is supported in the 10.4 (3b31) p1 version or later versions.

2. Configure the LNS address pool and user information.

```
vpdn pool test 100.1.1.1 100.1.1.100      //Configures the address pool for the L2TP user. The
command is different from the one for configuring the L2TP.
username ruijie@ruijie.com.cn password ruijie
username test@ruijie.com.cn password test              //Adds the account and password of the L2TP
client for local authentication.
```

3. Configure the LNS virtual-vpdn interface.

```
interface Virtual-vpdn 1
 ppp authentication chap
 ip address 10.1.1.1 255.255.255.0     //The virtual-vpdn interface must be configured with a static
IP address.
vpdn intf_pool test                 //Calls the address pool configured for the VPDN on the
interface. The command is different from the one for configuring the L2TP.
```

4. Configure the LNS compatibility command. (Optional)

In the 3G scenario, after configuration, the 3G client dial-up may fail because the LNS is incompatible with the LAC. Test the following compatibility commands separately.

Run the command to enable the LNS to ignore the PPP authentication message from the LAC and force the LNS to perform another CHAP authentication on the Client.

```
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)# force-local-chap
```

Run the command to enable the LNS to ignore the PPP negotiation message from the LAC and force the LNS to renegotiate LCP with Client.

```
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)# force-local-lcp
```

Run the command to ignore errors reported by control packets.

```
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)# lcp renegotiation always
```

5. Configure PPP dial-up for remote clients.

(1) In the 3G scenario, see Typical Configuration > WAN Interface Configuration > 3G Interface Dial-up > 3G VPDN.

(2) In case of ADSL dial-up, see Typical Configuration > WAN Interface Configuration > ADSL Dial-up.

(3) Dial up through common serial ports.

```
interface Serial0/0
ip address negotiated                    //Obtain addresses from the LNS through negotiation.
encapsulation ppp
ppp chap hostname test@ruijie.com.cn
ppp chap password  test
```

V. Verification

After configuration, dial-up is triggered on the L2TP client (or 3G client). If dial-up is successful, run the **show vpdn** command to view users that have successfully dialed in on the LNS.

1. Run the show vpdn command to view tunnels established on the LNS.

```
7708#show vpdn

VPDN ID : 1. DEVID 1. SessionLimit 10240,Server SessionCnt 2

L2TP Tunnel and Session Information Total tunnels 1 sessions 2

LocID RemID Remote Name          State  Remote Address  Port  Sessions L2TP Class/
                                                                      VPDN Group

57409 10901 R2                   est    192.168.57.233  1701  2        1

LocID       RemID       TunID       Username, Intf/      State    Last Chg
                                    Vcid, Circuit
67          53          57409       test@ruijie.,vpdn1   est      00:08:35
66          52          57409       ruijie@ruiji,vpdn1   est      00:08:37

%No active PPTP tunnels
```

As shown in the above figure, one tunnel has been established and two clients has been connected to the LNS.

View information on the virtual-vpdn interface.

```
7708#sh ip int b
Interface                  IP-Address(Pri)      IP-Address(Sec)      Status               Protocol
GigabitEthernet 4/1/0      no address           no address           up                   down
GigabitEthernet 4/1/1      no address           no address           down                 down
GigabitEthernet 4/1/2      no address           no address           down                 down
GigabitEthernet 4/1/3      no address           no address           down                 down
GigabitEthernet 4/2/0      no address           no address           down                 down
GigabitEthernet 4/2/1      172.18.10.201/24     no address           up                   up
GigabitEthernet 4/2/2      no address           no address           down                 down
GigabitEthernet 4/2/3      no address           no address           down                 down
GigabitEthernet 4/2/4      no address           no address           down                 down
GigabitEthernet 4/2/5      no address           no address           down                 down
GigabitEthernet 4/2/6      no address           no address           down                 down
GigabitEthernet 4/2/7      no address           no address           down                 down
Virtual-vpdn 1             10.1.1.1/24          no address           up                   up
Mgmt 0                     no address           no address           down                 down
7708#
```

Two clients have dialed in. There is only one virtual-vpdn interface as the logical interface.

2. After the tunnel is established, view PPP negotiation result on the clients.

```
client_test#sh interfaces s0/0
Serial0/0 is up, line protocol is up
  Hardware is M4T
  Internet address is 100.1.1.2/32
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Listen: CDPCP
  Open: IPCP, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:12:17, output 00:00:00, output hang never
  Last clearing of "show interface" counters 01:09:43
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1021 packets input, 17970 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     910 packets output, 15866 bytes, 0 underruns
     0 output errors, 0 collisions, 61 interface resets
     0 output buffer failures, 0 output buffers swapped out
     61 carrier transitions     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

client_test#
```

```
client_test#sh ip int b
Interface                  IP-Address      OK? Method Status                Protocol
Serial0/0                  100.1.1.2       YES IPCP   up                    up
Serial0/1                  unassigned      YES unset  administratively down down
Serial0/2                  unassigned      YES unset  administratively down down
Serial0/3                  unassigned      YES unset  administratively down down
client_test#
```

3. The clients obtain the IP addresses through successful PPP negotiation. View host routes learned by both clients.

```
client_test#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     100.0.0.0/32 is subnetted, 1 subnets
C       100.1.1.2 is directly connected, Serial0/0
     10.0.0.0/32 is subnetted, 1 subnets
C       10.1.1.1 is directly connected, Serial0/0
client_test#
client_test#
client_test#
```

```
7708#sh ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 172.18.10.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.18.10.1
C     10.1.1.0/24 is directly connected, Virtual-vpdn 1
C     10.1.1.1/32 is local host.
C     100.1.1.1/32 is directly connected, Virtual-vpdn 1
C     100.1.1.2/32 is directly connected, Virtual-vpdn 1
C     172.18.10.0/24 is directly connected, GigabitEthernet 4/2/1
C     172.18.10.201/32 is local host.
7708#
```

4. Test network connectivity.

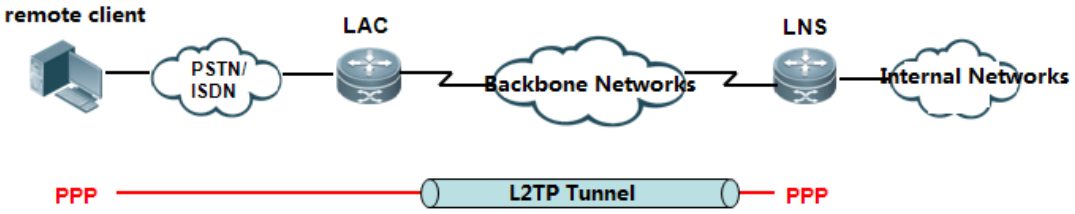
```
client_test#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/72/112 ms
client_test#
```

```
7708#ping 100.1.1.2
Sending 5, 100-byte ICMP Echoes to 100.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/92/110 ms
7708#
```

L2TP 2.0 Compulsory Tunnel Mode – AAA Authentication

Features

In L2TP Compulsory Tunnel Mode, the LAC ends calls from remote access clients, and then extends PPP sessions to the LNS in tunnel mode via an intermediate network. In this mode, the remote access clients are not required to know L2TP and only have to dial in to the LAC via PPP. 3G solutions adopt this mode.



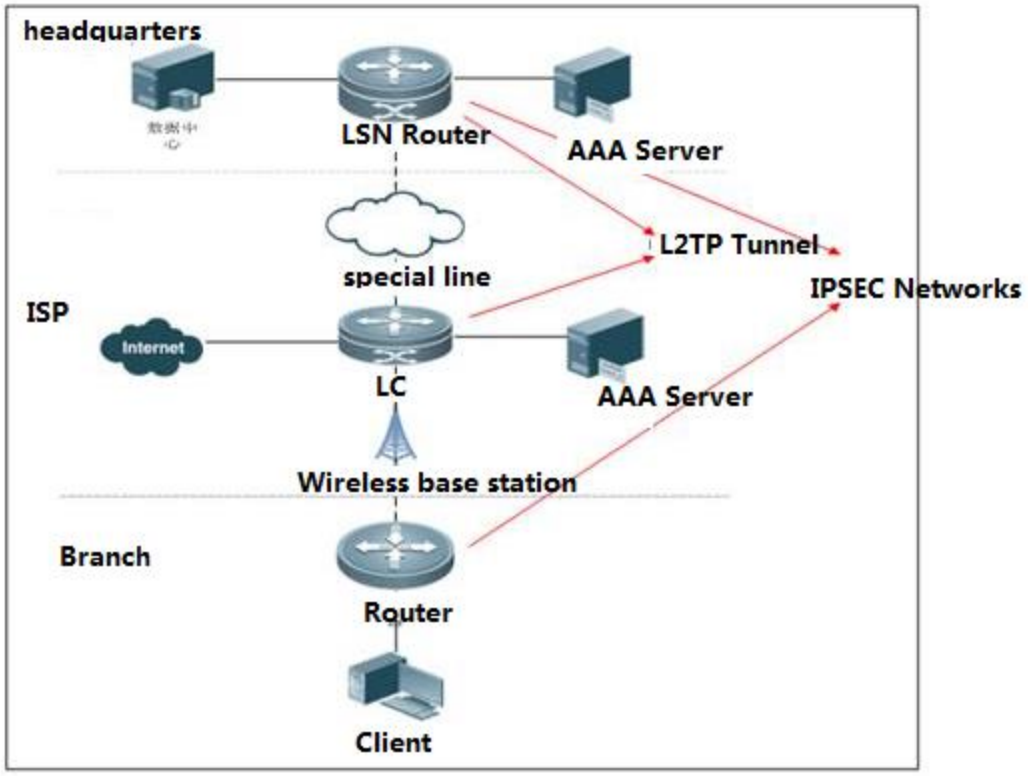
Scenario

A company rents a 3G network from an ISP. Its branch routers need to dial in to the intranet of the headquarters via the 3G network. The headquarters authenticates branch routers by AAA. For this purpose, you can set the compulsory L2TP tunnel mode between the ISP network and the headquarters intranet, and configure AAA authentication for PPP authentication.

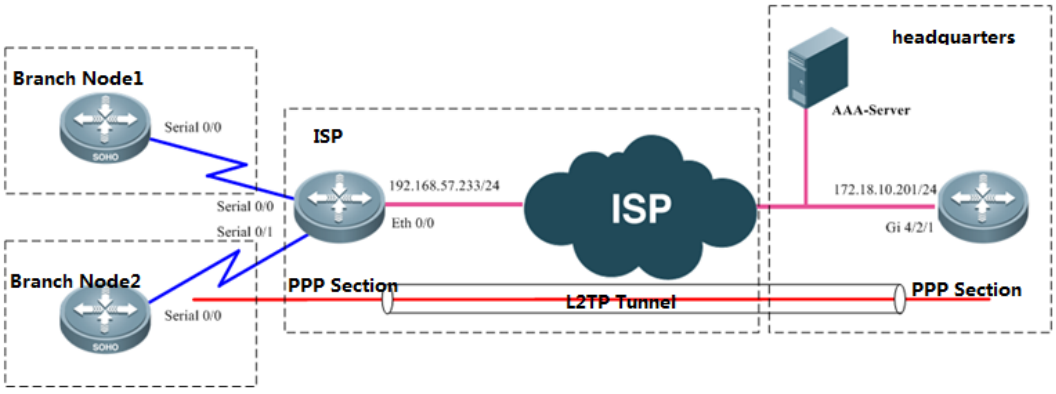
I.Networking Requirements

Take a 3G scenario for example: RSR series routers are used as the LNS and converge L2TP sessions of all clients. Perform authentication and assign IP addresses for all users on the RADIUS Server.

II. Network Topology



Anolog Topology:



III. Configuration Tips

The major difference between configurations of L2TP VPN 2.0 and 1.0 is LNS configuration: 1. A virtual-vpdn 2.0 interface must be created first; 2. The source IP address of the VPDN-Group of the LNS must be specified; 3. The virtual-vpdn interface must be configured with a static IP address; 4. A new command must be used to configure and call the address pool. Note: The virtual-vpdn interface automatically adjusts the MSS (the length of the header encapsulated by the L2TP is deducted). However, when the interface is used together with other VPNs, the MSS must be modified manually.

Configuration Steps:

1. Configure the LNS VPDN.
2. Configure the LNS address pool.
3. Configure the LNS virtual-vpdn interface.
4. Configure the LNS AAA authentication.
5. Configure the LNS AAA accounting.
6. Configure the LNS compatibility command. (Optional)
7. Configure PPP dial-up for remote clients.

IV. Configuration Steps

1. Configure the LNS VPDN.

```
vpdn enable
interface virtual-vpdn 1  //Creates a virtual-vpdn interface first. The interface must be created in advance.
vpdn-group 1
    accept-dialin
        source-ip 172.18.10.201    //(Mandatory) It indicates the destination address of the LAC dial-in request packet and is generally the egress address of the dedicated line.
protocol l2tp
virtual-vpdn 1            //It requires that the protocol is set to L2TP. Otherwise, this command is not displayed during configuration.
l2tp tunnel authentication                        //Enables L2TP tunnel authentication as required.
l2tp tunnel password ruijie          //Sets the L2TP tunnel authentication password to ruijie.
```

Note:

1) After configuring tunnel authentication and password on the LNS, configure the same on the L2TP client. Otherwise, L2TP negation fails.

2) If the destination address of the LAC dial-in request packet is the loopback address of the LNS, the **source-ip** command will not take effect and must be replaced with the **bind slot-id** command. The slot-id indicates the line card slot number of the dedicated line egress. This command is supported in the 10.4 (3b31) p1 version or later versions.

2. Configure the LNS address pool.

```
vpdn pool test 100.1.1.1 100.1.1.100              //Configures the address pool for the L2TP user. The command is different from the one for configuring the L2TP.
```

3. Configure the LNS virtual-vpdn interface.

```
interface Virtual-vpdn 1
```

```
 ppp authentication chap
 ip address 10.1.1.1 255.255.255.0   //The virtual-vpdn interface must be configured with a static IP address.
vpdn intf_pool test              //Calls the address pool configured for the VPDN on the interface. The command is different from the one for configuring the L2TP.
```

4. Configure the LNS AAA authentication.

```
aaa new-model
      radius-server host 192.168.57.222 key ruijie   //Specifies the RADIUS Server and the key.
aaa authentication ppp default group radius  //Specifies the RADIUS protocol for PPP authentication.
```

5. Configure the LNS AAA accounting.

```
aaa new-model
aaa accounting update periodic 1        //Sets the accounting update interval to 1 minute. It is 5 minutes by default and 1 minute at least.
aaa accounting update                       //Enables accounting update.
aaa accounting network default start-stop group radius  //Specifies the RADIUS protocol for start-accounting and end-accounting requests of network users.
```

Note:

Enable AAA accounting only when the RADIUS Server assigns IP addresses to users from the address pool, because the AAA address pool assigns and releases IP address using the user accounting function. If AAA assigns static IP addresses to AAA users, do not enable AAA accounting.

6. Configure the LNS compatibility command. (Optional)

In the 3G scenario, after configuration, the 3G client dial-up may fail because the LNS is incompatible with the LAC. Test the following compatibility commands separately.

Run the command to enable the LNS to ignore the PPP authentication message from the LAC and force the LNS to perform another CHAP authentication on the Client.

```
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)# force-local-chap
```

Run the command to enable the LNS to ignore the PPP negotiation message from the LAC and force the LNS to renegotiate LCP with Client.

```
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)# force-local-lcp
```

Run the command to ignore errors reported by control packets.

```
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)# lcp renegotiation always
```

7. Configure PPP dial-up for remote clients.

(1) In the 3G scenario, see Typical Configuration > WAN Interface Configuration > 3G Interface Dial-up > 3G VPDN.

(2) In case of ADSL dial-up, see Typical Configuration > WAN Interface Configuration > ADSL Dial-up.

(3) Dial up through common serial ports.

```
interface Serial0/0
ip address negotiated                          //Obtain addresses from the LNS through negotiation.
encapsulation ppp
ppp chap hostname test@ruijie.com.cn
ppp chap password  test
```

V. Verification

1. View VPDN tunnels established on the LNS.

After configuration, dial-up is triggered on the L2TP client (or 3G client). If dial-up is successful, run the **show vpdn** command to view users that have successfully dialed in on the LNS.

```
7708#show vpdn

VPDN ID : 1. DEVID 1. SessionLimit 10240,Server SessionCnt 2

L2TP Tunnel and Session Information Total tunnels 1 sessions 2

LocID RemID Remote Name          State  Remote Address  Port  Sessions L2TP Class/
                                                                      VPDN Group

57410 28941 R2                   est    192.168.57.233  1701  2        1

LocID       RemID       TunID       Username, Intf/      State    Last Chg
                                    Vcid, Circuit
69          135         57410       ruijie@ruiji,vpdn1   est      00:04:10
68          134         57410       test@ruijie.,vpdn1   est      00:04:10

%No active PPTP tunnels
```

View information on the virtual-vpdn interface.

```
7708#sh ip int b
Interface                  IP-Address(Pri)      IP-Address(Sec)      Status               Protocol
GigabitEthernet 4/1/0      no address           no address           up                   down
GigabitEthernet 4/1/1      no address           no address           down                 down
GigabitEthernet 4/1/2      no address           no address           down                 down
GigabitEthernet 4/1/3      no address           no address           down                 down
GigabitEthernet 4/2/0      no address           no address           down                 down
GigabitEthernet 4/2/1      172.18.10.201/24     no address           up                   up
GigabitEthernet 4/2/2      no address           no address           down                 down
GigabitEthernet 4/2/3      no address           no address           down                 down
GigabitEthernet 4/2/4      no address           no address           down                 down
GigabitEthernet 4/2/5      no address           no address           down                 down
GigabitEthernet 4/2/6      no address           no address           down                 down
GigabitEthernet 4/2/7      no address           no address           down                 down
Virtual-vpdn 1             10.1.1.1/24          no address           up                   up
Mgmt 0                     no address           no address           down                 down
7708#
```

Two clients dial in. There is only one virtual-vpdn interface as the logical interface.

2. After the tunnel is established, view PPP negotiation result on the client.

```
client_test#sh interfaces s0/0
Serial0/0 is up, line protocol is up
  Hardware is M4T
  Internet address is 100.1.1.2/32
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Listen: CDPCP
  Open: IPCP, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:12:17, output 00:00:00, output hang never
  Last clearing of "show interface" counters 01:09:43
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1021 packets input, 17970 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     910 packets output, 15866 bytes, 0 underruns
     0 output errors, 0 collisions, 61 interface resets
     0 output buffer failures, 0 output buffers swapped out
     61 carrier transitions     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

client_test#
```

```
client_test#sh ip int b
Interface                  IP-Address      OK? Method Status                Protocol
Serial0/0                  100.1.1.2       YES IPCP   up                    up
Serial0/1                  unassigned      YES unset  administratively down down
Serial0/2                  unassigned      YES unset  administratively down down
Serial0/3                  unassigned      YES unset  administratively down down
client_test#
```

3. The clients obtain the IP addresses through successful PPP negotiation. View host routes learned by both clients.

```
client_test#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     100.0.0.0/32 is subnetted, 1 subnets
C       100.1.1.2 is directly connected, Serial0/0
     10.0.0.0/32 is subnetted, 1 subnets
C       10.1.1.1 is directly connected, Serial0/0
client_test#
client_test#
client_test#
```

```
7708#sh ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 172.18.10.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.18.10.1
C     10.1.1.0/24 is directly connected, Virtual-vpdn 1
C     10.1.1.1/32 is local host.
C     100.1.1.1/32 is directly connected, Virtual-vpdn 1
C     100.1.1.2/32 is directly connected, Virtual-vpdn 1
C     172.18.10.0/24 is directly connected, GigabitEthernet 4/2/1
C     172.18.10.201/32 is local host.
7708#
```

4. Test network connectivity.

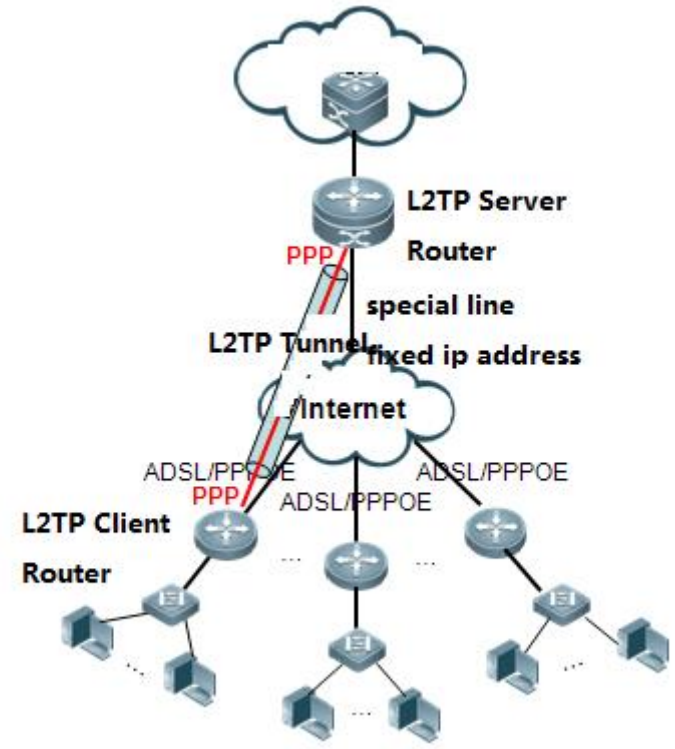
```
client_test#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/72/112 ms
client_test#
```

```
7708#ping 100.1.1.2
Sending 5, 100-byte ICMP Echoes to 100.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/92/110 ms
7708#
```

L2TP 2.0 Voluntary Tunnel Mode – Local User Authentication

Features

In voluntary tunnel mode, a remote client runs the L2TP software and functions as an LAC in the L2TP connection model. The remote client/LAC ("LAC customer" in RFC 2661) is connected to the LNS. PPP frames are directly forwarded through the L2TP tunnel between the customer and the LNS. It is generally used for mutual access between the headquarters and branches of a company.



Scenario

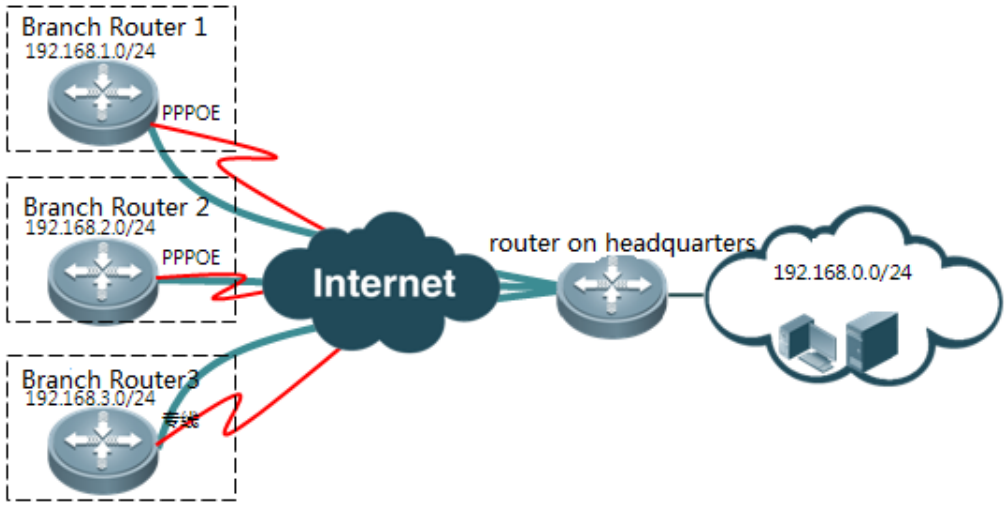
If the headquarters of a company and its branches need to share data through their intranets and the data security is not highly emphasized, the headquarters verifies branch routers by the local user names and passwords. For this purpose, you can enable L2TP VPN in compulsory mode on the network devices of the headquarters and branches, and configure local authentication for PPP authentication.

I.Networking Requirements

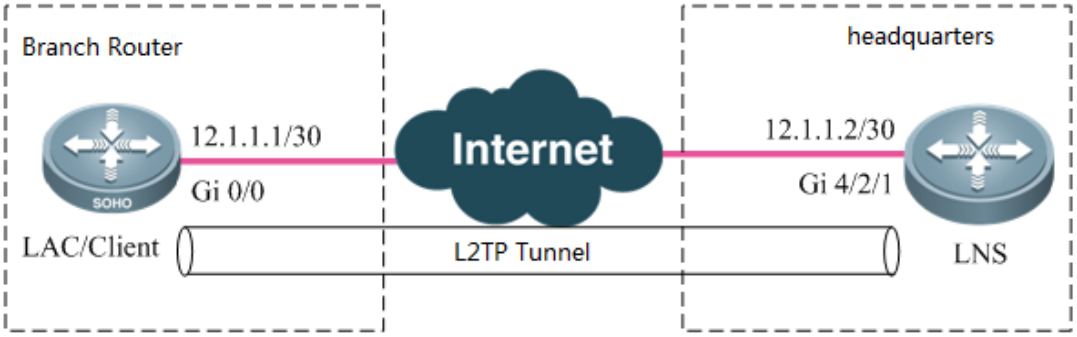
Due to business development, a company sets up multiple branches all over the country. The egress router in the headquarters is connected to the Internet through a dedicated line of an ISP, while the branches are connected to the Internet through a dedicated line or ADSL. The branches need to access the service server in the headquarters, and communication data between branches and the headquarters needs to be encrypted to ensure service security.

For this purpose, you can create an L2TP VPN between egress routers of the headquarters and the branches to realize mutual access.

II. Network Topology



Anolog Topology:



III. Configuration Tips

The major difference between configurations of L2TP VPN 2.0 and 1.0 is LNS configuration: 1. A virtual-vpdn 2.0 interface must be created first; 2. The source IP address of the VPDN-Group of the LNS must be specified; 3. The virtual-vpdn interface must be configured with a static IP address; 4. A new command must be used to configure and call the address pool. Note: The virtual-vpdn interface automatically adjusts the MSS (the length of the header encapsulated by the L2TP is deducted). However, when the interface is used together with other VPNs, the MSS must be modified manually.

Configuration Steps:

1. Configure the LNS VPDN.
2. Configure the LNS address pool and user information.
3. Configure the LNS virtual-vpdn interface.
4. Configure PPP dial-up for branch routers.

5. Configure an L2TP CLASS for branch routers.
6. Configure an L2TP pseudowire-class interface for branch routers.
7. Configure a virtual-ppp interface for branch routers.

IV. Configuration Steps

1. Configure the LNS VPDN.

```
vpdn enable
interface virtual-vpdn 1  //Creates a virtual-vpdn 2.0 interface first. The interface must be created in advance.
vpdn-group 1
    accept-dialin
        source-ip 12.1.1.2    //(Mandatory) It indicates the destination address of the LAC dial-in request packet and is generally the egress address of the dedicated line.
protocol l2tp
        virtual-vpdn 1              //It requires that the protocol is set to L2TP. Otherwise, this command is not displayed during configuration.
l2tp tunnel authentication           //Enables L2TP tunnel authentication as required.
l2tp tunnel password ruijie         //Sets the L2TP tunnel authentication password to ruijie.
```

Note:

1) After configuring tunnel authentication and password on the LNS, configure the same on the L2TP client. Otherwise, L2TP negation fails.

2) If the destination address of the LAC dial-in request packet is the loopback address of the LNS, the **source-ip** command will not take effect and must be replaced with the **bind slot-id** command. The slot-id indicates the line card slot number of the dedicated line egress. This command is supported in the 10.4 (3b31) p1 version or later versions.

2. Configure the LNS address pool and user information.

```
vpdn pool test 100.1.1.1 100.1.1.100   //Configures the address pool for the L2TP user. The command is different from the one for configuring the L2TP.
username test password test           //Adds the account and password of the L2TP client for local authentication.
```

3. Configure the LNS virtual-vpdn interface.

```
interface Virtual-vpdn 1
 ppp authentication chap
 ip address 10.1.1.1 255.255.255.0  //The virtual-vpdn interface must be configured with a static IP address.
vpdn intf_pool test              //Calls the address pool configured for the VPDN on the interface. The command is different from the one for configuring the L2TP.
```

The configuration of branch routers (client/LAC) is the same as that of L2TP VPN 1.0 clients in voluntary tunnel mode.

4. Configure PPP dial-up for branch routers.

   Ensure that branch routers have been connected to the Internet and communicate with the LNS.

   In case of ADSL dial-up, see **Typical Configuration** > **WAN Interface Configuration** > **ADSL Dial-up**.

5. Configure an L2TP CLASS for branch routers.

```
l2tp-class l2x
    hostname site1 //Optional.
authentication           //Enables L2TP tunnel authentication.
password ruijie            //Sets L2TP tunnel authentication password to ruijie.
```

Note: Configure the same tunnel authentication and password on the L2TP client as that on the LNS. Otherwise, L2TP negation fails.

6. Configure an L2TP pseudowire-class interface for branch routers.

```
pseudowire-class pw
    encapsulation l2tpv2   //Specifies L2TPv2 for encapsulation.
protocol l2tpv2 l2x   //Specifies L2TPv2 as the tunneling protocol and "l2x" as the L2TP class.
ip local interface gi 0/0       ///Specifies the source IP address for L2TP tunnel negotiation. It is
the address of the external network interface.
```

7. Configure a virtual-ppp interface for branch routers.

```
interface Virtual-ppp 1
    ip ref
    ppp chap hostname test    //Configures the user name of CHAP authentication.
ppp chap password test                          //Configures the password of CHAP authentication.
ip address negotiate                          //Configures IP addresses to be automatically assigned.
pseudowire 12.1.1.2 1 pw-class pw          //Specifies the LNS address and "pw" as the pseudowire-
class.
```

V. Verification

1. View the status on the L2TP client.

1) After configuration, the branch router automatically initiates L2TP dial-up. If dial-up is successful, run the show ip interface brief command to confirm that the interface is UP and a correct IP address has been obtained.

```
50#sh ip int b
Interface                      IP-Address(Pri)      OK?       Status
GigabitEthernet 0/0            12.1.1.1/24          YES       UP
GigabitEthernet 0/1            no address           YES       DOWN
GigabitEthernet 0/2            no address           YES       DOWN
GigabitEthernet 0/3            no address           YES       DOWN
Virtual-ppp 1                  100.1.1.1/32         YES       UP
50#
```

2) View the routing table and confirm that an IP address of the LNS virtual-vpdn interface directly connected to the virtual-ppp interface.

```
50#sh ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.1.1/32 is directly connected, Virtual-ppp 1
C    12.1.1.0/24 is directly connected, GigabitEthernet 0/0
C    12.1.1.1/32 is local host.
C    100.1.1.1/32 is local host.
50#
```

3) The L2TP client can ping the IP address of the virtual-vpdn interface of the LNS.

```
50#ping 10.1.1.1
Sending 5, 100-byte ICMP Echoes to 10.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
50#
50#
```

2. View the status on the LNS.

(1) Run the show vpdn command to view users that have dialed in.

```
77#show vpdn

VPDN ID : 1. DEVID 1. SessionLimit 10240,Server SessionCnt 2

L2TP Tunnel and Session Information Total tunnels 2 sessions 2

LocID RemID Remote Name          State  Remote Address  Port  Sessions L2TP Class/
                                                                      VPDN Group

57378 4     50                   est    12.1.1.1        1701  1        1
57379 1     3044                 est    12.1.1.3        1701  1        1

LocID      RemID      TunID      Username, Intf/      State    Last Chg
                                 Vcid, Circuit
3          1          57378      test,vpdn1           est      00:31:29
4          1          57379      test1,vpdn1          est      00:12:50

%No active PPTP tunnels
```

Two users have dialed in.

(2) View the VPDN interface generated on the LNS.

```
77#show ip int b | inc up
GigabitEthernet 4/2/1          12.1.1.2/24         no address          up                    up
Virtual-vpdn 1                 10.1.1.1/24         no address          up                    up
Mgmt 0                         no address          no address          up                    down
77#
```

Only one virtual-vpdn interface is generated.

(3) Check routing tables generated for the two clients.

```
77#sh ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.1.0/24 is directly connected, Virtual-vpdn 1
C    10.1.1.1/32 is local host.
C    12.1.1.0/24 is directly connected, GigabitEthernet 4/2/1
C    12.1.1.2/32 is local host.
C    100.1.1.1/32 is directly connected, Virtual-vpdn 1
C    100.1.1.2/32 is directly connected, Virtual-vpdn 1
```

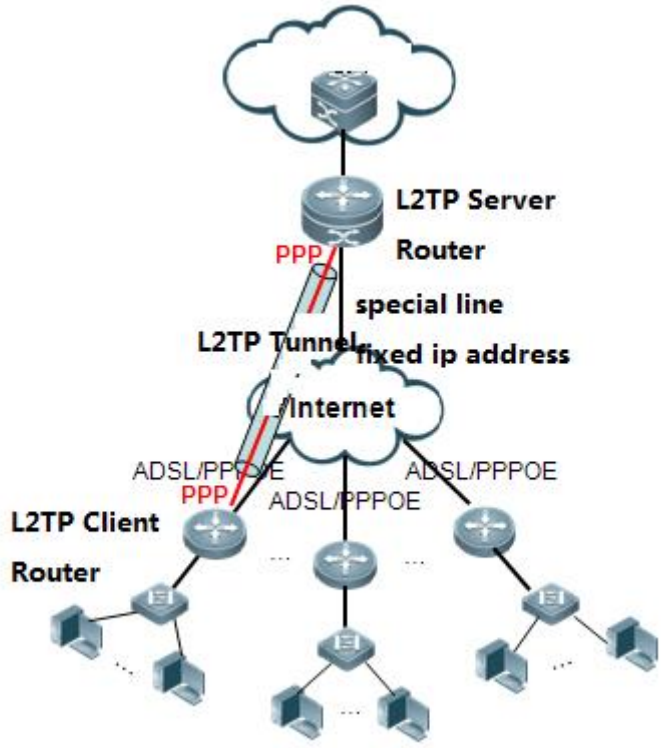
Two host routes are generated for the two clients.

L2TP 2.0 Voluntary Tunnel Mode – AAA Authentication

Features

In voluntary tunnel mode, a remote client runs the L2TP software and functions as an LAC in the L2TP connection model. The remote client/LAC ("LAC customer" in RFC 2661) is connected to the LNS, and PPP frames are directly forwarded through

the L2TP tunnel between a customer and the LNS. It is generally used for mutual access between the headquarters and branches of a company.



Scenario

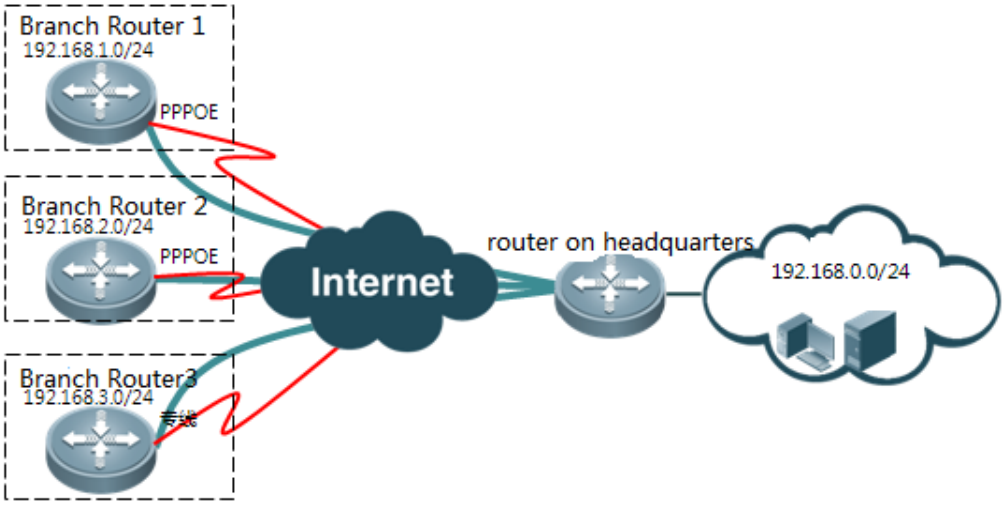
If the headquarters of a company and its branches need to share data through their intranets and the data security is not highly emphasized, the headquarters verifies branch routers by the local user names and passwords. For this purpose, you can enable L2TP VPN in compulsory mode on the network devices of the headquarters and branches, and configure local authentication for PPP authentication.

I.Networking Requirements

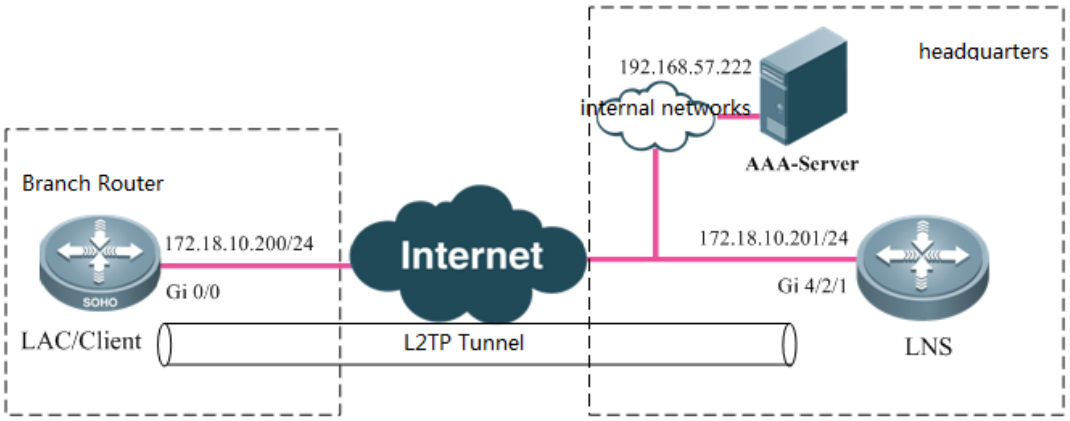
Due to business development, a company sets up multiple branches all over the country. The egress router in the headquarters is connected to the Internet through a dedicated line of an ISP, while the branches are connected to the Internet through a dedicated line or ADSL. The branches need to access the service server in the headquarters, and communication data between branches and the headquarters needs to be encrypted to ensure service security.

For this purpose, you can create an L2TP VPN between egress routers of the headquarters and the branches to realize mutual access.

II. Network Topology



Anolog Topology:



III. Configuration Tips

The major difference between configurations of L2TP VPN 2.0 and 1.0 is LNS configuration: 1. A virtual-vpdn 2.0 interface must be created first; 2. The source IP address of the VPDN-Group of the LNS must be specified; 3. The virtual-vpdn interface must be configured with a static IP address; 4. A new command must be used to configure and call the address pool. Note: The virtual-vpdn interface automatically adjusts the MSS (the length of the header encapsulated by the L2TP is deducted). However, when the interface is used together with other VPNs, the MSS must be modified manually.

Configuration Steps:

1. Configure the LNS VPDN.
2. Configure the LNS address pool.
3. Configure the LNS virtual-vpdn interface.
4. Configure the LNS AAA authentication.
5. Configure the LNS AAA accounting.

6. Configure PPP dial-up for branch routers.
7. Configure an L2TP CLASS for branch routers.
8. Configure an L2TP pseudowire-class interface for branch routers.
9. Configure a virtual-ppp interface for branch routers.

IV. Configuration Steps

1. Configure the LNS VPDN.

```
vpdn enable
interface virtual-vpdn 1   //Creates a virtual-vpdn interface first. The interface must be created in advance.
vpdn-group 1
    accept-dialin
        source-ip 172.18.10.201     //(Mandatory) It indicates the destination address of the LAC dial-in request packet and is generally the egress address of the dedicated line.
protocol l2tp
        virtual-vpdn 1            //It requires that the protocol is set to L2TP. Otherwise, this command will not be displayed during configuration.
l2tp tunnel authentication                      //Enables L2TP tunnel authentication as required.
l2tp tunnel password ruijie                    //Sets the L2TP tunnel authentication password to ruijie.
```

Note:

1) After configuring tunnel authentication and password on the LNS, configure the same on the L2TP client. Otherwise, L2TP negation fails.

2) If the destination address of the LAC dial-in request packet is the loopback address of the LNS, the **source-ip** command will not take effect and must be replaced with the **bind slot-id** command. The slot-id indicates the line card slot number of the dedicated line egress. This command is supported in the 10.4 (3b31) p1 version or later versions.

2. Configure the LNS address pool.

```
vpdn pool test 100.1.1.1 100.1.1.100              //Configures the address pool of the L2TP user. The command is different from the one for configuring the L2TP.
```

3. Configure the LNS virtual-vpdn interface.

```
interface Virtual-vpdn 1
 ppp authentication chap
 ip address 10.1.1.1 255.255.255.0     //The virtual-vpdn interface must be configured with a static IP address.
```

```
vpdn intf_pool test              //Calls the address pool configured for the VPDN on the interface. The command is different from the one for configuring the L2TP.
```

4. Configure the LNS AAA authentication.

```
aaa new-model
radius-server host 192.168.57.222 key ruijie   //Specifies the RADIUS Server and the key.
aaa authentication ppp default group radius         //Specifies the RADIUS protocol for PPP authentication.
```

5. Configure the LNS AAA accounting.

```
aaa new-model
aaa accounting update periodic 1      //Sets the accounting update interval to 1 minute. It is 5 minutes by default and 1 minute at least.
aaa accounting update                        //Enables accounting update.
aaa accounting network default start-stop group radius //Specifies the RADIUS protocol for start-accounting and end-accounting requests of network users.
```

Note:

Enable AAA accounting only when the RADIUS Server assigns IP addresses to users from the address pool, because the AAA address pool assigns and releases IP address using the user accounting function. If AAA assigns static IP addresses to AAA users, do not enable AAA accounting.

The configuration of branch routers (client/LAC) is the same as that of L2TP VPN 1.0 clients in voluntary tunnel mode.

6. Configure PPP dial-up for branch routers.

Ensure that branch routers have been connected to the Internet and can communicate with the LNS.

In case of ADSL dial-up, see **Typical Configuration** > **WAN Interface Configuration** > **ADSL Dial-up**.

7. Configure an L2TP CLASS for branch routers.

```
l2tp-class l2x
    hostname sitel
    authentication  //Enables L2TP tunnel authentication.
password ruijie            //Sets L2TP tunnel authentication password to ruijie.
```

Note: Configure the same tunnel authentication password on the L2TP client as that on the server. Otherwise, L2TP negation fails.

8. Configure an L2TP pseudowire-class interface for branch routers.

```
pseudowire-class pw
```

```
    encapsulation l2tpv2 //Specifies L2TPv2 for encapsulation.
protocol l2tpv2 l2x         //Specifies L2TPv2 as the tunneling protocol and "l2x" as the L2TP class.
ip local interface gi 0/0        ///Specifies the source IP address for L2TP tunnel negotiation. It
is the address of the external network interface.
```

9. Configure a virtual-ppp interface for branch routers.

```
interface Virtual-ppp 1
    ip ref
    ppp chap hostname test               //Configures the user name of CHAP authentication.
ppp chap password test                          //Configures the password of CHAP authentication.
ip address negotiate                                 //Configures IP addresses to be automatically
assigned.
pseudowire 172.18.10.201 1 pw-class pw          //Specifies the LNS address and "pw" as the
pseudowire-class.
```

V. Verification

1. Run the show vpdn command to check whether an L2TP tunnel is established.

(1) LAC/Client

```
50e#show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name          State  Remote Address  Port  Sessions L2TP Class/
                                                                      VPDN Group

1     57363 7708                 est    172.18.10.201   1701  1        xx

LocID       RemID       TunID       Username, Intf/      State    Last Chg
                                    Vcid, Circuit
1           35          1           1,vp1                est      01:43:27

%No active PPTP tunnels
50e#
```

(2) LNS

```
7708#show vpdn

VPDN ID : 1. DEVID 1. SessionLimit 10240,Server SessionCnt 1

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name          State  Remote Address  Port  Sessions L2TP Class/
                                                                      VPDN Group

57363 1     50e                  est    172.18.10.200   1701  1        1

LocID       RemID       TunID       Username, Intf/      State    Last Chg
                                    Vcid, Circuit
35          1           57363       test,vpdn1           est      01:36:10

%No active PPTP tunnels
7708#
```

2. Confirm that a tunnel has been established. Check whether the IP address of the virtual-ppp interface on the LAC/client is obtained.

```
50e#sh ip int b
Interface                      IP-Address(Pri)      OK?       Status
GigabitEthernet 0/0            172.18.10.200/24     YES       UP
GigabitEthernet 0/1            no address           YES       DOWN
GigabitEthernet 0/2            no address           YES       DOWN
GigabitEthernet 0/3            no address           YES       DOWN
Virtual-ppp 1                  100.1.1.1/32         YES       UP
50e#
```

The IP address assigned by the LNS has been obtained.

3. Check whether there is a host route to the peer end.

(1) LAC/Client

```
50e#sh ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.1.1/32 is directly connected, Virtual-ppp 1
C    100.1.1.1/32 is local host.
C    172.18.10.0/24 is directly connected, GigabitEthernet 0/0
C    172.18.10.200/32 is local host.
50e#
```

(2) LNS

```
7708#sh ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 172.18.10.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.18.10.1
C     10.1.1.0/24 is directly connected, Virtual-vpdn 1
C     10.1.1.1/32 is local host.
C     100.1.1.1/32 is directly connected, Virtual-vpdn 1
C     172.18.10.0/24 is directly connected, GigabitEthernet 4/2/1
C     172.18.10.201/32 is local host.
7708#
```

4. Verification

(1) LAC/client

```
50e#ping 10.1.1.1
Sending 5, 100-byte ICMP Echoes to 10.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
50e#
```

(2) LNS

```
7708#ping 100.1.1.1
Sending 5, 100-byte ICMP Echoes to 100.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
7708#
```

4.4.7 Local Attack Protection

Features:

Working Principle:

The local attack protection feature is a packet rate limit technology. It limits the rate of various packets sent to the CPU for processing, so as to avoid effects on data forwarding of the whole machine due to high CPU usage after a great amount of packets are sent to the CPU for processing.

Applying Rules:

Since this feature limits the rates based on packet types, it may also limit the rates of normal packets and thus affect the forwarding of normal packets (for example, the normal fragmented packets need to be sent to the CPU for processing). Therefore, this feature is not recommended in a clean network environment.(This feature is disabled by default in devices other than RSR77).

Command Interpretation:

```
control-plane
!
control-plane protocol
 no acpp        //Globally limits the rate of the protocol plane.
!
control-plane manage
 no port-filter  //Filters TCP and UDP not enabled locally.
 no arp-car    //Limits the rate of ARP.
 no acpp        //Globally limits the rate of the management plane.
!
control-plane data
 no glean-car   //Matches the packets which are directly connected to the route but of which the IP is not resolved.
 no acpp        //Globally limits the rate of the data plane.
```

Scenario:

1. The CPU usage is high because a great amount of abnormal packets are sent to the CPU for processing. Other situations resulting in high CPU usage include:

(1) There are many fragmented packets needing to be reassembled by the CPU: Use the ACPP on the data plane to control the rate.

(2) There are packets of which the routes are unreachable, and thus the CPU needs to process the packets and replies that the routes are unreachable: Use the glean-car on the data plane to control the rate.

(3) As for attacks on the local IP address: Use ACPP on the data plane to control the rate.

Others.

2. If the size of a specific packet in the network can be predicted, you can configure a threshold value to avoid abnormal attacks. For example, if it can be predicted that there are 10 normal ARP packets per second, you can make the following configuration:

```
control-plane manage
port-filter
 arp-car 10
 no acpp
```

Recommended Configuration:

Unless otherwise required, it is recommended to enable the local attack protection feature through the following configuration:

```
control-plane
!
control-plane protocol
acpp bw-rate 300 bw-burst-rate 600
!
control-plane manage
port-filter
 arp-car 10
 acpp bw-rate 300 bw-burst-rate 600
!
control-plane data
glean-car 5
 acpp bw-rate 300 bw-burst-rate 600
```

4.5 Network Management and Monitoring

4.5.1 IPFIX

4.5.1.1 IPv4

Features

IP Flow Information Export (IPFIX) is a standard protocol for flow information measurement that is released by Internet Engineering Task Force (IETF).The advantages of the protocol lie in that:

1. The protocol can be applied to network devices and management systems of any manufacturers and is able to export traffic statistics based on the network device. This makes it easy for network administrators to extract and display important traffic statistics.
2. The export format is highly extensible. Therefore, if the requirements for traffic monitoring change, a network administrator simply needs to modify configurations instead of upgrading software or management tools.

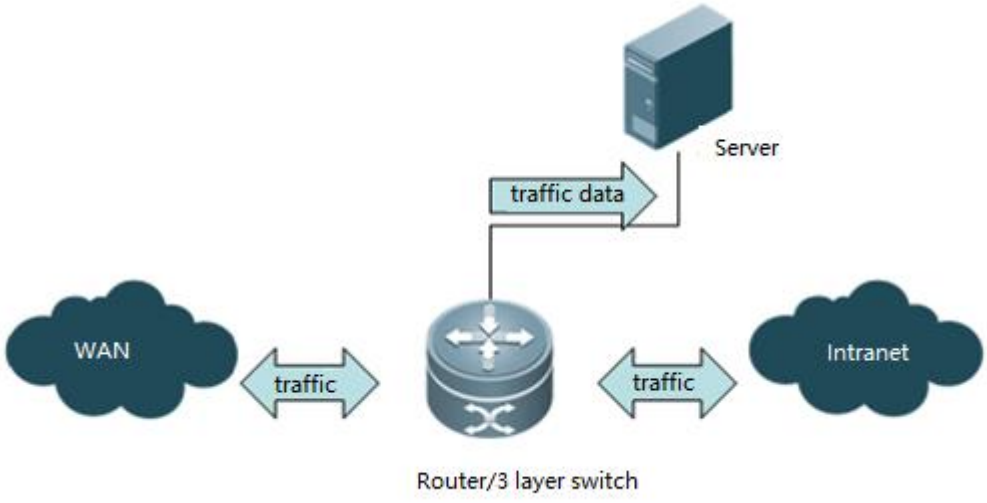
IPFIX is based on "flow". Network devices indicate the network traffic through seven key fields: source IP address, destination IP address, source port, destination port, type of Layer-3 protocol, type of service, and input logic interface. If all these key fields are matched in different IP packets, these packets will be regarded as the same flow. By recording the characteristics of the flow (for example, duration and average packet length), we can understand the network application and perform optimization, security detection and traffic-based billing accordingly.

IPFIX includes three devices: Export, Collector and Analyzer. The following describes the relationship among these devices:

1. The Export device analyzes the network traffic, extracts qualified traffic statistics and exports them to the Collector device. Generally, the Export device is a network device that enables IPFIX, for example, a router or a switch.

2. The Collector device analyzes packets of the Export device and collects statistics in the database for the Analyzer device to analyze.
3. The Analyzer device extracts statistics from the Collector device and processes them to provide a basis for services. The data is displayed on a graphical interface.

NOTE: In the current application scenario, the Collector device and the Analyzer device are usually integrated into a single server. For example, the devices can be integrated into a NetFlow server.



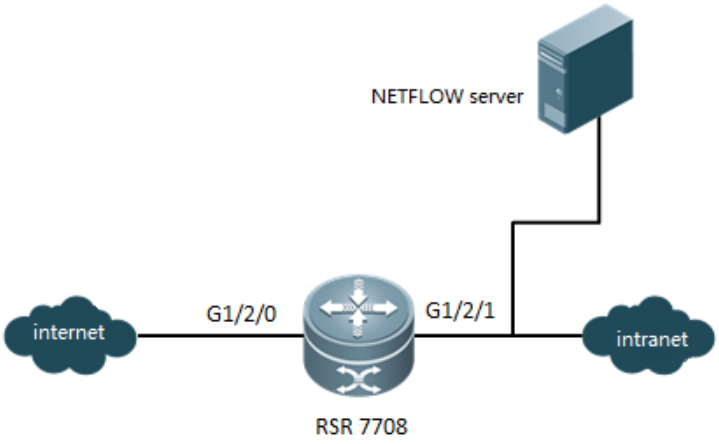
Scenario

If an enterprise network administrator who needs to monitor the network traffic collects traffic data of the router (including interface traffic and device-forwarded traffic) by deploying the NetFlow server, IPFIX can be enabled on the router to transmit traffic data to the network management software.

I.Networking Requirements:

The RSR50 router serves as an egress. A NetFlow server is deployed in the inside network to process traffic data that travels through the egress.

II. Network Topology:



III. Configuration:

1. Configure IPFIX for the router.
2. Configure the NetFlow server.

IV. Steps

1. Configure IPFIX for the router.

(1) Configure the IP address and port ID of the target NetFlow server. The default port ID is 9996.

```
ip flow-export destination 10.0.0.2 9996
```

(2) Configure the source IP address of the exported flow records. By default, the address is the IP address of the outbound interface.

```
ip flow-export source gigabitEthernet 0/1
```

(3) Configure the flow template export frequency.

```
ip flow-export template timeout-rate 5
ip flow-export template refresh-rate 30
```

NOTE: According to Step 3, flow templates are retransmitted every 30 packets or every five minutes. By default, flow templates are retransmitted every 20 packets or every five minutes.

(4) Configure the packet format for flow record export.

```
ip flow-export version 9  //Exports flow records in Version 9 format through IPFIX.
```

NOTE: Ruijie routers support IPFIX and Version 9 formats. However, as certain analysis software does not support Version 9 format, IPFIX format is recommended.

(5) Configure the aging flow records in the cache.

```
ip flow-cache timeout active 1            //Configures the aging time for active flows as 1 minute.
```

```
ip flow-cache timeout inactive 10        //Configures the aging time for inactive flows as 10
seconds.
```

IPFIX counts traffic based on the data flows forwarded by the router. Only when a flow ages will the flow information and traffic be converted into CFLOW data, encapsulated into User Datagram Protocol (UDP) packets and transmitted to the server. The following describes how to judge whether a flow ages.

(1) If no packets of the flow are detected within a time period (inactive time), such flow ages, and flow information should be exported.

(2) When a flow lasts for a long time, you cannot record its information without limit; instead, you can set a time limit (active time). When the time limit is exceeded, the flow should be aged and the flow information should be exported.

The aging time for data flows varies in different applications. For example, data flows of Hyper Text Transport Protocol (HTTP) generate unexpected traffic. Each flow will rapidly age so that IPFIX can send the state of the flow to the NetFlow server in real time. Data flows of File Transfer Protocol (FTP) and Xunlei might age after all downloads are finished. If downloading a file by FTP takes one hour, as the default aging time for active flows is 30 minutes, the state of FTP data flows is updated every 30 minutes and transmitted to the NetFlow server. As a result, line traffic is very instable and large unexpected traffic is often generated.

Therefore, configuration of the aging time for flow records in the cache is critical.

NOTE: The parameters of flow record aging are very important. Improper configuration will result in faults such as inaccurate traffic, so the values described above are recommended (aging time for active/inactive flows is 1 minute/10 seconds, respectively).

(6) Enable traffic counting.

```
ip access-list standard 1
10 permit any              //Configures the Access Control List (ACL) to define the traffic to be
counted.
interface gigabitEthernet 0/0
ip flow egress            //Enables traffic counting at the egress.
ip flow ingress          //Enables traffic counting at the ingress.
flow-sample 255 filter 1     //Configures the flow sampling rate and associates the traffic to be
counted.
```

NOTE: It is recommended to configure the flow sampling rate by running the ip flow sample fix xx filter y command on routers RSR77 later than Version 3B21.

Command interpretation:

The sampling rate cannot be adjusted by running the "flow-sample 255 filter 1" command. Even if "255" is configured, the sampling rate is 1:1.

The sampling rate can be adjusted by running the "ip flow-sample fix xx filter y" command. Run the "ip flow-sample fix 2 filter 1" commend to configure the sampling rate as 1:2.

Notes:

1. As IPFIX of RSR routers is implemented by software, the sampling rate cannot be configured on versions **earlier than 3B21**. However, you can filter the sampled data flows through standard or extended ACLs.

2. After running the **ip flow egress** or **ip flow ingress** command on the interface, you must run the **flow-sample** command to configure flow filtration; otherwise, port traffic cannot be converted into IPFIX traffic.

2. Configure the NetFlow server.

Check whether the monitoring port matches the export destination port of the RSR router. If the two ports are not matched, the server cannot analyze traffic.

NOTE: For detailed configuration, see the *NetFlow Analyzer Operation Manual.pdf*.

V. Verification

1. Display the interfaces on which NetFlow is enabled.

```
Ruijie#show ip flow interface
GigabitEthernet 0/0
  ip flow ingress
  ip flow egress
```

2. Display flow information in the cache.

```
Ruijie#show ip flow cache
ip flow switching cache, 60000 entries
    38 active, 59962 inactive
    active flows timeout in 1 minutes
    inactive flows timeout in 10 seconds

Protocol       Total Flows    Total packets  Total bytes    Active time
tcp-http       14             71             14296          294
udp-ntp        1              1              76             62
udp-http       2              2              60             123
udp-dns        6              10             896            296
udp-other      1425           2081           122699         82620
udp            1434           2094           123731         83101
tcp            14             71             14296          294
Total:         1448           2165           138027         83395
```

```
Display entries in main cache :
SrcIf   SrcIPAddress      DstIf   DstIPAddress      Pr   Tos  SrcPort DstPort Pkts        ActiveTime
1       84.229.249.50     2   192.168.33.187    17   0    4671    23887    0       37
2       192.168.33.187    1   83.149.116.231    17   0    15005   4254     1       54
2       192.168.33.187    1   193.138.230.251   17   0    15005   4254     1       9
2       192.168.33.187    1   190.51.222.59     17   0    23887   11331    1       41
```

```
2        192.168.33.187     1    88.191.40.237      17    0     15005    3310     1        24
2        192.168.51.34      65535 192.168.51.255     17    0     137      137      0        7
2        192.168.33.62      1    192.168.33.255     17    0     137      137      1        13
```

NOTE: Flows in the cache are activated. After flows age, the device will transmit flow statistics to the NetFlow server.

3. Display exported flow information.

```
Ruijie#show ip flow export
cache for main metering process:
       flow export is enabled
        Exporting flows to 10.0.0.2 (2055)
        Exporting using source interface GigabitEthernet 0/1
        Template export information:
           Template timeout = 5 minutes
           Template refresh rate = 30 packets
        total 2070 packets metering
        total 0 packets dropped for no memory
        total 1366 flows exported in 180 udp datagrams
        0 ipfix message export failed
```

NOTE: When the NetFlow server cannot detect traffic, pay attention to

the **show ip flow export** command. Confirm the exported destination addresses, ports and packet statistics.

4. Display the monitored data on the NetFlow server.

(1) Display interface traffic and rates.

(2) Display real-time traffic on an interface.

Appendix: FAQ

1. UDP packets of IPFIX can be captured on the NetFlow server, but data cannot be obtained.

Check configurations of firewall and antivirus software on the operating system (OS).

2. The real-time flow diagram on the NetFlow server is inaccurate and fluctuates wildly.

The flow aging parameter is set to a low value.

ip flow-cache timeout active 1

ip flow-cache timeout inactive 10

The shorter the aging time is, the more accurate the real-time traffic value is.

3. RSR routers cannot configure the sampling rate of IPFIX.

As IPFIX of RSR routers is used for software implementation, sampling does not take effect despite the **flow-sample packet-number filter acl-name** command. The purpose of running this command is to filter the traffic transmitted to the IPFIX module (the traffic is generated by running the **ip flow ingress** and **ip flow egress** commands on the port) by using an ACL

so as to analyze the traffic matched to the ACL and export traffic data to the NetFlow server. The **packet-num** parameter makes no sense. The ultimate sampling rate is 1:1.

As IPFIX of the switch is implemented by hardware, the sampling rate can be modified.

4. The NetFlow server cannot display the interface name.

By default, the NetFlow server cannot display the interface name but the index number. To have the interface name displayed, configure Simple Network Management Protocol (SNMP) parameters on the router and add an SNMP management device to the NetFlow server.

Add an SNMP management device to the NetFlow server:

4.5.1.2 IPv6

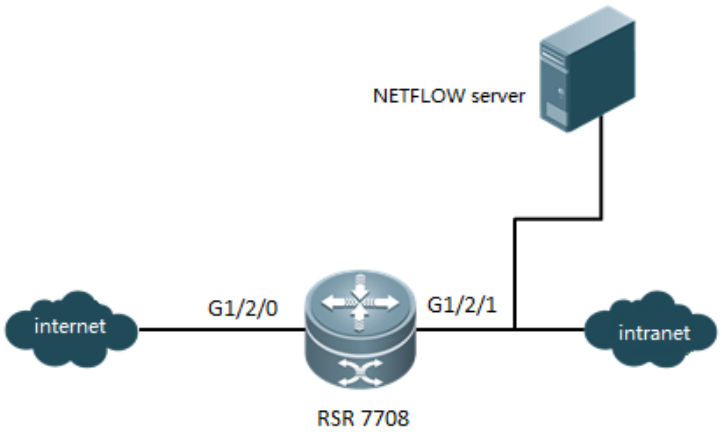
Scenario

If an enterprise network administrator who needs to monitor the network traffic collects traffic data of the router (including interface traffic and device-forwarded traffic) by deploying the NetFlow server, IPFIX can be enabled on the router to transmit traffic data to the network management software.
Currently, only RSR77 routers with versions later than Release 3B21 support IPv6 IPFIX.

I.Networking Requirements:

The RSR7708 router serves as an egress. A NetFlow server is deployed in the inside network to process traffic data that travels through the egress.

II. Network Topology:



III. Configuration Tips

1. Configure IPFIX for the router.
2. Configure the NetFlow server.

IV. Configuration Steps

1. Configure IPFIX for the router.

(1) Configure the IP address and port ID of the target NetFlow server.

```
ipv6 flow-export destination 140.1.1.66 2055          //The exported flow records should be sent to the IP address of the collector as well as the port monitored by the collector. The port ID must be consistent with that of the server.
```

(2) Configure the source IP address of the exported flow records. By default, the address is the IP address of the outbound interface.

```
ipv6 flow-export source GigabitEthernet 1/2/0  //Configures the IPv6 address of the interface as the source IPv6 address of exported packets.
```

(3) Configure the flow template export frequency.

```
ipv6 flow-export template timeout-rate 5   //Configures the frequency of data template and option retransmission. Retransmits a template every 5 minutes.
ipv6 flow-export template refresh-rate 10  //Configures the frequency of data template and option transmission. Transmits a template every 10 packets.
```

(4) Configure the packet format for flow record export.

```
ipv6 flow-export version 9  //Specifies the IPFIX version.
```

NOTE: Ruijie routers support IPFIX and Version 9 formats. However, as certain analysis software does not support Version 9 format, IPFIX format is recommended.

(5) Configure the aging flow records in the cache.

```
ipv6 flow-cache timeout active 1   //Configures the aging time for active flows. If flows last for a long time, export the flow information every minute.
ipv6 flow-cache timeout inactive 10            //Configures the aging time for inactive flows. If no packets are detected within 10 seconds, export the flow information.
```

NOTE: The parameters of flow record aging are very important. Improper configuration will result in faults such as inaccurate traffic, so the values described above are recommended (aging time for active/inactive flows is 1 minute/10 seconds, respectively).

For information on active and inactive flows, see the "IPv4" section.

(6) Enable traffic counting.

```
ipv6 access-list v6
 10 permit ipv6 any any     //Analyzes all traffic on the interface.
interface GigabitEthernet 1/2/0
```

```
ipv6 flow egress  //Enables sampling at the egress.
ipv6 flow ingress //Enables sampling at the ingress.
ipv6 flow-sample fix 1 filter v6    //Samples the ACL v6-matched packet flows at a rate of 1:1.
```

2. Configure the NetFlow server.

See the "IPv4" section.

V. Verification

1. Display the interfaces on which NetFlow is enabled.

```
Ruijie#show ipv6 flow interface
```

```
Ruijie#show ipv6 flow interface
MPLS flow cache disable, include ip fields, no mpls length
Interface      Direction      Mode           Packet-num     Acl
Gi4/1/3        both           Fix            1              v6
Ruijie#
```

2. Display flow information in the cache.

```
Ruijie#show ipv6 flow cache
```

```
Ruijie#show ipv6 flow cache

Ipfixv6 collect data from CM-CARD
ipv6 flow switching cache, 65536 entries
    0 active, 65536 inactive
    active flows timeout in 1 minutes
    inactive flows timeout in 10 seconds

Protocol       Total Flows    Total packets  Total bytes    Active time
Total:         0              0              0              0

Display entries in main cache :


Ipfix collect data from device 13
ip flow switching cache, 65536 entries
    0 active, 65536 inactive
    active flows timeout in 1 minutes
    inactive flows timeout in 10 seconds

Protocol       Total Flows    Total packets  Total bytes    Active time
Total:         0              0              0              0

Display entries in main cache :
Protocol SrcIf/DstIf                          SPort-DPort    SrcIPAddress/DstIPAddress
Ruijie#
```

As no traffic is generated in the test, the result is 0.

3. Display exported flow information.

```
Ruijie#show ipv6 flow export
```

```
Ruijie#show ipv6 flow export

Ipfix collect data from CM-CARD
cache for main metering process:
        Flow export is disabled
        Source interface to IPv4 network: --
        Source interface to IPv6 network: GigabitEthernet 4/1/3
        Exporting flows to -- source: --
        Exporting flows to 140.1.1.66 (2055) source: --
        Template export information:
        Version 9 flow records
        IPV6 Template ID = 257
           Template timeout = 5 Minute(s)
           Template refresh rate = 10
        0 flows exported in 0 udp datagrams
        0 flows failed to export
        0 messages failed to export

Ipfix export information from device 13
cache for main metering process:
        Flow export is disabled
        Source interface to IPv4 network: --
        Source interface to IPv6 network: GigabitEthernet 4/1/3
        Exporting flows to -- source: --
        Exporting flows to 140.1.1.66 (2055) source: --
        Template export information:
        Version 9 flow records
        IPV6 Template ID = 257
           Template timeout = 5 Minute(s)
           Template refresh rate = 10
        0 flows exported in 0 udp datagrams
        0 flows failed to export
        0 messages failed to export
Ruijie#
```

4. Display the monitored data on the NetFlow server.

See the "IPv4" section.

4.5.1.3 MPLS

Scenario

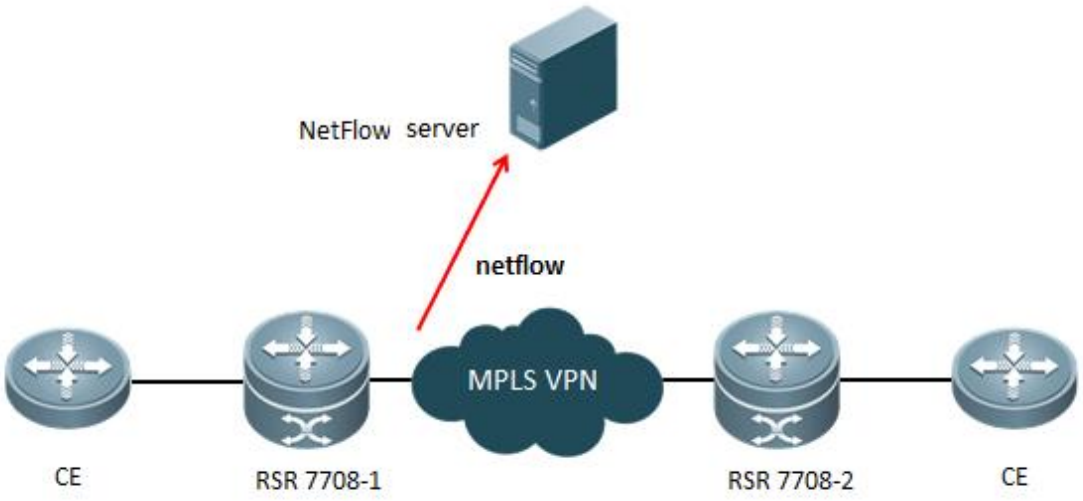
If an enterprise network administrator who needs to monitor the Multiple Protocol Label Switching (MPLS) traffic collects traffic data of the router (including interface traffic and device-forwarded traffic) by deploying the NetFlow server, IPFIX can be enabled on the router to transmit traffic data to the network management software.

Currently, only RSR77 routers with versions later than Release 3B21 support MPLS IPFIX.

I.Networking Requirements:

Two RSR7708 routers serve as Provider Edge (PE) devices for the deployment of an MPLS Virtual Private Network (VPN). A NetFlow server is deployed in the inside network to process traffic data that travels through the egress.

II. Network Topology:



III. Configuration Tips

1. Configure IPFIX for the router.
2. Configure the NetFlow server.

IV. Configuration Steps

Release 3B21 and later versions support MPLS IPFIX, and the Real-time Intelligent Infrastructure Library (RIIL) supports MPLS IPFIX-based presentation. IPFIX configuration on an MPLS VPN is unrelated to the MPLS VPN type. L2 VPN and L3 VPN share the same command and method.

1. Configure IPFIX for the router.

(1) Enable IPFIX sampling for MPLS.

```
ip flow-cache mpls label-positions            //Enables MPLS sampling.
ip flow-cache mpls label-positions 1 2 3  //Configures the positions of sampling labels. There is no sampling label by default.
```

(2) Configure the IP address and port ID of the target NetFlow server.

```
ip flow-export destination 10.1.1.2 9996        //The exported flow records should be sent to the IP address of the collector as well as the port monitored by the collector. The port ID must be consistent with that of the server.
```

(3) Configure the source IP address of the exported flow records. By default, the address is the IP address of the outbound interface.

```
ip flow-export source GigabitEthernet 3/0/1    //Configures the IPv6 address of the interface as the source IPv6 address of exported packets.
```

(4) Configure the flow template export frequency.

```
ip flow-export template timeout-rate 5   //Configures the frequency of data template and option retransmission. Retransmits a template every 5 minutes.
ip flow-export template refresh-rate 10  //Configures the frequency of data template and option transmission. Transmits a template every 10 packets.
```

(5) Configure the packet format for flow record export.

```
ip flow-export version 9    //Specifies the IPFIX version.
```

NOTE: Ruijie routers support IPFIX and Version 9 formats. However, as certain analysis software does not support Version 9 format, IPFIX format is recommended.

(6) Configure the aging flow records in the cache.

```
ip flow-cache timeout active 1   //Configures the aging time for active flows. If flows last for a long time, export the flow information every minute.
ip flow-cache timeout inactive 10          //Configures the aging time for inactive flows. If no packets are detected within 10 seconds, export the flow information.
```

NOTE: The parameters of flow record aging are very important. Improper configuration will result in faults such as inaccurate traffic, so the values described above are recommended (aging time for active/inactive flows is 1 minute/10 seconds, respectively).

For information on active and inactive flows, see the "IPv4" section.

(7) Enable traffic counting.

```
ip access-list standard 1
 10 permit any     //Analyzes all traffic on the interface.
interface GigabitEthernet 3/0/1
 ip flow egress    //Enables sampling at the egress.
 ip flow ingress   //Enables sampling at the ingress.
 ip flow-sample fix 1 filter 1       //Samples the ACL 1-matched packet flows at a rate of 1:1.
```

2. Configure the NetFlow server.

See the "IPv4" section.

V. Verification

1. Display the interfaces on which NetFlow is enabled.

```
Ruijie#show ip flow interface
```

2. Display flow information in the cache.

```
Ruijie#show ip flow cache
```

3. Display exported flow information.

```
Ruijie#show ip flow export
```

4. Display the monitored data on the NetFlow server.

See the "IPv4" section.

4.6 Reliability

4.6.1 BFD

4.6.1.1 Multihop BFD

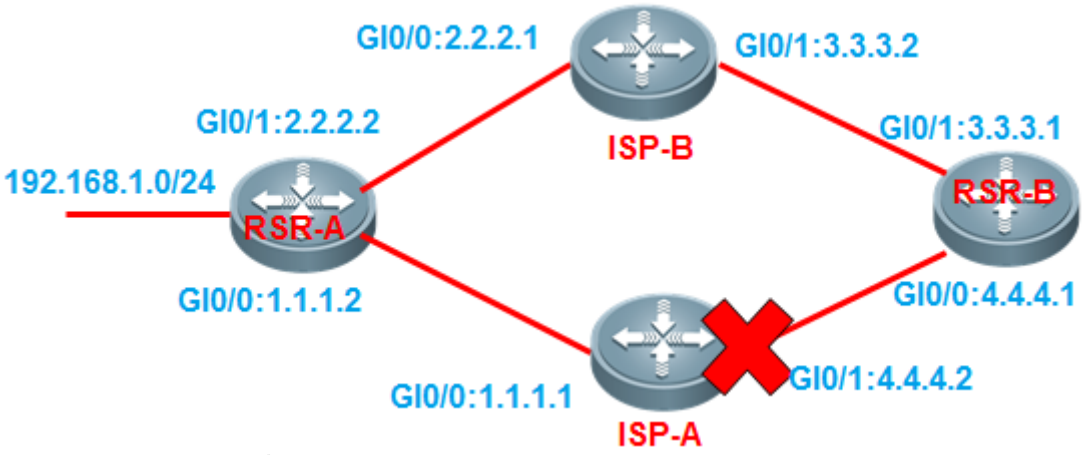
Scenario

An enterprise rents a Multi-Service Transmission Platform (MSTP) line from an Internet Service Provider (ISP)to configure static recursive routing. As the local router at the egress cannot detect intermediate link interruption and whether the next hop of static recursive routing is reachable, routes cannot be converged and thereby causes faults to the network. In this case, you can associate static routing with multihop Bidirectional Forwarding Detection (BFD) on the router to detect interruption of the ISP's network and timely switch to other backup lines to access the Internet.

I.Networking Requirements

RSR-A serves as a router of a financial service office. Two MSTP links are connected. Floating static routing is used. ISP-A serves as an active link. When ISP-A is unavailable, the device switches to ISP-B. Without a detection mechanism, an Ethernet link considers a line available if the interface is in UP state. Therefore, BFD protocol is used as a link detection protocol.Different from "direct BFD association", a router serves as the ISP, that is, the connectivity of the entire link must be detected every two hops for routing switchover.

II. Network Topology



III. Configuration Tips

Access port:

1. Configure floating static routing.
2. Associate BFD with static routing.
3. Configure static Address Resolution Protocol (ARP)-based binding.

Aggregation port:

1. Configure floating static routing.
2. Associate BFD with static routing.
3. Configure static ARP-based binding.

IV. Configuration Steps

Access port:

1. Configure floating static routing.

```
RSR-A(config)#interface gigabitEthernet 0/0
RSR-A(config-GigabitEthernet 0/0)#ip address 1.1.1.2 255.255.255.0
RSR-A(config)#interface gigabitEthernet 0/1
RSR-A(config-GigabitEthernet 0/1)#ip address 2.2.2.2 255.255.255.0
RSR-A(config)#ip route 0.0.0.0 0.0.0.0  gigabitEthernet 0/0 4.4.4.1
//NOTE: Configure the next hop as 4.4.4.1 to detect the connectivity of the entire link.
RSR-A(config)#ip route 0.0.0.0 0.0.0.0   2.2.2.1 200     //Configures the floating routing.
```

2. Associate BFD with static routing.

```
RSR-A(config)#interface gigabitEthernet 0/0
RSR-A(config-GigabitEthernet 0/0)#bfd interval 500 min_rx 500 multiplier 3
```

```
//Configures BFD time, which is necessary because BFD is enabled on the interface by running this command.
500/500/3 is recommended, which means to transmit a detection packet every 500 ms and announce link failure if no response is received after transmitting consecutive 3 packets.
RSR-A(config-GigabitEthernet 0/0)#no bfd echo
//Ctrl mode is recommended, and the default mode is BFD echo mode.
Ctrl mode is recommended for connection to devices of other industry peers; otherwise, connection might fail.
RSR-A(config)#ip route static bfd GigabitEthernet 0/0 4.4.4.1 source 1.1.1.2          //Associates BFD with static routing.
```

3. Configure static ARP-based binding.

```
RSR-A(config)#arp 4.4.4.1 0011.1111.111 arpa
//You must bind the address of the next hop based on ARP, or ARP cannot be parsed.0011.1111.1111 is the Media Access Control (MAC) address of the port GIO/0 on ISP-A.
```

Aggregation port:

1. Configure floating static routing.

```
RSR-B(config)#interface gigabitEthernet 0/0
RSR-B(config-GigabitEthernet 0/0)#ip address 4.4.4.1 255.255.255.0
RSR-B(config)#interface gigabitEthernet 0/1
RSR-B(config-GigabitEthernet 0/1)#ip address 3.3.3.1 255.255.255.0
RSR-B(config)#ip route 192.168.1.0 255.255.255.0 gigabitEthernet 0/0 1.1.1.2
RSR-B(config)#ip route 192.168.1.0 255.255.255.0 3.3.3.2 200
```

2. Associate BFD with static routing.

```
RSR-B(config)#interface gigabitEthernet 0/0
RSR-B(config-GigabitEthernet 0/0)#bfd interval 500 min_rx 500 multiplier 3
RSR-B(config-GigabitEthernet 0/0)#no bfd echo
RSR-B(config)#ip route static bfd GigabitEthernet 0/0 1.1.1.2 source 4.4.4.1
```

3. Configure static ARP-based binding.

```
RSR-A(config)#arp 1.1.1.2 0022.2222.2222 arpa
//You must bind the address of the next hop based on ARP.0022.2222.2222 is the MAC address of the portGIO/1 on ISP-A.
```

V. Verification

1. Run the **show bfd neighbors** command to confirm the state of BFD neighbors.

```
R1#sh bfd nei
OurAddr   NeighAddr  LD/RD RH/RS  Holdown(mult)  State  Int
1.1.1.2   4.4.4.1       2/1  Up       0(5   )        Up     GigabitEthernet 0/0
```

2. Run the **show ip route** command to display the routing table.
3. If configuration and link are correct, run the **tracert** command on RSR-A to trace the inside network address of the aggregation port so as to confirm that ISP-A is used as the path.
4. Shut down the GI0/0 port on RSR-B to simulate an ISP-A failure. Then run the **tracert** command on RSR-A to trace the inside network address of the aggregation port so as to confirm that the path is switched to ISP-B.

4.6.1.2 BFD for RIP

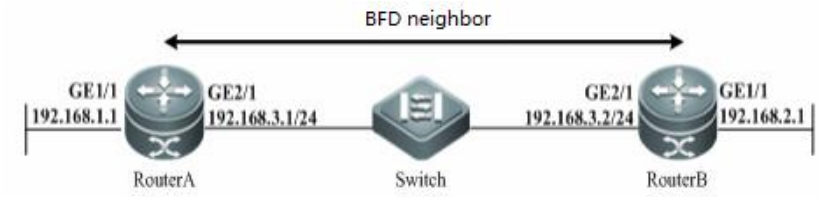
Scenario

An enterprise rents a Multi-Service Transmission Platform (MSTP) line from an Internet Service Provider (ISP) to configure Routing Information Protocol (RIP). As the local router at the egress cannot detect intermediate link interruption, routers cannot be converged quickly and the device cannot switch to other backup lines timely. In this case, you can associate RIP with Bidirectional Forwarding Detection (BFD) on the router to quickly detect interruption of the ISP's network and timely switch to other backup lines to improve user experience.

I.Networking Requirements

Connect Router A to Router B through the Layer-2 switch. Generate routes by running RIP. Enable association between RIP and BFD on interfaces of the routers. BFD quickly detects faults on the link between Router B and the Layer-2 switch and notifies RIP to trigger quick convergence.

II. Network Topology



III. Configuration Tips

1. Configure RIP routing.
2. Associate RIP with BFD.

(1) Enable BFD on the interface.

(2) Select BFD mode.

(3) Associate RIP with BFD.

IV. Configuration Steps

Router A configuration:

1. Configure RIP routing.

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#ip ref
RSR-A(config-GigabitEthernet 2/1)#ip address 192.168.3.1 255.255.255.0
RSR-A(config)#interface gigabitEthernet 1/1
RSR-A(config-GigabitEthernet 1/1)#ip ref
RSR-A(config-GigabitEthernet 1/1)#ip address 192.168.1.1 255.255.255.0
RSR-A(config-router)#  router rip
RSR-A(config-router)#  version 2
RSR-A(config-router)#  network 192.168.3.0
RSR-A(config-router)#  network 192.168.1.0
```

2. Associate RIP with BFD.

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
//Configures BFD time, which is necessary because BFD is enabled on the interface by running this command.
500/500/3 is recommended, which means to transmit a detection packet every 500 ms and announce link failure if no response is received after transmitting consecutive 3 packets.
RSR-A(config-GigabitEthernet 2/1)#no bfd echo
//Ctrl mode is recommended, and the default mode is BFD echo mode.
Ctrl mode is recommended for connection to devices of other industry peers; otherwise, connection might fail.
RSR-A(config-GigabitEthernet 2/1)#ip rip bfd //Associates RIP with BFD on the correct interface.
```

Router B configuration:

1. Configure RIP routing.

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#ip ref
RSR-B(config-GigabitEthernet 2/1)#ip address 192.168.3.2 255.255.255.0
RSR-B(config)#interface gigabitEthernet 1/1
RSR-B(config-GigabitEthernet 1/1)#ip ref
RSR-B(config-GigabitEthernet 1/1)#ip address 192.168.2.1 255.255.255.0
```

```
RSR-B(config-router)#  router rip
RSR-B(config-router)#  version 2
RSR-B(config-router)#  network 192.168.3.0
RSR-B(config-router)#  network 192.168.2.0
```

2. Associate RIP with BFD.

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
RSR-B(config-GigabitEthernet 2/1)#no bfd echo
RSR-B(config-GigabitEthernet 2/1)#ip rip bfd
```

V. Verification

1. Run the **show bfd neighbors** command to confirm the state of BFD neighbors.

```
Ruijie# show bfd neighbors details
OurAddr       NeighAddr     LD/RD  RH/RS  Holdown(mult) State  Int
192.168.3.1   192.168.3.2   1/2        Up      532 (3 )      Up     Ge2/1
```

4.6.1.3 BFD for OSPF

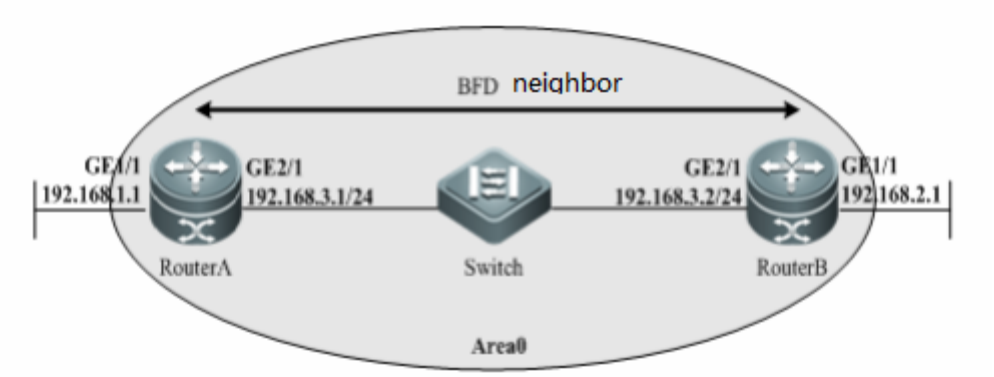
Scenario

An enterprise rents a Multi-Service Transmission Platform (MSTP) line from an Internet Service Provider (ISP) to configure Open Shortest Path First (OSPF). As the local router at the egress cannot detect intermediate link interruption, routes cannot be converged quickly and the device cannot switch to other backup lines timely. In this case, you can associate OSPF with Bidirectional Forwarding Detection (BFD) on the router to quickly detect interruption of the ISP's network and timely switch to other backup lines to improve user experience.

I.Networking Requirements

Connect Router A to Router B through the Layer-2 switch. Generate routes by running OSPF. Enable association between OSPF and BFD on interfaces of the routers. BFD quickly detects faults on the link between Router B and the Layer-2 switch and notifies OSPF to trigger quick convergence.

II. Network Topology



III. Configuration Tips

1. Configure OSPF routing.
2. Associate OSPF with BFD.
   (1) Enable BFD on the interface.
   (2) Select BFD mode.
   (3) Associate OSPF with BFD.

IV. Configuration Steps

Router A configuration:

1. Configure OSPF routing.

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#ip ref
RSR-A(config-GigabitEthernet 2/1)#ip address 192.168.3.1 255.255.255.0
RSR-A(config)#interface gigabitEthernet 1/1
RSR-A(config-GigabitEthernet 1/1)#ip ref
RSR-A(config-GigabitEthernet 1/1)#ip address 192.168.1.1 255.255.255.0
RSR-A(config-router)#  router ospf 123
RSR-A(config-router)#  network 192.168.3.0 0.0.0.255 area 0
RSR-A(config-router)#  network 192.168.1.0 0.0.0.255 area 0
```

2. Associate OSPF with BFD.

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
//Configures BFD time, which is necessary because BFD is enabled on the interface by running this command.
```

```
500/500/3 is recommended, which means to transmit a detection packet every 500 ms and announce link failure if no response is received after transmitting consecutive 3 packets.
RSR-A(config-GigabitEthernet 2/1)#no bfd echo
//Ctrl mode is recommended, and the default mode is BFD echo mode.
Ctrl mode is recommended for connection to devices of other industry peers; otherwise, connection might fail.
RSR-A(config-GigabitEthernet 2/1)#ip ospf bfd   //Associates OSPF with BFD on the correct interface.
```

Router B configuration:

1. Configure OSPF routing.

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#ip ref
RSR-B(config-GigabitEthernet 2/1)#ip address 192.168.3.2 255.255.255.0
RSR-B(config)#interface gigabitEthernet 1/1
RSR-B(config-GigabitEthernet 1/1)#ip ref
RSR-B(config-GigabitEthernet 1/1)#ip address 192.168.2.1 255.255.255.0
RSR-B(config-router)#  router ospf 123
RSR-B(config-router)#  network 192.168.3.0 0.0.0.255 area 0
RSR-B(config-router)#  network 192.168.2.0 0.0.0.255 area 0
```

2. Associate OSPF with BFD.

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
RSR-B(config-GigabitEthernet 2/1)#no bfd echo
RSR-B(config-GigabitEthernet 2/1)#ip ospf bfd
```

V. Verification

1. Run the **show bfd neighbors** command to confirm the state of BFD neighbors.

```
Ruijie# show bfd neighbors details
OurAddr         NeighAddr      LD/RD  RH/RS  Holdown(mult) State  Int
192.168.3.1     192.168.3.2    1/2        Up      532 (3 )       Up      Ge2/1
```

4.6.1.4 BDF for BGP

Scenario

An enterprise rents a Multi-Service Transmission Platform (MSTP) line from an Internet Service Provider (ISP) to configure Border Gateway Protocol (BGP). As the local router at the egress cannot detect intermediate link interruption, routes cannot

be converged quickly and the device cannot switch to other backup lines timely. In this case, you can associate BGP with Bidirectional Forwarding Detection (BFD) on the router to quickly detect interruption of the ISP's network and timely switch to other backup lines improve user experience.

I.Networking Requirements

Connect Router A to Router B through the Layer-2 switch. Generate routes by running BFD. Enable association between BFD and BFD on interfaces of the routers.BFD quickly detects faults on the link between Router B and the Layer-2 switch and notifies BGP to trigger quick convergence.

II. Network Topology

III. Configuration Tips

1. Configure BGP routing.
2. Associate BGP with BFD.

(1) Enable BFD on the interface.

(2) Select BFD mode.

(3) Associate BGP with RIP.

IV. Configuration Steps

Router A configuration:

1. Configure BGP routing.

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#ip ref
RSR-A(config-GigabitEthernet 2/1)#ip address 172.16.11.1 255.255.255.0
RSR-A(config)#interface gigabitEthernet 1/1
RSR-A(config-GigabitEthernet 1/1)#ip ref
```

```
RSR-A(config-GigabitEthernet 1/1)#ip address 172.19.0.1 255.255.255.0
RSR-A(config-router)#  router bgp 45000
RSR-A(config-router)#  bgp log-neighbor-changes
RSR-A(config-router)#  neighbor  172.16.11.2 remote-as  40000
RSR-A(config-router)#  address-family ipv4
RSR-A(config-router-af)# neighbor  172.16.11.2 activate
RSR-A(config-router-af)# no auto-summary
RSR-A(config-router-af)# no synchronization
RSR-A(config-router-af)# network  172.19.0.0  mask 255.255.255.0
```

2. Associate BGP with BFD.

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
//Configures BFD time, which is necessary because BFD is enabled on the interface by running this command.
500/500/3 is recommended, which means to transmit a detection packet every 500 ms and announce link failure if no response is received after transmitting consecutive 3 packets.
RSR-A(config-GigabitEthernet 0/0)#no bfd echo
//Ctrl mode is recommended, and the default mode is BFD echo mode.
Ctrl mode is recommended for connection to devices of other industry peers; otherwise, connection might fail.
RSR-A(config-router)#  router bgp 45000
RSR-A(config-router)#  neighbor 172.16.11.2 fall-over bfd     //Associates BGP with BFD.
```

Router B configuration:

1. Configure BGP routing.

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#ip ref
RSR-B(config-GigabitEthernet 2/1)#ip address 172.16.11.2 255.255.255.0
RSR-B(config)#interface gigabitEthernet 1/1
RSR-B(config-GigabitEthernet 1/1)#ip ref
RSR-B(config-GigabitEthernet 1/1)#ip address 172.20.0.1 255.255.255.0
RSR-B(config-router)#  router bgp 40000
RSR-B(config-router)#  bgp log-neighbor-changes
RSR-B(config-router)#  neighbor  172.16.11.1 remote-as  45000
RSR-B(config-router)#  address-family ipv4
RSR-B(config-router-af)# neighbor  172.16.11.1 activate
RSR-B(config-router-af)# no auto-summary
RSR-B(config-router-af)# no synchronization
RSR-B(config-router-af)# network  172.20.0.0  mask 255.255.255.0
```

2. Associate BGP with BFD.

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
RSR-B(config-GigabitEthernet 0/0)#no bfd echo
RSR-B(config-router)#  router bgp 40000
RSR-B(config-router)#  neighbor 172.16.11.1 fall-over bfd
```

V. Verification

1. Run the **show bfd neighbors** command to confirm the state of BFD neighbors.

```
Ruijie# show bfd neighbors details
OurAddr        NeighAddr      LD/RD  RH/RS  Holdown(mult) State  Int
192.168.3.1    192.168.3.2    1/2        Up      532 (3 )       Up      Ge2/1
```

4.6.2 VRRP

Features:

Virtual Router Redundancy Protocol (VRRP) adopts master/backup mode to ensure that when the master router is faulty, a backup router functions without affecting internal and external communication or modifying parameters of the inside network. Multiple routers under VRRP are mapped to one virtual router. VRRP ensures that only one router serves as a virtual router to transmit packets. The host transmits packets to the virtual router, and such router is selected as a master router. If the master router fails, one of the backup routers will replace it. Under VRRP, it seems that a host on a local area network (LAN) uses only one router, and the route remains functional even when the first-hop router fails.

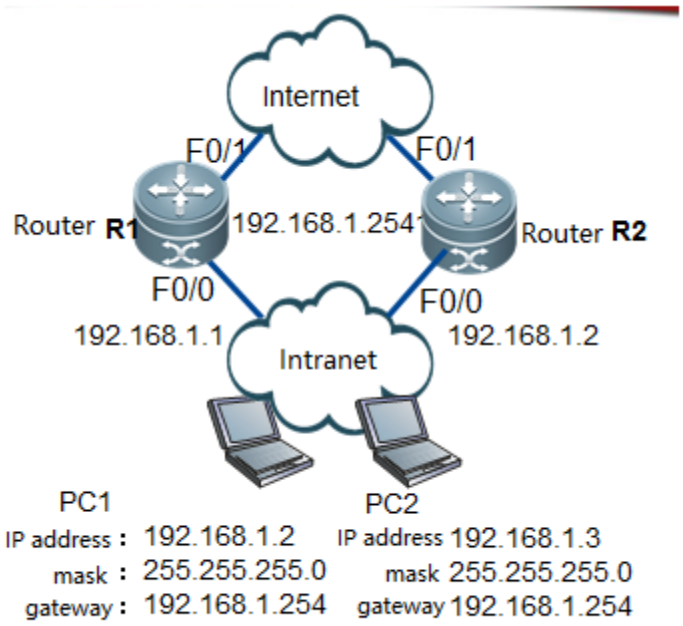
Scenario

An enterprise has two gateway routers (master and backup). Redundancy backup is required between them. Normally, the master router is used. When the master router is faulty, the system automatically switches to the backup router. In this case, you can enable VRRP on both routers for redundancy backup.

I.Networking Requirements

1. Two routers are available on the inside network to connect egress devices.
2. Gateway backup is performed on both routers. The inside network has only one gateway address.
3. When the uplink interface or line of either router is disconnected, master/backup switchover can be automatically triggered for network connectivity.

II. Network Topology



III. Configuration Tips

1. Perform basic Internet configuration (deploy according to network design).
2. Configure VRRP on the inside network port.
3. Configure a virtual gateway address on the client.

IV. Configuration Steps

R1 configuration:

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface fastEthernet 0/0
Ruijie(config-if-FastEthernet 0/0)#ip address 192.168.1.1 255.255.255.0      //Configures the real interface IP address.
Ruijie(config-if-FastEthernet 0/0)#vrrp 1 ip 192.168.1.254       //Specifies a virtual VRRP address.
Ruijie(config-if-FastEthernet 0/0)#vrrp 1 priority 120           //Specifies VRRP priority for the interface. The higher the value, the higher the priority. The default is 100.
Ruijie(config-if-FastEthernet 0/0)#vrrp 1 track FastEthernet 1/0 30    //When the detection uplink port f1/0 is down, the priority is lowered to 30, and the system switches to the backup gateway.
```

```
Ruijie(config-if-FastEthernet 0/0)#end
Ruijie#write            //Verifies and saves the configuration.
```

R2 configuration:

```
Ruijie#configure terminal
Ruijie(config)#interface fastEthernet 0/0
Ruijie(config-if-FastEthernet 0/0)#ip address 192.168.1.2 255.255.255.0
Ruijie(config-if-FastEthernet 0/0)#vrrp 1 ip 192.168.1.254
Ruijie(config-if-FastEthernet 0/0)#end
Ruijie#write           //Verifies and saves the configuration.
```

V. Verification

1. Run the **sh vrrp brief** command to display the VRRP negotiation state:

```
Ruijie#sh vrrp  brief
Interface                Grp       Pri        timer          Own              Pre            State
Master addr              Group
 addr
FastEthernet 0/0        1        120         3                -                P
Master      192.168.1.1           192.168.1.254
Interface              VRRP group priority keepalive time  Is the interface address is preempted?
VRRP state Local address Virtual gateway address
No. The gateway address is the VRRP group address.
Ruijie#show vrrp 1
FastEthernet 0/0 - Group 1
State is Master                                  //The address of this interface is a master
address.
Virtual IP address is 192.168.1.254 configured          //Indicates the VRRP group IP address.
Virtual MAC address is 0000.5e00.0101              //Indicates the VRRP group MAC address.
Advertisement interval is 1 sec                         //Indicates the interval of VRRP packets.
Preemption is enabled                              //Indicates that VRRP preemption is enabled.
min delay is 0 sec
Priority is 120       //It indicates VRRP priority.
Master Router is 192.168.1.1  (local), priority is 120      //Indicates the master VRRP address and
priority.
Master Advertisement interval is 1 sec             //Indicates the interval of master VRRP packets.
Master Down interval is 3 sec                 //If master VRRP packets are not received within 3
seconds, the master VRRP address does not function.
```

4.6.3 Link-Based Interface Backup

Features

Link-based interface backup:

(1) When active links are connected, standby interfaces are DOWN.

(2) If active links are disconnected and the routes to destination addresses are lost, the system will enable standby links within the backup time.

(3) If active links are re-connected, the system will disable standby interfaces and switch to active links within the backup time.

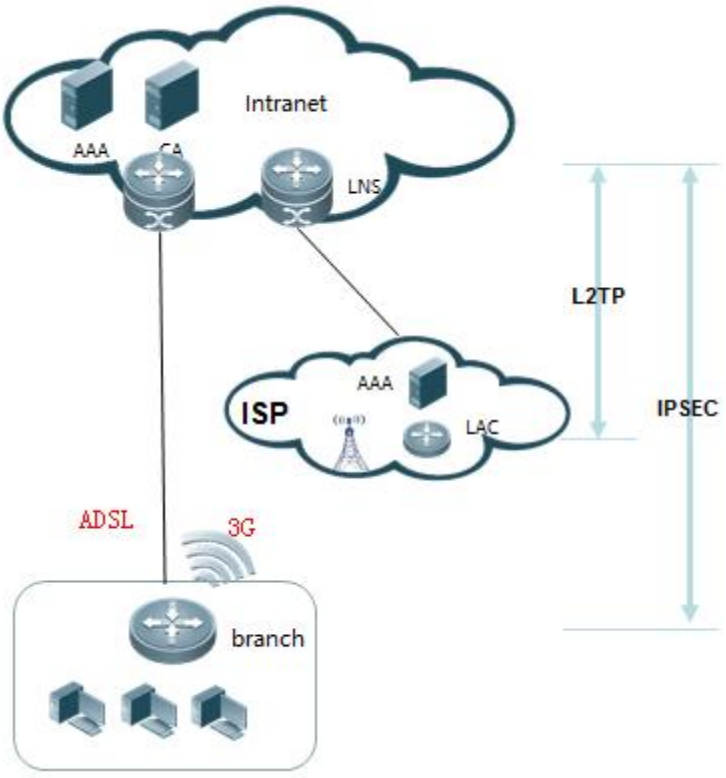
Scenario

An enterprise rents two egress lines. The wired dedicated line serves as the active line, which is normally used to forward traffic. The 3G line serves as the standby line. As traffic-based accounting is applied to the 3G line, the line is normally in standby mode. When the wired dedicated line is disconnected, the 3G line is enabled. In this case, you can configure the 3G interface as the standby interface to enable redundancy backup.

I.Networking Requirements

1. All users transmit data through the dedicated line, and the 3G line serves as a standby line.
2. To save 3G traffic, the system prohibits 3G dialing when the active link is connected.
3. When the dedicated line is faulty, the system switches to the 3G line.

II. Network Topology



III. Configuration Tips

1. Configure the standby interface for the active interface.
2. Configure the active/standby switchover delay.
3. Configure routing between the active and standby interfaces.

IV. Configuration Steps

Router configuration:

```
interface dialer 0          //Configures the active link (Asymmetric Digital Subscriber Line, ADSL)
interface.
standby delay 0 0       //Configures the time for switchover to the standby interface. 0 indicates
immediate switchover.
standby interface async 1    //Configures the standby interface (3G dialer interface).
ip route 0.0.0.0 0.0.0.0 dialer 0     //Configures routing.
ip route 0.0.0.0 0.0.0.0 async 1
//For detailed ADSL and 3G dialing configuration, see the corresponding section.
```

V. Verification

1. Run the **show interface** command to display the state of the standby interface.

```
Ruijie#show interface async 1
async 1  is standby mode  , line protocol is DOWN
//The interface is in standby mode and DOWN.
```

4.6.4 GR

Features

Technical Background:

1. Devices of distributed architecture that support uninterrupted forwarding require separation of the control plane and the data plane.
2. The control plane calculates routing and assigns entries. The data plane forwards data according to these forwarded entries.
3. During active/standby engine switchover, the standby engine with information on the data plane can quickly replace the active engine to forward data. However, the standby engine has no information on the control plane (such as information on the dynamic routing database or neighborship). As a result, the adjacent device detects dynamic protocol interruption, its dynamic route re-converges, and thereby black-hole or bypass route is generated on the entire network.
4. The convergence time for a dynamic route is measured in minutes, which is not adequate for uninterrupted forwarding.

Principle:

Graceful Restart (GR) aims to realize uninterrupted data forwarding during protocol restart. During active/standby switchover of supervisor modules, GR maintains the entries forwarded by dynamic routing neighbors and refreshes them after new neighbors complete negotiation and convergence so that the network topology keeps stable, the forwarding table is maintained, and service is uninterrupted.

Roles of GR:

Restarter: It is a device that enables GR.

Helper: It is a device adjacent to the Restarter to assist it in GR.

Scenario

The router of an enterprise has dual control engines. When the active engine is faulty, the device switches to the standby engine, and the dynamic routing protocol re-converges, which results in network interruption. To solve this problem, you can

enable GR on the router to maintain routing forwarded entries and data forwarding during active/standby engine switchover, and refresh the entries after the routing protocol re-converges to shorten the network interruption time and improve user experience.

GR Configuration

RIP-GR configuration: Configure the Restarter on the local end rather than on the adjacent device because Routing Information Protocol (RIP) supports the Helper.

```
RSR7708(config)#router rip
RSR7708(config-router)#graceful-restart
```

OSPF-GR configuration: Configure the Restarted on the local end and the Helper on the adjacent device. (By default, the Helper is enabled on Ruijie devices and enabled in most cases on partners' devices.)

```
RSR7708(config)#router ospf 1
RSR7708(config-router)#graceful-restart
```

BGP-GR configuration: Configure the Restarter on both ends. //Border Gateway Protocol (BGP) neighbors must be re-established.

```
RSR7708(config)#router bgp 1
RSR7708(config-router)#bgp graceful-restart
```

Notes:

1. Routers with a single control engine do not support the GR Restarter, so GR is configured on routers with dual control engines such as RSR77, RSR77-X and RSR50E-40.
2. The GR Helper is enabled by default on Ruijie devices.

4.6.5 DLDP

Basic Configuration for DLDP

Functions and Principles

As the Ethernet has no link keepalive protocol, the MSTP dedicated line is connected via the Ethernet interface in the WAN. While the intermediate link of an ISP is often unavailable, the status of the local end protocol is UP, resulting in slow route convergence and more difficulties in locating faults. Device Link Detection Protocol (DLDP) sends ICMP packets to check whether the peer end is reachable and whether communication over the MSTP dedicated line is normal. If the peer end is unreachable, set the interface protocol status to DOWN and accelerate convergence of status for application-based routes related to the interface.

Configuration Description

In interface configuration mode, use the following command syntax for configuration.

Dldp *ip* [*next-hop ip*] interval *x* retry *y* resume *z*

Dldp ip: Indicates the destination address for detection, that is, the reachability of ICMP packets to this address.

Next-hop ip: If the destination address and the interface are not in the same network segment, add the next-hop IP address of the interface.

Interval: Indicates the interval of sending ICMP echoes. It is 10 tickets by default (1 ticket ≈ 10 ms), that is, 10 ICMP echoes are sent every second. It can be changed based on the actual condition. 100 is recommended, that is, one ICMP echo is sent every second.

Retry: Configures retransmission times. It is 3 times by default.

Resume: Sets the recovery threshold of the device link. The threshold indicates the required times of receiving consecutive responses for detection packets before the link status is recovered from DOWN to UP. Link recovery time = Resume times * DLDP IP interval. The value is 1 by default.

Scenario

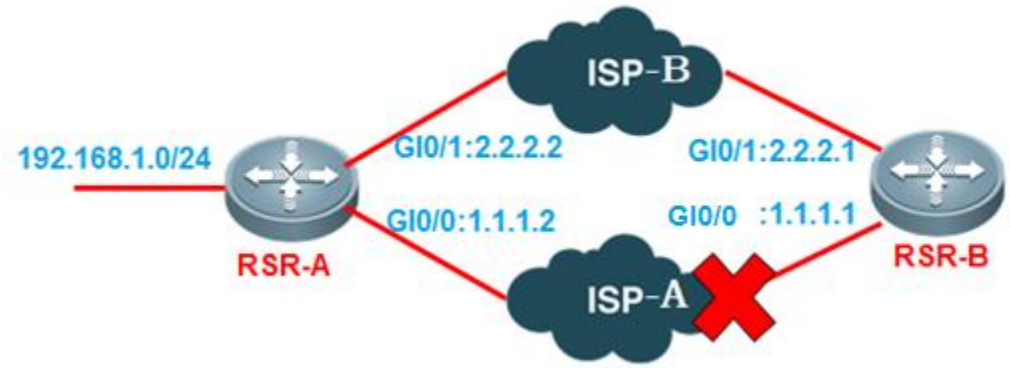
DLDP is generally used when a company rents an MSTP dedicated line from an ISP. The local egress router of the company cannot detect communication interruption in the intermediate link, resulting in slow route convergence or even convergence failure, and unavailable Internet access. To solve this problem, you can enable DLDP on the outbound interface, which can detect network interruption of the ISP and promptly switch to other backup links for users to access the Internet.

I.Networking Requirements

RSR-A serves as an access router of a financial service office. It is connected to two MSTP links and uses a floating static route with ISP-A as the active link and ISP-B as the backup link. As Ethernet links have no detection mechanism, a link is considered available as long as the interface status is UP. Therefore, DLDP should be used as the link detection protocol.

Devices on the aggregation port have the same link detection problem, so enable DLDP on the aggregation port.

II. Network Topology



III. Configuration Tips

Access Port:

1. Configure a floating static route.
2. Configure DLDP.

Aggregation Port:

1. Configure a floating static route.
2. Configure DLDP.

IV. Configuration Steps

Access Port:

1. Configure a floating static route.

```
RSR-A(config)#interface gigabitEthernet 0/0
RSR-A(config-GigabitEthernet 0/0)#ip address 1.1.1.2 255.255.255.0
RSR-A(config)#interface gigabitEthernet 0/1
RSR-A(config-GigabitEthernet 0/1)#ip address 2.2.2.2 255.255.255.0
RSR-A(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.1
RSR-A(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1 200      //Indicates a floating static route.
```

2. Configure DLDP.

```
RSR-A(config)#interface gigabitEthernet 0/0
RSR-A(config-GigabitEthernet 0/0)#dldp 1.1.1.1 interval 100      //Configures the peer address for DLDP detection. It is recommended to set the detection interval to at least one second so as to alleviate pressure on the aggregation port. 100 indicates that 100*10 ms=1s.
//If the address of the hopping device is detected, for example 3.3.3.3, configure next-hop IP address to dldp 3.3.3.3 1.1.1.1 interval 100;
//If the peer devices are not from Ruijie, note that if other vendors set rate limit for ping packets by default, DLDP detection on the access devices may be affected. (As H3C and Huawei devices set rate limit for ping packets by default, disable it).
RSR-A(config)#interface gigabitEthernet 0/1
RSR-A(config-GigabitEthernet 0/1)#dldp 2.2.2.1 interval 100
```

Aggregation Port:

1. Configure a floating static route.

```
RSR-B(config)#interface gigabitEthernet 0/0
RSR-B(config-GigabitEthernet 0/0)#ip address 1.1.1.1 255.255.255.0
RSR-B(config)#interface gigabitEthernet 0/1
RSR-B(config-GigabitEthernet 0/1)#ip address 2.2.2.1 255.255.255.0
RSR-B(config)#ip route 192.168.1.0 255.255.255.0 1.1.1.2
```

```
RSR-B(config)#ip route 192.168.1.0 255.255.255.0 2.2.2.2 200
```

2. Configure DLDP.

```
RSR-B(config)#interface gigabitEthernet 0/0
RSR-B(config-GigabitEthernet 0/0)#dldp 1.1.1.2 interval 100
RSR-B(config-GigabitEthernet 0/0)#dldp passive
//Serves as the aggregation port. It is recommended to set it to the passive mode and alleviate the burden on it.Configurations for the detection interval of the aggregation port and access port are the same.
RSR-B(config)#interface gigabitEthernet 0/1
RSR-B(config-GigabitEthernet 0/1)#dldp 2.2.2.2 interval 100
RSR-B(config-GigabitEthernet 0/1)#dldp passive
```

V. Verification

1. Run the **show dldp interface** command to check the status of DLDP.

```
Ruijie(config)#sho dldp interface
Id  Ip_addr       Next-hop      Mode   Interval Retry Resume State Down_times
Up_times Start_time       Interface
--- --------------- --------------- ------- -------- ----- ------ ----- ---------- -------- ------------
------- -------------------
1  1.1.1.1       1.1.1.1       active  100    3    1    UP   0        0       2013-3-14
6:23:18  gigabitEthernet 0/0
```

2. If both the configuration and link status are correct, perform a tracert on the intranet address of the aggregation port on the RSR-A and confirm that the path taken is ISP-A.
3. Shut down the GI0/0 interface on the RSR-B to simulate an ISP-A fault. Perform a tracert on the intranet address of the aggregation port on the RSR-A and confirm that the path is switched to ISP-B.

4.6.6 RNS+Track

Features

RNS(Ruijie Network Service) is used to monitor end to end connection by detecting whether there is a response packet received from peer. RNS function is able to send ICMP echo and DNS request for probing. By integrating with Track object, it allows to monitor whether an IP is reachable or Interface is up or not.

Scenario

An enterprise has multi egress lines from ISP and request the company services can be switchover to the other egress even one of Internet line is down.

Configuration Steps

1. Create RNS profile

```
Ruijie>enable
Ruijie(config)#ip rns 1  --->Create RNS profile number 1
Ruijie(config-ip-rns)#icmp-echo 12.12.12.1 out-interface gigabitEthernet 0/0 source-ipaddr 12.12.12.2
--->Use ICMP-echo to detect destination 12.12.12.1 and output interface gigabitEthernet 0/0, source
IP address 12.12.12.2
Notes: if needs to specify the next hop on RNS profile, add "next-hop x.x.x.x" parameter.
Ruijie(config-ip-rns-icmp-echo)#timeout 5000 --->Detection timeout threshold 5000 msec
Ruijie(config-ip-rns-icmp-echo)#frequency 5000 --->Detection interval threshold 5000 msec
Ruijie(config-ip-rns-icmp-echo)#exit
Ruijie(config)#
```

2. Create Track template

```
Ruijie(config)#track 1 rns 1 --->Create track template and bind with RNS profile
Ruijie(config-track)#delay up 10 down 10   --->delay interval for track status change
Ruijie(config-track)#exit
```

3. Track integrating with Static Route

```
Ruijie(config)#ip route 10.1.1.0 255.255.255.0 gigabitEthernet 0/0 1.1.1.1 track 1----> Integrating
with static route. If the track status is down, this route will be invalidated.
```

4. Track integrating with Policy Map(partial command)

```
Ruijie(config-route-map)#set ip next-hop verify-availability 12.12.12.1 track 1  ---> Integrating
with policy route. If the track status is down, this policy route will be invalidated.
```

Verification

Verify track status(show track)

```
Ruijie#show track 1
Track 1
  Reliable Network Service 1
  The state is Down   --->status
1 change,current state last:648 secs
  Delay up 10 secs,down 10 secs
```

Verify RNS status(show ip rns statiscs)

```
Ruijie#show ip rns statistics
IP rns index    1
Number of successes:2 --->success times
Number of failures:16  --->failure times
Round-trip min/avg/max = 10/12/15 ms
```

4.7 QOS

4.7.1 Traffic Classification and Marking

I. Definition

Traffic classification refers to the classification of traffic into different priorities or service types. For example, the first three bits of the Type of Service (ToS) field in an IP packet header or the Differentiated Service Code Point (DSCP) field is used to mark a packet. After packet classification, other QoS features can be applied to different classes to achieve congestion management and traffic shaping based on classes.

Packet classification refers to simple classification based on Layer-2 or Layer-3 information. It is a collection of packet classification mechanisms.

Packet marking is a function that allows network devices to mark packet classes.

II. Purpose

The main purpose of traffic marking is to enable other application systems or devices to make clear the packet classes and then process the packets as agreed.

Packet classification and marking are the basis for QoS implementation.

Technology for packet classification: ACL and IP precedence

Packets are transferred to other modules based on classification results or marked (colored) for differentiated use by the core network

III. Methods

Three methods are available:

Class-map

CAR

PBR

IV. Method Selection

Class-map is the most recommended method. Class-map is combined with CBWFQ/LLQ, offering uniform and clear commands. Note that the function of class-map method is limited for interface applying in input direction.

Input direction for interfaces with class-map method is not supported by baseline v10.3 while it is supported by baseline v10.4.

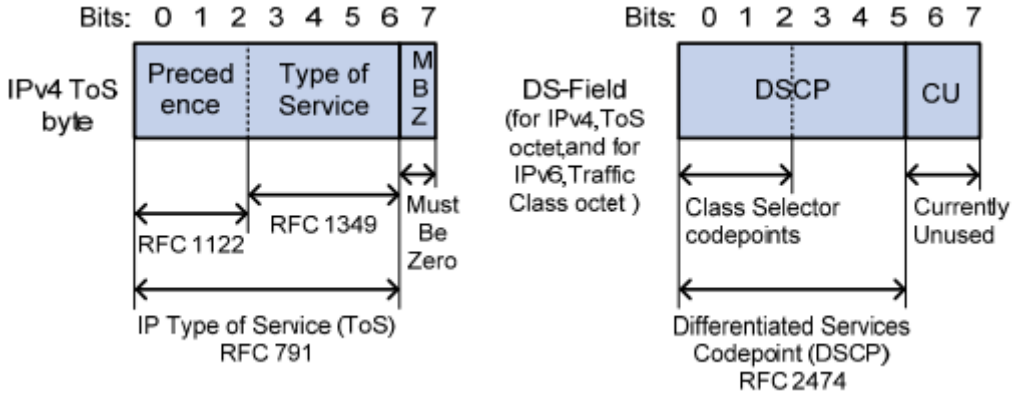
CAR method comes second.

PBR method is effective only in input direction.

4.7.1.1 IP Priority and DSCP Priority

Features:

IP priority and DSCP priority:



As shown in the figure above, the ToS field in the IP packet header has 8 bits, in which the first three bits indicate IP priority ranging from 0 to 7.In RFC 2474, the ToS field in an IP packet header is redefined as the DS (Differentiated Services) field, in which the first six bits (0 to 5th) indicate DSCP priority ranging from 0 to 63 and the last two bits (6th to 7th) are reserved bits.

EXP priority:

EXP priority is indicated in an MPLS label for marking MPLS QoS.

Encapsulation structure of an MPLS label

In the figure above, the Exp field is the EXP priority with 3 bits, ranging from 0 to 7.

IP priority/DSCP/EXP mapping comparison table:

IP Priority	DSCP	EXP
0	0 ~ 7	0
1	8 ~ 15	1
2	16 ~ 23	2
3	24 ~ 31	3
4	32 ~ 39	4
5	40 ~ 47	5
6	48 ~ 55	6
7	56 ~ 63	7

IP priority binary value/decimal value/keyword comparison table:

IP priority (decimal value)	IP priority(binary value)	Keyword
0	000	routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

DSCP priority binary value/decimal value/keyword comparison table:

DSCP priority (decimal value)	DSCP prioriy (binary value)	Keyword
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be（default）

4.7.1.2 Class Map

Features:

A class map defines a traffic classification: network traffic that is of interest to you. A policy map defines a series of actions (functions) that you want to apply to a set of classified inbound traffic.

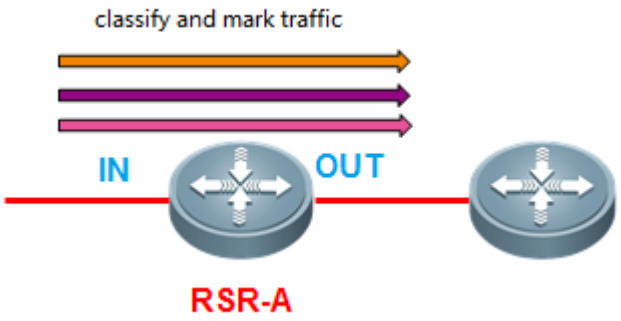
I.Networking Requirements

For RSR-A routers, the following data is marked:

1. For VOIP traffic, IP priority is 5

2. For telnet traffic, IP priority is 4
3. For traffic from 172.16.1.0, IP priority is 2

II. Network Topology



III. Configuration Tips

1. Classify traffic by ACL.
2. Define a class mapping list, and associate class-map with an ACL.

   Router(config)#class-map ?
   WORD class-map name
   match-all Logical-AND all matching statements under this classmap----------The match condition is "and" (logical "and")
   match-any Logical-OR all matching statements under this classmap----------The match condition is "or"(logical "or")
   Router(config)#class-map ruijie ----------If only the name is given but match-all or match-any is not indicated, match-all is used by default
3. Define a policy mapping list, associate with class-map, and mark class-map classes.
4. Apply policy-map on the target interface.

IV. Configuration Steps

1. Classify traffic by ACL.

```
RSR-A(config)#access-list 100 permit udp any any range 16384 32767
RSR-A(config)#access-list 101 permit tcp any any eq 23
RSR-A(config)#access-list 102 permit ip 172.16.1.0 0.0.0.255 any
```

2. Define a class mapping list, and associate class-map with an ACL.

```
RSR-A(config)#class-map VOIP            //Note that the naming is case-sensitive here
```

```
RSR-A(config-cmap)#match access-group 100
RSR-A(config-cmap)#class-map TELNET
RSR-A(config-cmap)#match access-group 101
RSR-A(config-cmap)#class-map  NETWORK
RSR-A(config-cmap)#match access-group 102
```

3. Define a policy mapping list, associate with class-map, and mark class-map classes.

```
RSR-A(config)#policy-map ruijie
RSR-A(config-pmap)#class VOIP
RSR-A(config-pmap-c)#set ip precedence 5
RSR-A(config-pmap-c)#class TELNET
RSR-A(config-pmap-c)#set ip precedence 4
RSR-A(config-pmap-c)#class NETWORK
RSR-A(config-pmap-c)#set ip precedence 2
```

4. Apply policy-map on the target interface

```
RSR-A(config)#interface gigabitEthernet 0/0
RSR-A(config-if-GigabitEthernet 0/0)#service-policy output ruijie       //Specifies the direction in which the traffic policy should be applied (either on packets coming into the interface or packets leaving the interface).Input direction for interfaces with class-map method is not supported by baseline v10.3 while it is supported by baseline v10.4.
```

V. Verification

1. Run the show policy-map interface gigabitEthernet 0/0command to display the policy applied on the target interface.

```
RSR-A#sho policy-map interface gigabitEthernet 0/0

GigabitEthernet 0/0  output(tc policy): XWX
    Class VOIP
      set ip precedence 5
      mark count 0

    Class TELNET
      set ip precedence 4
      mark count 0

    Class NETWORK
      set ip precedence 2
      mark count 0
```

4.7.1.3 CAR

Features:

CAR has two features: rate limit and priority setting. CAR statements require both rate limit and IP precedence configurations.

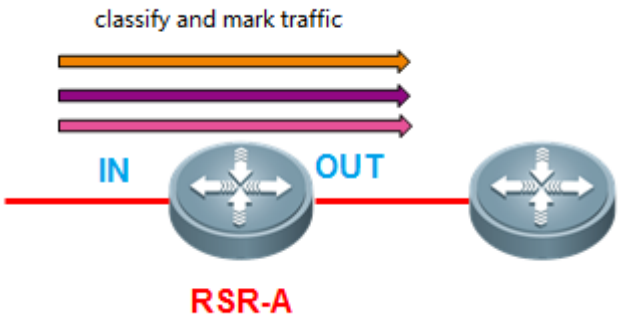
CAR is used to classify packets based on their ToS or CoS values (IP or DSCP precedence for IP packets) and Quintet Vector (protocol port IDs of the source and destination addresses), mark these packets and monitor traffic.

I.Networking Requirements

For RSR-A routers, the following data is marked:

1. For VOIP traffic, DSCP priority is 10.
2. For telnet traffic, DSCP priority is 20.
3. For traffic from 172.16.1.0, DSCP priority is 30.

II. Network Topology



III. Configuration Tips

1. Classify traffic by ACL.
2. Configure rate-limit to mark traffic classes.

IV. Configuration Steps

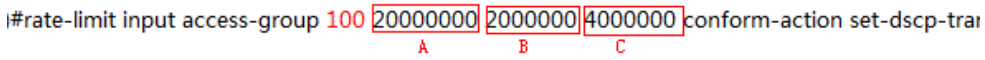
1. Classify traffic by ACL.

```
RSR-A(config)#access-list 100 permit udp any any range 16384 32767
RSR-A(config)#access-list 101 permit tcp any any eq 23
RSR-A(config)#access-list 102 permit ip 172.16.1.0 0.0.0.255 any
```

2. Configure rate-limit to mark traffic classes.

```
RSR-A(config)#interface gigabitEthernet 0/1        //Accesses the interface requiring the marking
policy
RSR-A(config-if-GigabitEthernet 0/1)#rate-limit input access-group 10020000000 2000000 4000000
conform-action set-dscp-transmit 10 exceed-action transmit
RSR-A(config-if-GigabitEthernet 0/1)#rate-limit input access-group 101 20000000 2000000 4000000
conform-action set-dscp-transmit 20 exceed-action transmit
RSR-A(config-if-GigabitEthernet 0/1)#rate-limit input access-group 102 20000000 2000000 4000000
conform-action set-dscp-transmit 30 exceed-action transmit
//Every traffic class is defined with a rate-limit command
```

Notes:

1. The **rate-limit** command is used only for marking in input direction
2. For the **rate-limit** command itself, a rate limit must be set. However, if the interface bandwidth is 2Mbps and the rate limit is set to 20Mbps, it equals to no rate limit because the set value is larger.
3. 

Refer to the empirical values below to configure B and C values.

   B=A/10

   C=A/5

Command interpretation:

```
Ruijie(config-if)# rate-limit { input | output} bps burst-normal burst-max conform-action action
exceed-action action
```

Input|output: expected input/output traffic limit.

Bps: expected traffic rate upper limit (unit: bps).

Burst-normal burst-max: size of the token bucket (unit: bytes).

Conform-action: processing policy for traffic conforming to the rate limit.

Exceed-action: Exceed-action: processing policy for traffic exceeding the rate limit.

Action: The following processing policies are available.

Continue to match the next policy

- Continue: Matches the next policy
- Drop: Drops the packet
- Set-dscp-continue: Sets a DSCP field for the packet, and continues to match the next policy
- Set-dscp-transmit: Sets a DSCP field for the packet, and transmits the packet
- Set-dscp-continue: Sets an IP Precedence field for the packet, and continues to match the next policy
- Set-prec-transmit: Sets an IP Precedence field for the packet, and transmits the packet

- Transmit: Transmits the packet

V. Verification

1. Run the **sho rate-limit interface gigabitEthernet 0/1** command to display the policy applied on the target interface.

```
RSR-A#sho rate-limit interface gigabitEthernet 0/1
GigabitEthernet 0/1
  Input
    matches access-group 100
      params:  20000000 bps, 2000000 limit, 4000000 extended limit
      conformed 0 packets, 0 bytes; action: set dscp transmit
      exceeded 0 packets, 0 bytes; action: transmit
      cbucket 6000000, cbs 6000000; ebucket 0 ebs 0
    matches access-group 101
      params:  20000000 bps, 2000000 limit, 4000000 extended limit
      conformed 0 packets, 0 bytes; action: set dscp transmit
      exceeded 0 packets, 0 bytes; action: transmit
      cbucket 6000000, cbs 6000000; ebucket 0 ebs 0
    matches access-group 102
      params:  20000000 bps, 2000000 limit, 4000000 extended limit
      conformed 0 packets, 0 bytes; action: set dscp transmit
      exceeded 0 packets, 0 bytes; action: transmit
      cbucket 6000000, cbs 6000000; ebucket 0 ebs 0
```

4.7.1.4 PBR

Features:

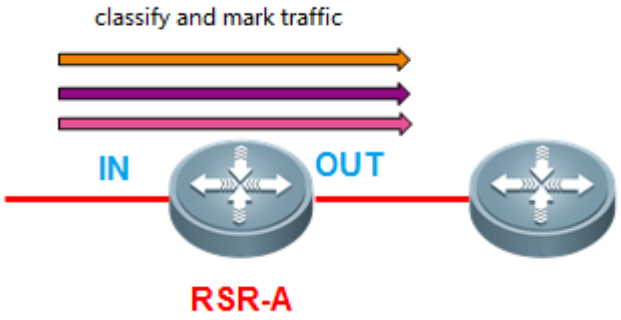
Policy routing is a packet forwarding mechanism that is more flexible than routing based on a target network. Using the policy routing, a device decides how to process the packet to be routed based on the routing map.

I.Networking Requirements

For RSR-A routers, the following data is marked:

1. For VOIP traffic, DSCP priority is 10.
2. For telnet traffic, DSCP priority is 20.
3. For traffic from 172.16.1.0, DSCP priority is 30.

II. Network Topology



III. Configuration Tips

1. Classify traffic by ACL.
2. Define a route-map policy, and mark traffic classes.
3. Apply the route-map policy onthe target interface.

IV. Configuration Steps

1. Classify traffic by ACL.

```
RSR-A(config)#access-list 100 permit udp any any range 16384 32767
RSR-A(config)#access-list 101 permit tcp any any eq 23
RSR-A(config)#access-list 102 permit ip 172.16.1.0 0.0.0.255 any
```

2. Define a route-map policy, and mark traffic classes.

```
RSR-A(config)#route-map ruijie
RSR-A(config-route-map)#match ip address 100
RSR-A(config-route-map)#set ip dscp 10          //Runs the set command to set DSCP or IP Precedence
RSR-A(config-route-map)#match ip address 101
RSR-A(config-route-map)#set ip dscp 20
RSR-A(config-route-map)#match ip address 102
RSR-A(config-route-map)#set ip dscp 30
```

3. Apply the route-map policy on the target interface.

```
RSR-A(config)#interface gigabitEthernet 0/2       //Accesses the target interface and applies the
route-map policy in input direction
RSR-A(config-if-GigabitEthernet 0/1)#ip policy route-map ruijie
```

V. Verification

1. Run the **show ip policy** command to display the policy applied on the target interface.

```
RSR-A#show ip policy
Balance mode: redundance
Interface                               Route map
GigabitEthernet 0/1                     ruijie

RSR-A#show ip policy ruijie
Balance mode: redundance
Interface                               Route map
GigabitEthernet 0/1                     ruijie
```

4.7.2 Congestion Avoidance

4.7.2.1 PQ

Features:

In Priority Queuing (PQ), packets with higher communication priorities can be transmitted prior to packets with lower priorities, so as to ensure timely transmission of packets with higher priorities.

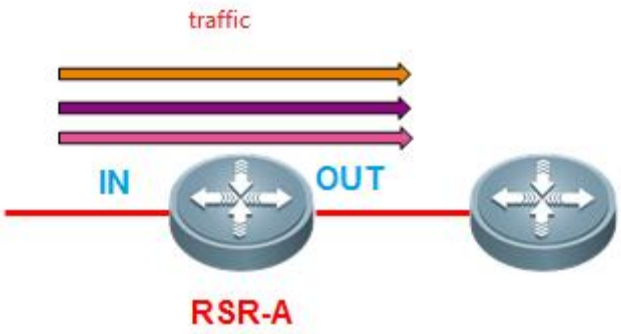
PQ is used to define strict priorities for important network data, and flexibly specify priorities based on network protocols (e.g. IP protocol), lengths of packets at data input interfaces, and source addresses/destination addresses, so as to ensure the fastest processing of the most important network data on network nodes.

I.Networking Requirements

For RSR-A routers, the following data is processed based on priorities in the order of VOIP, telnet, 172.16.1.0 segment, and other traffic.

1. VOIP traffic is provided with the highest priority to ensure low latency.
2. Telnet traffic is provided with a medium priority.
3. Traffic from 172.16.1.0 is provided with a low priority.

II. Network Topology



III. Configuration Tips

1. Classify traffic by ACL.
2. Define a PQ policy.
3. Apply the PQ policy on the target interface.

IV. Configuration Steps

1. Classify traffic by ACL.

```
RSR-A(config)#access-list 100 permit udp any any range 16384 32767
RSR-A(config)#access-list 101 permit tcp any any eq 23
RSR-A(config)#access-list 102 permit ip 172.16.1.0 0.0.0.255 any
```

2. Define a PQ policy.

```
RSR-A(config)#priority-list 1 protocol ip high list 100
RSR-A(config)#priority-list 1 protocol ip medium list 101
RSR-A(config)#priority-list 1 protocol ip normal list 102
```

//NOTE:

1. PQ is classified into four classes in the priority order of high>medium>normal>low.

2. Queuing can be established based on interfaces, for example, priority-list 1 interface gigabitEthernet 0/0 low.

3. Apply the PO policy on the target interface.

```
RSR-A(config)#int gigabitEthernet 0/1
RSR-A(config-if-GigabitEthernet 0/1)#priority-group 1
```

V. Verification

1. Run the **show queue interface *gigabitEthernet 0/1*** command to display the PQ policy applied on the target interface.

```
RSR-A(config)#sho queue interface gi0/1

  Queueing strategy: priority-list 1
  Output queues: (queue #: size/max/send/drops)
  Output queue: high 0/20/0/0, medium 0/40/0/0, normal 0/60/0/0, low 0/80/0/0

  Qos Ref queue information
  Current Policy(s) : PQ
  Queueing strategy: priority-list 1
  interface cir: 1000000000
  Dequeue threshold:  Green 25000, Yellow 37500, Red 50000
  Queues: Queues total len 0, MeanBurst 62501
  Queues: gts gap 0, deta bits 1000, token bucket 25000000
  Queues: Max 9678 pkts, used 0 pkts
  Queues: rtpQ: 0 pkts, 0 bytes
  Queues: llQ:  0 pkts, 0 bytes
  Queues: genQ: 0 pkts, 0 bytes
  Queues: pktQ: 0 pkts, 0 bytes
  Threshold: MeanBurst 62501, Priority LOW, Dec 187503, Inc 187503, Drop 687511
  Counter:   PriInc 0, PriDec 0, Drop 0
  Queues: Queues len 0, MeanBurst 62501, gts token bucket 25000000
  Queues: Max 9678 pkts, used 0 pkts, rtpQ: 0 pkts, 0 bytes. genQ: 0 pkts, 0 byt
es
  (size/max/send/drops)
  high 0/0/0/0, medium 0/0/0/0, normal 0/0/0/0, low 0/0/0/0
```

4.7.2.2 CBWFQ

Features:

Class Based Weighted Fair Queuing (CBWFQ) extends functions of standard Weighted Fair Queuing (WFQ) and supports custom data flow classes. Data flow classes can be defined based on multiple conditions (protocol/ACL/input interface).

CBWFQ can specify the minimum bandwidth guarantee value or proportion for each class based on the policy.

Differences between CBWFQ and LLQ:

(1) CBWFQ is weighted fair, which guarantees the minimum bandwidth but cannot ensure low latency;

(2) Low Latency Queuing (LLQ) is an additional PQ based on CBWFQ, namely, LLQ=CBWFQ+PQ. Latency-sensitive data, such as VOIP, can be placed in PQ to ensure low latency.

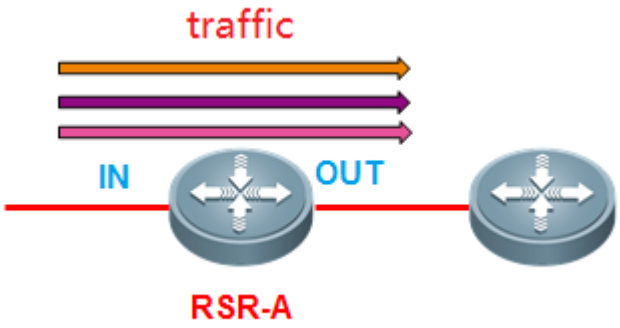
NOTE: Ruijie queuing mechanism has a default queue. All undefined data flows are subject to the default queue. In case of network congestion, the default queue is processed with a low priority by default and occupies the unallocated bandwidth. This is similar to Cisco default queue. However, Cisco default queue needs configuration while Ruijie default queue needs no configuration.

I.Networking Requirements

For RSR-A routers, serial2/1 is the outbound interface and the bandwidth is 2M. The following traffic classes need bandwidth guarantee:

1. Production network traffic is provided with 800Kbps bandwidth guarantee.
2. Office network traffic is provided with 1,000Kbps bandwidth guarantee.

II. Network Topology



III. Configuration Tips

1. Configure a bandwidth proportion for the target interface.
2. Classify traffic by ACL.
3. Define a class mapping list, and associate class-map with ACL.

```
Router(config)#class-map ?
  WORD       class-map name
match-all  Logical-AND all matching statements under this classmap-----------The match condition is "and" (logical "and")
match-any  Logical-OR all matching statements under this classmap-----------The match condition is "or" (logical "or")
Router(config)#class-map ruijie ------------------If only the name is given but match-all or match-any is not indicated, match-all is used by default
```

4. Define a policy mapping list, associate with class-map, and provide class-map with bandwidth guarantee.
5. Apply policy-map on the target interface.

IV. Configuration Steps

1. Configure a bandwidth proportion for the target interface.

```
RSR-A(config)#interface Serial 2/1
RSR-A(config-if - Serial 2/1)#max-reserved-bandwidth 95
```

```
//By default, the total bandwidth allocated to all classes must not exceed 75% of the available bandwidth on the interface. The remaining 25% is used to transmit control data flow and routing data flow. The recommended proportion is 95%-99%, which ensures full use of link bandwidth and the reserved bandwidth used by control packets such as routing and negotiation packets.
```

2. Classify traffic by ACL.

```
RSR-A(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 any     //Define the production network data flow
RSR-A(config)#access-list 101 permit ip 172.16.1.0 0.0.0.255 any       //Define the office network data flow
```

3. Define a class mapping list, and associate class-map with ACL.

```
RSR-A(config)#class-map SC             //Define the production traffic classes. Note that naming is case-sensitive here
RSR-A(config-cmap)#match access-group 100
RSR-A(config-cmap)#class-map BG      //Define the office traffic classes
RSR-A(config-cmap)#match access-group 101
```

4. Define a policy mapping list, associate with class-map, and mark class-map classes.

```
RSR-A(config)#policy-map ruijie
RSR-A(config-pmap)#class SC
RSR-A(config-pmap-c)#bandwidth 800     //The production traffic class is provided with 800Kbps bandwidth guarantee. Bandwidth is the keyword of CBWFQ bandwidth guarantee (Unit: Kbps).
RSR-A(config-pmap-c)#class BG
RSR-A(config-pmap-c)#bandwidth 1000    //Bandwidth proportion may be configured, e.g. bandwidth percent 50
```

5. Apply policy-map on the target interface.

```
RSR-A(config)#interface Serial 2/1
RSR-A(config-if - Serial 2/1)#service-policy output ruijie       //Queue scheduling, which can only be applied in output direction
```

V. Verification

1. Run the **show policy-map interface *Serial 2/1*** command to display the CBWFQ policy applied on the target interface.

```
Ruijie#sh policy-map interface gigabitEthernet 0/1
 Policy-map Output: 1
  Class 1
   Bandwidth 960 kbps
     conformed 17545 packets, 10103698 bytes
     exceeded 0 packets, 0 bytes
     violated 8988 packets, 11355863 bytes
     cbucket 1010, cbs 128000; ebucket 46 ebs 128000
     gap 9, detabits 491
  Class 2
   Bandwidth 3000 kbps
     conformed 25574 packets, 20688306 bytes
     exceeded 0 packets, 0 bytes
     violated 0 packets, 0 bytes
     cbucket 124720, cbs 128000; ebucket 128000 ebs 128000
     gap 7, detabits 384
```

4.7.2.3 LLQ

Features:

Low Latency Queuing (LLQ) is a feature to bring strict PQ to CBWFQ. LLQ allows traffic with a strict priority to be given preferential treatment and get the bandwidth before services for other CBWFQ queues.

Low Latency Queuing: LLQ applies the absolute priority queuing technology to CBWFQ, thereby mitigating shaking voice. The absolute priority queuing technology is applicable to latency-sensitive data (such as voice and video).This feature allows latency-sensitive data to be sent first.

Though various real-time data flows can be added to PQ, we recommend that the most demanding data such as voice and video be added.

Differences between CBWFQ and LLQ:

(1) CBWFQ is weighted fair, which guarantees the minimum bandwidth but cannot ensure low latency;

(2) LLQ is an additional PQ based on CBWFQ, namely, LLQ = CBWFQ + PQ. Latency-sensitive data, such as VOIP, can be placed in PQ to ensure low latency.

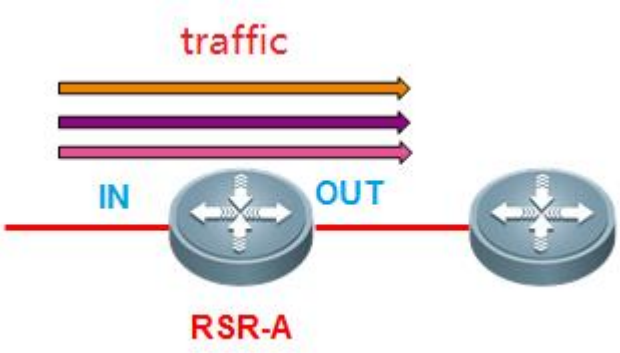
NOTE: Ruijie queuing mechanism has a default queue. All undefined data flows are subject to the default queue. In case of network congestion, the default queue is processed with a low priority by default and occupies the unallocated bandwidth. This is similar to Cisco default queue. However, Cisco default queue needs configuration while Ruijie default queue needs no configuration.

I.Networking Requirements

For RSR-A routers, serial2/1 is the outbound interface and the bandwidth is 2M. The following traffic classes need bandwidth guarantee:

1. Video monitoring needs low latency and 500Kbps bandwidth guarantee.
2. Production traffic network needs 600Kbps bandwidth guarantee.
3. Office network traffic needs 800Kbps bandwidth guarantee.

II. Network Topology



III. Configuration Steps

1. Configure a bandwidth proportion for the target interface.
2. Classify traffic by ACL.
3. Define a class mapping list, and associate class-map with ACL.

```
Router(config)#class-map ?
  WORD       class-map name
match-all  Logical-AND all matching statements under this classmap  ----------The match condition is "and" (logical "and")
match-any  Logical-OR all matching statements under this classmap  ----------The match condition is "or" (logical "or")
Router(config)#class-map ruijie ----------------If only the name is given but match-all or match-any is not indicated, match-all is used by default
```

4. Define a policy mapping list, associate with class-map, and provide class-map with bandwidth guarantee.
5. Apply policy-map on the target interface

IV. Steps

1. Configure a bandwidth proportion for the target interface.

```
RSR-A(config)#interface Serial 2/1
RSR-A(config-if - Serial 2/1)#max-reserved-bandwidth 95
//By default, the total bandwidth allocated to all classes should not exceed 75% of the available bandwidth on the interface. The remaining 25% is used to transmit control data flow and routing data flow. The recommended proportion is 95%-99%, which ensures full use of link bandwidth and the reserved bandwidth used by control packets such as routing and negotiation packets.
```

2. Classify traffic by ACL.

```
RSR-A(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 any     //Define the video network data flow
RSR-A(config)#access-list 101 permit ip 172.16.1.0 0.0.0.255 any       //Define the production network data flow
RSR-A(config)#access-list 102 permit ip 172.16.1.0 0.0.0.255 any       //Define the office network data flow
```

3. Define a class mapping list, and associate class-map with ACL.

```
RSR-A(config)#class-map SP             //Define the video traffic class. Note that naming is case-sensitive here
RSR-A(config-cmap)#match access-group 100
RSR-A(config-cmap)#class-map SC      //Define the production traffic class
RSR-A(config-cmap)#match access-group 101
RSR-A(config-cmap)#class-map BG      //Define the office traffic class
RSR-A(config-cmap)#match access-group 102
```

4. Define a policy mapping list, associate with class-map, and mark class-map classes.

```
RSR-A(config)#policy-map ruijie
RSR-A(config-pmap)#class SP
RSR-A(config-pmap-c)#priority 500          //The video traffic class is provided with 500Kbps bandwidth guarantee. Priority is the keyword of LLQ bandwidth guarantee (Unit: Kbps).
RSR-A(config-pmap)#class SC
RSR-A(config-pmap-c)#bandwidth 600     //The production traffic class is provided with 800Kbps bandwidth guarantee. Bandwidth is the keyword of CBWFQ bandwidth guarantee (Unit: Kbps).
RSR-A(config-pmap-c)#class BG
RSR-A(config-pmap-c)#bandwidth 800    //Bandwidth proportion may be configured, e.g. bandwidth percent 50
```

5. Apply policy-map on the target interface

```
RSR-A(config)#interface Serial 2/1
RSR-A(config-if - Serial 2/1)#service-policy output ruijie       //Queue scheduling, which can be applied only in output direction
```

V. Verification

1. Run the **show policy-map interface *Serial 2/1*** command to display the CBWFQ policy applied on the target interface.

```
Ruijie#sh policy-map interface gigabitEthernet 0/1
 Policy-map Output: 1
  Class 1
   Bandwidth 960 kbps
     conformed 17545 packets, 10103698 bytes
     exceeded 0 packets, 0 bytes
     violated 8988 packets, 11355863 bytes
     cbucket 1010, cbs 128000; ebucket 46 ebs 128000
     gap 9, detabits 491
  Class 2
   Bandwidth 3000 kbps
     conformed 25574 packets, 20688306 bytes
     exceeded 0 packets, 0 bytes
     violated 0 packets, 0 bytes
     cbucket 124720, cbs 128000; ebucket 128000 ebs 128000
     gap 7, detabits 384
```

4.7.3 Traffic Control

I. Differences between rate-control and rate-limit:

1. Rate-control is used for bandwidth and session limits of each user in an ACL while rate-limit is used for overall bandwidth limit with an ACL or an interface as a group. They are different in control objects and granularities.
2. Rate-limit can be used both in input direction and output direction while rate-control is generally used at the egress and applicable to upload and download directions.

II. Differences between GTS and rate-limit:

1. Generic Traffic Shaping (GTS) has a cache mechanism by which packets exceeding the preset traffic are cached and the traffic is made smooth. As rate-limit has no cache mechanism, such packets are dropped directly.
2. GTS functional module is used after the interface queuing mechanism while rate-limit is used before packets enter the queue. As a result, when rate-limit is used, the queuing mechanism remains ineffective while GTS can be combined with the queuing mechanism to form a complete QoS guarantee mechanism.

4.7.3.1 Rate-Limit

Features:

CAR has two features: rate limit and priority setting. CAR statements require both rate limit and IP precedence configurations.

CAR is used to classify packets based on their ToS or CoS values (IP or DSCP precedence for IP packets) and Quintet Vector (protocol port IDs of the source and destination addresses), mark these packets and monitor traffic.

CAR is used in traffic policing, usually for rate limit. Note the difference between rate limit and bandwidth guarantee in the queuing mechanism.

Rate limit means that a traffic class cannot exceed the defined bandwidth value, no matter whether the link has idle bandwidth.

Bandwidth guarantee means that a traffic class can occupy the idle bandwidth or get certain bandwidth guarantee based on policy in case of link congestion.

Scenario

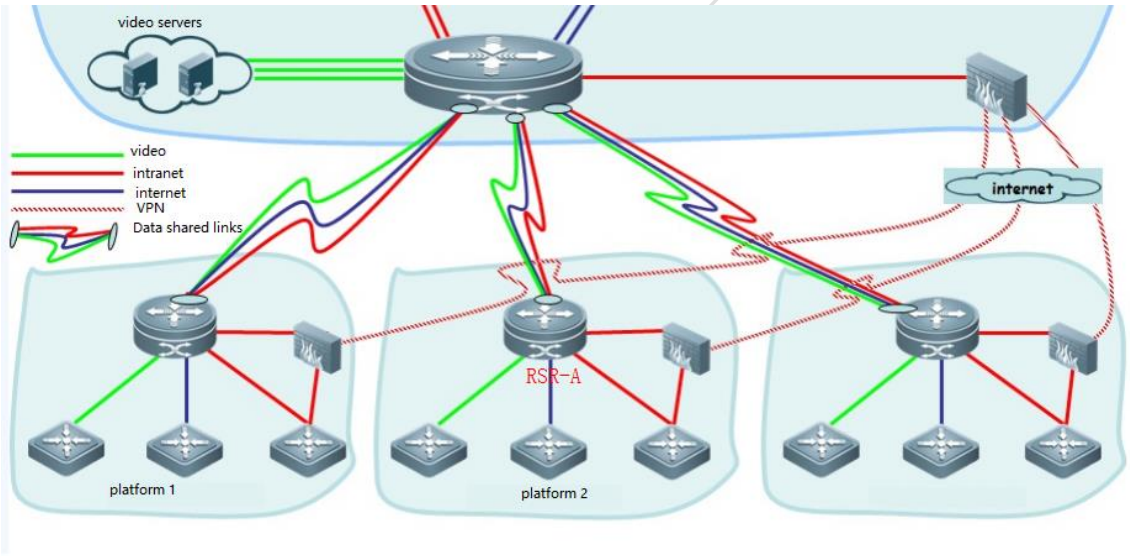
A user needs to limit the traffic rate for an interface. Once the interface traffic exceeds the threshold, the excessive traffic is dropped while the traffic within the threshold is transferred. In this case, the rate-limit feature may be configured.

I.Networking Requirements

RSR-A router, as a network access router, is connected to the headquarters through a 10M MSTP dedicated line. There are 3 sub-interfaces, respectively serving video, intranet data and Internet data. Independent bandwidth is allocated to the three services and must not be occupied:

1. Video connection sub-interface is GI0/0.1 with the rate limit of 2Mbps
2. Intranet connection sub-interface is GI0/0.2 with the rate limit of 3Mbps
3. Internet connection sub-interface is GI0/0.3 with the rate limit of 5Mbps

II. Network Topology



III. Configuration Tips

1. Classify traffic by ACL.
2. Configure rate-limit.

IV. Configuration Steps

1. Classify traffic by ACL.

```
RSR-A(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 any     //Defines the video network data flow
```

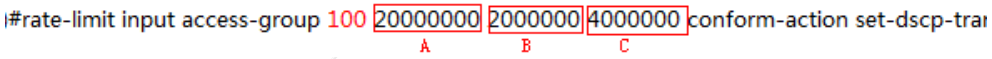
2. Configure rate-limit

```
RSR-A(config)#interface gigabitEthernet 0/0.1        //Accesses the video sub-interface
RSR-A(config-if-GigabitEthernet 0/0.1)#rate-limit output 2000000 200000 400000 conform-action transmit  exceed-action drop
RSR-A(config)#interface gigabitEthernet 0/0.2        //Accesses the intranet sub-interface
RSR-A(config-if-GigabitEthernet 0/0.2)#rate-limit output  3000000 300000 600000 conform-action transmit  exceed-action drop
RSR-A(config)#interface gigabitEthernet 0/0.3        //Accesses the Internet sub-interface
RSR-A(config-if-GigabitEthernet 0/0.3)#rate-limit output  5000000 500000 1000000 conform-action transmit  exceed-action drop
```

//NOTE:

1. This is interface-based rate limit, so it is not necessary to define ACL.

2. The **rate-limit** command is used to configure the limited rate, token bucket and burst rate. Refer to the empirical values below to configure B and C values.

1. 

   B=A/10

   C=A/5

Command interpretation:

```
Ruijie(config-if)# rate-limit { input | output} bps burst-normal burst-max conform-action action
exceed-action action
```

Input|output: expected input/output traffic limit.

Bps: expected traffic rate upper limit (unit: bps).

Burst-normal burst-max: size of the token bucket (unit: bytes).

Conform-action: processing policy for traffic conforming to the rate limit.

Exceed-action: processing policy for traffic exceeding the rate limit.

Action: The following processing policies are available.

Continue to match the next policy

- Continue: Matches the next policy
- Drop: Drops the packet
- Set-dscp-continue: Sets a DSCP field for the packet, and continues to match the next policy
- Set-dscp-transmit: Sets a DSCP field for the packet, and transmits the packet
- Set-dscp-continue: Sets an IP Precedence field for the packet, and continues to match the next policy
- Set-prec-transmit: Sets an IP Precedence field for the packet, and transmits the packet
- Transmit: Transmits the packet

V. Verification

1. Run the **sho rate-limit interface gigabitEthernet 0/0.1** command to display the rate limit applied on the target interface.

```
RSR-A#sho rate-limit interface gigabitEthernet 0/1
GigabitEthernet 0/1
  Input
    matches access-group 100
      params:  20000000 bps, 2000000 limit, 4000000 extended limit
      conformed 0 packets, 0 bytes; action: set dscp transmit
      exceeded 0 packets, 0 bytes; action: transmit
      cbucket 6000000, cbs 6000000; ebucket 0 ebs 0
    matches access-group 101
      params:  20000000 bps, 2000000 limit, 4000000 extended limit
      conformed 0 packets, 0 bytes; action: set dscp transmit
      exceeded 0 packets, 0 bytes; action: transmit
      cbucket 6000000, cbs 6000000; ebucket 0 ebs 0
    matches access-group 102
      params:  20000000 bps, 2000000 limit, 4000000 extended limit
      conformed 0 packets, 0 bytes; action: set dscp transmit
      exceeded 0 packets, 0 bytes; action: transmit
      cbucket 6000000, cbs 6000000; ebucket 0 ebs 0
```

4.7.3.2 Rate-Control

Features:

The purpose of rate control is to prevent a user or an application from occupying too many resources (such as bandwidth). The object is controlled by an ACL in terms of permissible bandwidth, maximum concurrent connections, and new connections per user in a user group. Uplink and downlink bandwidths are controlled respectively. If uplink and downlink bandwidth configurations are the same, the system automatically changes the keyword to both. Concurrent connections and new connection rates are optional.

Differences between rate-control and rate-limit:

1. Rate-control is used for bandwidth and session limits of each user in an ACL while rate-limit is used for overall bandwidth limit with an ACL or an interface as a group. They are different in control objects and granularities.
2. Rate-limit can be used both in input direction and output direction while rate-control is generally used at the egress and applicable to upload and download directions.

Scenario

An enterprise needs to limit the traffic of intranet users and the maximum traffic threshold of each user is the same. Once the traffic of a user exceeds the threshold, the excessive traffic is dropped while the traffic within the threshold is transferred. All users have the same traffic behavior. In this case, the rate-control feature may be configured.

I.Networking Requirements

RSR-A router is used as the egress router of a campus network. Due to the previous unlimited rates, many students use BT/Thunder or other P2P software to download, leading to network congestion and insufficient bandwidth in peak hours. Teachers in the network management center want to limit downloading via the router. They request to ensure the web page opening first while BT is not completely prohibited but cannot occupy large bandwidth;

Two methods can be used to meet the requirements:

Method 1: Limit the bandwidth per user.

This method is direct and easy.

Method 2: Limit sessions via UDP concurrent connection per user.

Characteristics of P2P applications:

UDP protocol is most used to download a file and connection with hundreds of users is created. Independent control of UDP protocol will not affect TCP protocol, so TCP protocol is used by web pages. It is a good way to limit sessions via UDP concurrent connection.

In terms of the second method, the bandwidth per user is set to 2Mb/s, maximum UDP new connections per second are set to 5, and maximum UDP connections are set to 100.

II. Network Topology

III. Configuration Tips

1. Use an ACL to define the user group and protocol requiring rate limit.
2. Configure rate-control to control sessions per user.

IV. Configuration Steps

1. Use an ACL to define the user group and protocol requiring rate limit.

```
RSR-A(config)#ip access-list extended 199
RSR-A(config-ext-nacl)# 5 deny udp any any eq domain     //Domain name resolution (DNS) is the perquisite for opening web pages, so DNS packets must not be limited
DNS packets are limited
```

```
RSR-A(config-ext-nacl)# 20 deny ip any any   //Except DNS packets, other packets are not limited
```

2. Configure rate-control to control sessions per user.

```
RSR-A(config)#interface GigabitEthernet 0/0        //In the egress application, this step is generally used in the outside interface in the NAT environment
RSR-A(config-GigabitEthernet 0/0)#ip rate-control 199 bandwidth both 256
//In an ACL, the uploading and downloading bandwidth of each IP address is 2 MB/S and 256 KB/S respectively.

Session limit is also available, such as ip rate-control 199 bandwidth both 256 session total 100 rate 5        ///In an ACL, the uploading and downloading bandwidth of each IP address is 2 MB/s and 256 KB/S respectively, maximum UDP connections are 100, and maximum UDP new connections per second are 5 (not recommended for actual deployment)
```

V. Verification

1. Run the **show ip rate-control** command to display the rate control policy applied on the target interface.

```
RSR-A#show ip rate-control
Rate Control Rule Configuration
  Interface GigabitEthernet 0/0
      Rate control rule(id:1):
          matching acl 199
          per-user upstream rate limit is 2000 kBps, downstream rate limit is 2000 kBps
          per-user total sessions is 100
          per-user session rate limit is 5
```

4.7.4 Generic Traffic Shaping (GTS)

Features:

Ruijie Generic Traffic Shaping (GTS) can be used for shaping of irregular packet flows or packet flows not conforming to the preset traffic characteristics, so as to facilitate bandwidth matching between upstream and downstream.

GTS is achieved through the packet buffer zone and token bucket. When packet flows are transmitted at a high rate, the packet flows are cached in the buffer zone and then uniformly transmitted under the control of the token bucket.

Differences between GTS and rate-limit:

1. GTS has a cache mechanism by which packets exceeding the preset traffic are cached and the traffic is made smooth. As rate-limit has no cache mechanism, such packets are dropped directly.
2. GTS functional module is used after the interface queuing mechanism while rate-limit is used before packets enter the queue. As a result, when rate-limit is used, the queuing mechanism remains ineffective while GTS can be combined with the queuing mechanism to form a complete QoS guarantee mechanism.

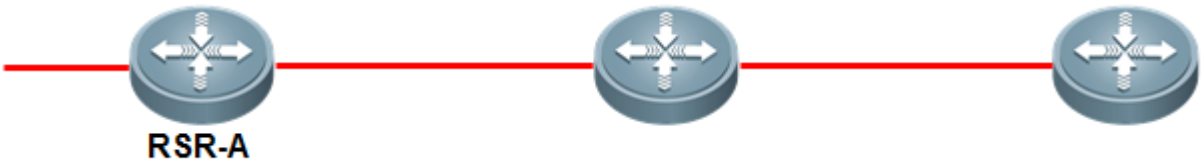
Scenario

When an enterprise rents a dedicated line from Telecom operator, the available bandwidth may be far less than the physical bandwidth on the interface (such as MSTP dedicated line), resulting in packet loss and affecting user experience. We can limit rates by limiting the traffic on the outbound interface to the available bandwidth of the operator, cache the excessive traffic and transfer packets in small traffic.

I.Networking Requirements

RSR-A router serves as a network access router with an MSTP dedicated line as the egress and the bandwidth of 2M.

II. Network Topology



III. Configuration Tips

1. Run the **tracffic-shap** command for traffic shaping on the target interface.

IV. Configuration Steps

1. Run the **tracffic-shaprate** command for traffic shaping on the target interface.

```
RSR-A(config)#interface GigabitEthernet 0/0
RSR-A(config-GigabitEthernet 0/0)#traffic-shape rate 1900000
```

//NOTE:

(1) The configuration value is 1.9Mbps (unit: bps).

(2) Token bucket and burst parameters are optional which will be automatically generated by the system, so manual configuration is not recommended.

```
RSR-A (config-GigabitEthernet 0/0)#traffic-shape rate 2000000 ?
<0-100000000> Bits per interval, sustained
<cr>
```

Tips:

The MSTP link bandwidth provided by the operator is 2Mbps, but the configuration value is 1.9Mbps because the former is a design value. The difference between the design value and the practical value will affect QoS performance. For example, the practical value is 1.9Mbps but GTS configuration value is 2Mbps. When the traffic reaches 1.99Mbps, the queuing mechanism is not effective while 0.09Mbps traffic has been dropped by the operator and packets with a high priority are dropped in equal proportion. In this case, QoS performance cannot be ensured.

2. Empiric value:

   Ethernet link: 95% of the bandwidth provided by the operator

   ATM link: 80% of the bandwidth provided by the operator. NOTE: As QoS is an IP-layer function, after data entering the ATM interface is encapsulated as a cell, extra packet overhead will be incurred. Therefore, if ATM bandwidth is 10Mbps and GTS rate limit is 8Mbps, the overhead is approximately 10Mbps together with the ATM cell.

V. Verification

1. Run the **sho queue interface *gigabitEthernet 0/0***command to display the policy applied on the target interface.

```
RSR-A(config)#sho queue interface gigabitEthernet 0/0

  Queueing strategy: fifo
  Output queue 0/40/264/0 (size/max/send/drops)

  Qos Ref queue information
  Current Policy(s) : GTS
  Queueing strategy: FIFO
  interface cir: 1900000
  Dequeue threshold:  Green 25000, Yellow 37500, Red 50000
  Queues: Queues total len 0, MeanBurst 800
  Queues: gts gap 8, deta bits 486, token bucket 47500
  Queues: Max 19357 pkts, used 0 pkts
  Queues: rtpQ: 0 pkts, 0 bytes
  Queues: llQ:  0 pkts, 0 bytes
  Queues: genQ: 0 pkts, 0 bytes
  Queues: pktQ: 0 pkts, 0 bytes
```

4.7.5 QoS Implementation Guide

Features:

The implementation of QoS is an integration of "traffic classification and marking", "congestion management (queuing mechanism)" and "traffic shaping" rather than merely the applying of queuing mechanism.

CBWFQ and LLQ must be applied in combination with GTS.

NOTE: Ruijie queuing mechanism has a default queue. All undefined data streams are subject to the default queue. In case of network congestion, the default queue is processed with a low priority by default and occupies the unallocated bandwidth. This

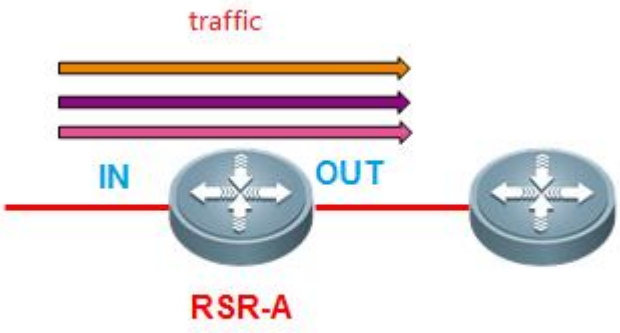
is similar to Cisco default queue. However, Cisco default queue needs configuration while Ruijie default queue needs no configuration.

I.Networking Requirements

RSR-A serves as a financial access router with GI0/0 as the outbound interface, the leased MSTP dedicated line, and the bandwidth of 2M. The following traffic classes must be provided with bandwidth guarantee by LLQ mechanism, and the corresponding traffic must be marked to facilitate control:

1. Video monitoring needs low latency and 500Kbps bandwidth guarantee, and IP precedence is set to 5
2. Production network traffic needs 600Kbps bandwidth guarantee, and IP precedence is set to 4
3. Office network traffic needs 800Kbps bandwidth guarantee, and IP precedence is set to 2

II. Network Topology



III. Configuration Tips

1. Traffic class marking
2. LLQ queuing policy configuration
   (1) Configure a bandwidth proportion.
   (2) Classify traffic by ACL.
   (3) Define a class mapping list, and associate class-map with ACL.
   (4) Define a policy mapping list, associate with class-map, mark class-map classes and apply a QoS policy.
   (5) Apply policy-map on the target interface.
3. GTS configuration

IV. Configuration Steps

a) Traffic class marking

Traffic classes can be marked either in input direction or output direction with the class-map, CAR or PBR method.

In the LLQ or CBWFQ scenario, the class-map method is recommended for marking. Marking is synchronized with LLQ or CBWFQ configuration so as to streamline configuration.

The following procedure marks traffic classes with the class-map method. If other marking methods are needed, refer to the section "Traffic Classification and Marking" (Typical Configuration--->QoS--->Traffic Classification and Marking).

2. LLQ queuing policy configuration

(1) Configure a bandwidth proportion.

```
RSR-A(config)#interface GigabitEthernet 0/0
RSR-A(config-GigabitEthernet 0/0)#max-reserved-bandwidth 95
//By default, the total bandwidth allocated to all classes must not exceed 75% of the available bandwidth on the interface. The remaining 25% is used to transmit control data stream and routing data stream. The recommended proportion is 95%-99%, which ensures full use of link bandwidth and the reserved bandwidth used by control packets such as routing and negotiation packets.
```

(2) Classify traffic by ACL.

```
RSR-A(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 any     //Defines the video network data flow
RSR-A(config)#access-list 101 permit ip 172.16.1.0 0.0.0.255 any       //Defines the production network data flow
RSR-A(config)#access-list 102 permit ip 172.16.1.0 0.0.0.255 any       //Defines the office network data flow
```

(3) Define a class mapping list, and associate class-map with ACL.

```
RSR-A(config)#class-map SP            //Define the video traffic class. Note that naming is case-sensitive here
RSR-A(config-cmap)#match access-group 100
RSR-A(config-cmap)#class-map SC      //Define the production traffic class
RSR-A(config-cmap)#match access-group 101
RSR-A(config-cmap)#class-map BG      //Define the office traffic class
RSR-A(config-cmap)#match access-group 102
```

(4) Define a policy mapping list, associate with class-map, mark class-map classes and apply a QoS policy.

```
RSR-A(config)#policy-map ruijie
RSR-A(config-pmap)#class SP
```

```
RSR-A(config-pmap-c)#priority 500    //The video traffic class is provided with 500Kbps bandwidth guarantee. Priority is the keyword of LLQ bandwidth guarantee (Unit: Kbps).
RSR-A(config-pmap-c)#set ip precedence 5 //Configures IP precedence for bandwidth guarantee ad marking at the same time
RSR-A(config-pmap)#class SC
RSR-A(config-pmap-c)#bandwidth 600     //The production traffic class is provided with 600Kbps bandwidth guarantee. Bandwidth is the keyword of CBWFQ bandwidth guarantee (Unit: kbps).
RSR-A(config-pmap-c)#set ip precedence 4 //Configures IP priority for bandwidth guarantee ad marking at the same time
RSR-A(config-pmap-c)#class BG
RSR-A(config-pmap-c)#bandwidth 800    //Bandwidth proportion may be configured, e.g. bandwidth percent 50
RSR-A(config-pmap-c)#set ip precedence 2   //Configures IP priority for bandwidth guarantee ad marking at the same time
```

(5) Apply policy-map on the target interface.

```
RSR-A(config)#interface GigabitEthernet 0/0
RSR-A(config-if - Serial 0/0)#service-policy output ruijie       //Queue scheduling, which can only be applied in the output direction
```

3. GTS configuration

```
    RSR-A(config-GigabitEthernet 0/0)#traffic-shape rate 1900000
```

//Tips:

(1) Purpose: Gigabit Interface is connected to MSTP, so GI0/0 interface is in Gigabit full-duplex mode.

In case of interface congestion, the queuing mechanism is effective. However, Gigabit Interface here will not be congested, and packets are dropped at the operator end.GTS plays the role of traffic shaping and provides a reference bandwidth for QoS module, namely, the network is congested when the traffic exceeds 2Mbps and the queuing mechanism is scheduled on demand.

(2) The MSTP link bandwidth provided by the operator is 2Mbps, but the configuration value is 1.9Mbps because the former is a design value. The difference between the design value and the practical value will affect QoS performance. For example, the practical value is 1.9Mbps but GTS configuration value is 2Mbps. When the traffic reaches 1.99Mbps, the queuing mechanism is not effective while 0.09Mbps traffic has been dropped by the operator and packets with high priorities are dropped in equal proportion. In this case, QoS performance cannot be ensured.

(3) Empiric value:

Ethernet link: 95% of the bandwidth provided by the operator

ATM link: 80% of the bandwidth provided by the operator. NOTE: As QoS is an IP-layer function, after data entering the ATM interface is encapsulated as a cell, extra packet overhead will be incurred. Therefore, if ATM bandwidth is 10Mbps and GTS rate limit is 8Mbps, the overhead is approximately 10Mbps together with the ATM cell.

//Remarks:

Bandwidth: Remaining available interface bandwidth

Percent: All available interface bandwidth

All available bandwidth: 75% of the interface bandwidth. This proportion may be adjusted with the **max-reserved-bandwidth** command. If GTS traffic-shaping is configured on the interface, all available bandwidth is 75% of the traffic after shaping.

V. Verification

1. Run the **show policy-map interface** command to display LLQ policy on the target interface.

```
Ruijie#sh policy-map interface gigabitEthernet 0/1
 Policy-map Output: 1
  Class 1
   Bandwidth 960 kbps
     conformed 17545 packets, 10103698 bytes
     exceeded 0 packets, 0 bytes
     violated 8988 packets, 11355863 bytes
     cbucket 1010, cbs 128000; ebucket 46 ebs 128000
     gap 9, detabits 491
  Class 2
   Bandwidth 3000 kbps
     conformed 25574 packets, 20688306 bytes
     exceeded 0 packets, 0 bytes
     violated 0 packets, 0 bytes
     cbucket 124720, cbs 128000; ebucket 128000 ebs 128000
     gap 7, detabits 384
```

2. Run the **sho queue interface *gigabitEthernet 0/0***command to display GTS and queue scheduling on the target interface.

```
RSR-A(config)#sho queue interface gigabitEthernet 0/0

  Queueing strategy: fifo
  Output queue 0/40/264/0 (size/max/send/drops)

  Qos Ref queue information
  Current Policy(s) : GTS
  Queueing strategy: FIFO
  interface cir: 1900000
  Dequeue threshold:  Green 25000, Yellow 37500, Red 50000
  Queues: Queues total len 0, MeanBurst 800
  Queues: gts gap 8, deta bits 486, token bucket 47500
  Queues: Max 19357 pkts, used 0 pkts
  Queues: rtpQ: 0 pkts, 0 bytes
  Queues: llQ:  0 pkts, 0 bytes
  Queues: genQ: 0 pkts, 0 bytes
  Queues: pktQ: 0 pkts, 0 bytes
```

5 Solution Configuration Guide

5.1 4G Solutions

5.1.1 4G Products and Common Commands

Ruijie 4G Routers

Ruijie 4G Routers

Ruijie 4G routers fall into two types: box routers and SIC-4G line cards connected to devices. The following is an introduction to the two types of devices.

1. Line Cards of Box Routers

A box router is commonly known as a 4G mobile router with a built-in 4G module and it can be used separately. Box routers inlcude RSR820-T and RSR10-01G-T series. Box routers are divided into specific models by different ISP standards and functions can be simply distinguished by specific models (view the specific model and hardware version on the label of the router base).

The following is the naming rule of Ruijie box routers.

T indicates 4G.

W indicates that WiFi function is supported.

M indicates application in the car scenario.

A indicates that multi-standard 7 communication modes for 2G, 3G, and 4G are supported.

For example, RSR820-TW (MA) indicates that this model has 4G and WiFi functions, is applicable to the car scenario, and supports 7 modes.

2. SIC-4G-LTE Line Cards

A SIC-4G-LTE line card supports 7 modes, namely all communication modes for 2G, 3G, and 4G. A line card cannot be separately used and should be used in combination with an access router host of a specific model. The supported host models include RSR1002E/RSR2004E/RSR20-14E and RSR20-14F. The following is the specific combination.

RSR1002E/RSR2004E: 10.4 (3b35), Release (183253) and later versions are supported. The latest version is recommended. The hardware version of a host is not restricted, that is, a host with any hardware version is supported.

RSR20-14E/F: 10.4 (3b34), Release (183259) and later versions are supported. The latest version is recommended. The hardware version of a host is restricted: Only a hosts with a hardware version latter than V1.2 is supported. A host with hardware V1.1 is not supported

Common Commands

1. 4G Interface Type

All 4G interfaces used by 4G devices are Cellular interfaces. The interfaces of box routers, such as RSR820-T and RSR10-01G-T series, are Cellular 0/0 by default. The interfaces of SIC-4G-LTE are Cellular x/0 (x indicates the slot number of the module).

2. Command Interpretation

1) Configuring the APN number

```
Ruijie(config-if-Cellular0/0)#profile create master apn apn-string        //(Optional) The apn-string is the APNstring assigned by the ISP. For public network dial-up, the APN number is automatically generated.
```

2) Configuring the user name and password

```
Ruijie(config-if-Cellular0/0)#profile create master username uname password 0 pw      //(Optional) It sets the dial-up user name and password to uname and pw.
```

3) Selecting the 4G network access mode

```
Ruijie(config-if-Cellular0/0)# plmn mode  { auto | manual } {cdma-1x|cdma2000 | fdd-lte | gsm | lte | td-lte | td-scdma }     //Configures the ISP access mode. Auto indicates automatic access. Manual indicates compulsory access of a mode without manual selection generally, and 4G is the primary choice.
```

4) Configuring authentication mode switch

```
profile authtype pap_protocol | chap_protocol | papchap_protocol
```

5) Configuring communication link detection

```
Ruijie(config)#ip rns 1
Ruijie(config-ip-rns)#icmp-echo 10.1.1.1 out-interface cellular 0/0
Ruijie(config-ip-rns-icmp-echo)#timeout 1000
Ruijie(config-ip-rns-icmp-echo)#frequency 1000
Ruijie(config)#track 1 rns 1
Ruijie(config-track)#delay down 2
Ruijie(config-track)#delay up 2
Ruijie(config-if-Cellular0/0)#profile create master track track_id
```

//(Recommended) Configuring TRACK enables real-time detection of the communication status of links and initiation of dial-up again after communication interruption to promptly recover the communication of links.

Explanation on the traffic consumed by TRACK configuration:

Note: Configuring TRACK support for link detection may incur extra traffic expenses. The following is the specific calculation formula.

Size of one ICMP request/reply packet = 100 (ICMP header + load) + 20 (IP header) = 120 bytes

Traffic generated in one detection cycle = 120 (ICMP request) + 120 (ICMP reply) = 240 bytes

In case one detection cycle is 10 seconds, traffic generated in one day = 240*6*60*24 = 2073600 bytes = 2.07 MB.

In case one detection cycle is 10 seconds, traffic generated in one month = 2.07*30 = 62.1 MB.

6) Configuring the interesting traffic to trigger dial-up

```
Ruijie(config)# access-list 100 permit ip any host 7.7.7.7
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular 0/0)# apply detect dial-list 100
Ruijie(config-if-Cellular 0/0)# apply dial-on-demand
```

//Configures the interesting traffic to trigger dial-up. ID number 100 in the ACL rule is used as the condition for triggering 4G dial-up, that is, an IP packet with any source IP address and the destination IP address 7.7.7.7 triggers 4G dial-up.

7) Configuring a backup wired link on the 4G interface

```
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular 1)# apply detect interface vlan 10 track 10
Ruijie(config-if-Cellular 1)# apply dial-on-demand
```

//Enables disaster recovery detection on the 4G interface. When the returned status of track object 10 is DOWN, the 4G interface automatically performs dial-up. When the returned status of track object 10 is UP, the 4G interface stops dial-up.

5.1.2 4G Typical Scenario Configuration Guide

4G-based Internet Access Scenario

4G Router as Internet NAT Egress

Features

A 4G router dials in a 4G network of an ISP to provide Internet services for clients connected to the router.

Scenario

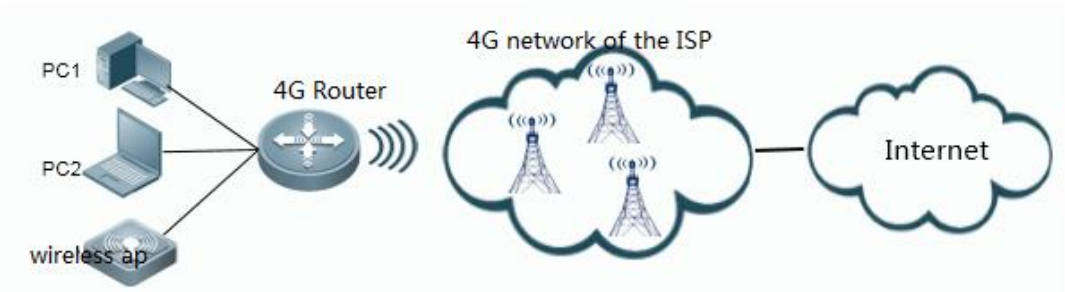
1. Some new communities or remote areas unreachable for ADSL/PON lines of an ISP can access Internet resources via the 4G network.

2. Internet services are needed in mobile scenarios (such as mobile office and on-board WiFi).

I.Networking Requirements

Several intranet users are connected to the 4G router. The 4G router dials in the Internet via 4G to provide Internet access for intranet users.

II. Network Topology



III. Configuration Tips

1. Configure the 4G interface of the router to dial in 4G Internet.
2. Configure a default route.
3. Configure TRACK support for the 4G interface. (Recommended)
4. Configure intranet services (intranet gateway and DHCP).
5. Configure an NAT policy.

IV. Configuration Steps

1. Configure the 4G interface of the router to dial in 4G Internet.

   The 4G router dials in the 4G interface of the Internet without manual configuration. After a 4G card is inserted, the device automatically detects the 4G network type and automatically perform 4G dial-up with the default APN account (APN: cmnet; password: blank).

   Run the **show ip interface** and **show cellular info** commands to check whether dial-up is successful.

2. Configure a default route.

```
ip route 0.0.0.0 0.0.0.0 cellular 0/0
```

3. Configure TRACK support for the 4G interface. (Recommended)

```
ip rns 1
 icmp-echo 8.8.8.8  out-interface celluar0/0  //It is recommended to change the detection address 8.8.8.8 to the local Internet DNS address so as to reduce delay and packet loss and ensure accurate link detection.
```

```
frequency 10000      //The detection frequency is 10 seconds. It can be lowered to increase the switchover speed in case of faults.
timeout 10000      //The detection interval of packet timeout is 10 seconds. It can be lowered to increase the switchover speed in case of faults.
track 1 rns 1
 delay up 30 down 30 //If all detection packets fail to reach the peer end within 30 seconds, the track status is changed to DOWN and dial-up is triggered again. If all detection packets reach the peer end within 30 seconds, the track status is changed to UP.
exit
interface cellular 0/0
profile create master track 1
```

Note: Configuring TRACK support for link detection may incur extra traffic expenses. The following is the specific calculation formula.

Size of one ICMP request/reply packet = 100 (ICMP header + load) + 20 (IP header) = 120 bytes

Traffic generated in one detection cycle = 120 (ICMP request) + 120 (ICMP reply) = 240 bytes

In case one detection cycle is 10 seconds, traffic generated in one day = 240*6*60*24 = 2073600 bytes = 2.07 MB.

In case one detection cycle is 10 seconds, traffic generated in one month = 2.07*30 = 62.1 MB.

In actual application, it is recommended to set the detection cycle to 10 seconds.

4. Configure intranet services (intranet gateway and DHCP).

   a) Configure the intranet gateway.

```
interface vlan 1
 ip address 192.168.1.1 255.255.255.0       //Sets the IP address of the intranet gateway to 192.168.1.1.
```

   b) Configure DHCP services (as required).

```
service dhcp
ip dhcp pool ruijie
network 192.168.1.0 255.255.255.0
dns-server 8.8.8.8  6.6.6.6           //Configures different primary/secondary DNS servers for different ISPs and different provinces.It is recommended to configure the local DNS after confirmation with the ISP, ensuring fast DNS parsing.
default-router 192.168.1.1
ip dhcp excluded-address 192.168.1.1
```

5. Configure an NAT policy.

```
interface vlan 1
```

```
ip nat inside
interface cellular 0/0
ip nat outside
ip access-list standard 10
10 permit 192.168.1.0 0.0.0.255
ip nat inside source list 10 interface cellular 0/0 overload
```

V. Verification

1. On the 3G client router, run the **show ip interface brief** command to confirm that the Cellular interface has obtained the IP address and both "status" and "protocol" are UP.

```
Ruijie#show ip interface brief
Interface        IP-Address(Pri)          IP-Address(Sec)      Status        Protocol
Cellular 0/0      10.230.7.181/32       no address              up              up
//The Cellular interface has obtained the IP address, indicating successful 4G dial-up.
```

2. The router can ping the address of the public network.

```
Ruijie#ping 8.8.8.8
Sending 5, 100-byte ICMP Echoes to 192.168.0.111, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

3. The intranet interface connected to the PC can automatically obtain the IP address, and the PC can access the Internet.

4G-based Internal Private Network Data Intercommunication

Internet-based Networking

Internet-based Video and Data Transmission Solution

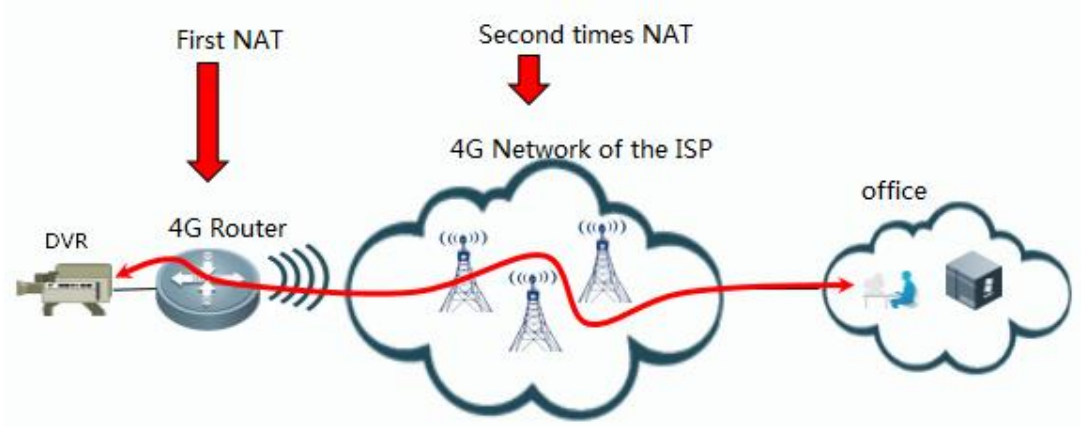
I. Internet-based 4G Router Solution for Video and Data Transmission

A 4G SIM card carried by a 4G router is a public network card of an ISP, namely a common network card. The IP address automatically obtained by the 4G interface is assigned by the ISP. The 4G router uses the public network address to directly communicate with egress devices at the aggregation port via the Internet.

For Internet-based networking, two solutions are available to realize communication between the 4G router and the aggregation center: NAT solution and VPN solution.

NAT Solution:

(The access port can actively access the aggregation port while the aggregation port cannot actively access the access port.)



Advantages: The 4G router only provides basic NAT function and simple deployment. The camera can actively be registered at the upper server through NAT, so that it is managed by the upper end and returns videos.

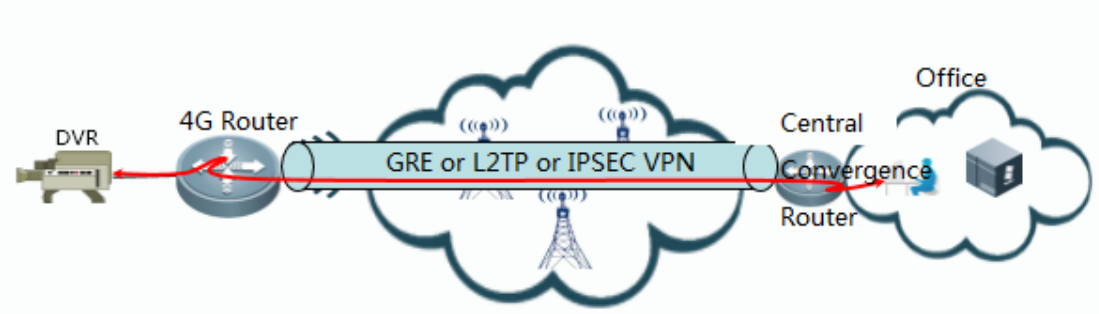
Disadvantages: It is complicated to manage the intranet camera. As the camera passes through double NATs: NAT configured on the 4G router and NAT at the ISP egress (the 4G interface of the 4G router first obtains the internal private network address of the ISP and then translates the private address to access the ISP's Internet), the upper server cannot access or manage the camera directly via the IP address. As all video surveillance device manufacturers have released their own solutions, please confirm the specific solution with DVR vendors.

Networking Requirements:

1. A 4G SIM card is a common SIM card with the Internet function enabled (to dynamically obtain the IP address).
2. The headquarters has an Internet egress with a fixed IP address (if it is a dynamic address, an dynamic domain name should be deployed and the lower camera should support domain name registration).
3. The headquarters is equipped with a video server which is mapped to the Internet on the egress device.

VPN Solution:

(The 4G router and the central aggregation router can access each other.)



Advantages: As the 4G router and upper aggregation router establish a VPN connection, the camera and upper video server are in the same intranet and the IP address of the camera is fixed, which facilitates management.

Disadvantages: The VPN function should be deployed on the 4G router and central aggregation router, and (static or dynamic) routes on both ends should be connected, making deployment and maintenance of the network devices difficult.

Networking Requirements:

1. If L2TP or IPSec VPN is deployed, the 4G SIM card can be a common SIM card with the Internet function enabled (to dynamically obtain the IP address).
2. If GRE VPN is deployed, the 4G SIM card is required to obtain the static IP address of the public network.
3. The headquarters has an Internet egress with a fixed IP address (if it is a dynamic address, an dynamic domain name should be deployed).
4. Egress devices on both ends support VPN (L2TP/IPSec/GRE VPN).

5.1.2.1 NAT Networking Solution (for Video or Data Transmission)

Features

A 4G router dials in a 4G network of an ISP to provide Internet services for cameras connected to the router.

Scenario

Videos need to be returned via the 4G network (the camera actively transmits data to the central server).

I.Networking Requirements

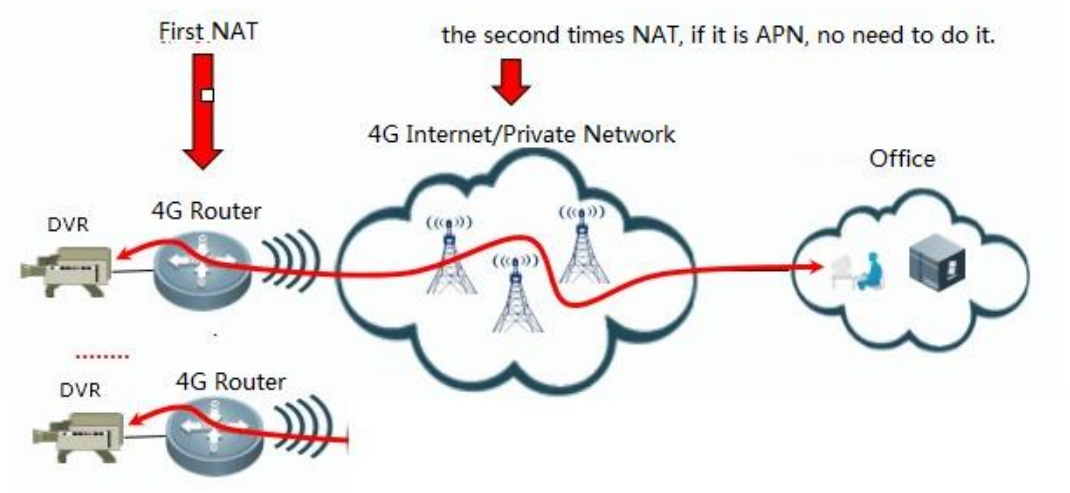
1. The camera can be actively registered at the upper server through NAT, and the upper server can manage it and retrieve videos on it.Note that:
    1) After a common 4G SIM card is used to dial in the Internet, the 4G router first obtains a private network address and passes through double NATs from the camera to the public network. (The IP address obtained is the private network 10.x.x.x. After it is mapped on the 4G router, the camera still cannot be accessed.
    2) As different manufacturers have surveillance devices of different models, confirm with the manufacturer whether a device is applicable in this scenario.
2. A 4G SIM card is a common SIM card with the Internet function enabled (to dynamically obtain the IP address).

3. The headquarters has an egress with a fixed IP address.

   For Internet-based networking, an egress with a fixed IP address is required (if it is a dynamic address, an dynamic domain name should be deployed and the lower camera should support domain name registration).

4. The headquarters is equipped with a video server which is mapped to the Internet on the egress device.

II. Network Topology



III. Configuration Tips

1. Configure the router to dial in the 4G Internet.
2. Configure a default route.
3. Configure TRACK support for the 4G interface. (Recommended)
4. Configure intranet services (intranet gateway and DHCP).
5. Configure an NAT policy.
6. Enable video transmission optimization.

IV. Configuration Steps

1. Configure the router to dial in the 4G Internet.

   The 4G router dials in the 4G interface of the Internet without manual configuration. After a 4G card is inserted, the device automatically detects the 4G network type and automatically perform 4G dial-up with the default APN account (APN: cmnet; password: blank).

   Run the **show ip interface** and **show cellular info** commands to check whether dial-up is successful.

2. Configure a default route.

```
ip route 0.0.0.0 0.0.0.0 cellular 0/0
```

3. Configure TRACK support for the 4G interface. (Recommended)

```
ip rns 1
 icmp-echo 8.8.8.8 out-interface celluar0/0        //It is recommended to change the detection address 8.8.8.8 to the local Internet DNS address or another address directly accessible in APN network so as to reduce delay and packet loss and ensure accurate link detection.
frequency 10000           //The detection frequency is 10 seconds. It can be lowered to increase the switchover speed in case of faults.
timeout 10000       //The detection interval of packet timeout is 10 seconds. It can be lowered to increase the switchover speed in case of faults.
track 1 rns 1
 delay up 30 down 30     //If all link detection packets time out within 30 seconds, the track status is changed to DOWN and dial-up is triggered again. If all link detection packets are received from  the peer within 30 seconds, the track status is changed to UP.
exit
interface cellular 0/0
profile create master track 1
```

Note: Configuring TRACK support for link detection may incur extra traffic expenses. The following is the specific calculation formula.

Size of one ICMP request/reply packet = 100 (ICMP header + Load) + 20 (IP header) = 120 bytes

Traffic generated in one detection cycle = 120 (ICMP request) + 120 (ICMP reply) = 240 bytes

In case one detection cycle is 10 seconds, traffic generated in one day = 240*6*60*24 = 2073600 bytes = 2.07 MB.

In actual application, it is recommended to set the detection cycle to 10 seconds.

4. Configure intranet services (intranet gateway and DHCP).

(1) Configure the intranet gateway.

```
interface vlan 1
 ip address 192.168.1.1 255.255.255.0           //Sets the IP address of the intranet gateway to 192.168.1.1.
```

(2) Configure DHCP services (as required).

```
service dhcp
ip dhcp pool ruijie
network 192.168.1.0 255.255.255.0
dns-server 8.8.8.8  6.6.6.6        //Configures different primary/secondary DNS servers for different ISPs.
default-router 192.168.1.1
```

```
ip dhcp excluded-address 192.168.1.1
```

5. Configure an NAT policy.

```
interface vlan 1
ip nat inside
interface cellular 0/0
ip nat outside
ip access-list standard 10
10 permit 192.168.1.0 0.0.0.255
ip nat inside source list 10 interface cellular 0/0 overload
```

6. Enable video transmission optimization.

   1) Enable video transmission optimization on the 4G router.

```
wan-ta enable //Enables the video transmission optimization function.
ip access-list extended 101 //Defines the video data flow to be optimized from the camera 192.168.1.2 to the server 66.1.1.0.
10 permit ip host 192.168.1.2 66.1.1.0 0.0.0.255
wan-ta policy video  //Configures the video transmission optimization policy. TCP acceleration feature is used by default.
match-port all
interface Cellular 0/0  //Enables the video transmission optimization function on the interface.
wan-ta-policy video list 101
```

   2) Enable the video transmission optimization (WAN-TA+RTP shaping) function on the aggregation router. (Optional for aggregation routers of other vendors)

```
wan-ta enable //Enables the video transmission optimization function.
ip access-list extended 101 //Defines the video data flow to be optimized.
10 permit ip any any
wan-ta policy video
traffic classifier rtp or  //Enables the video shaping function.
  if-match acl 101
traffic behavior rtp
 rtp-shaping delay 2000 clock-rate 90000
traffic policy rtp
 classifier rtp behavior rtp precedence 1
interface GigabitEthernet 1/1/0
wan-ta-policy video list 101
traffic-policy rtp inbound
```

Note: For the detailed video transmission optimization configuration, see Video Transmission Optimization in **Ruijie Router Implementation Manual**.

V. Verification

1. On the 3G client router, run the **show ip interface brief** command to confirm that the Cellular interface has obtained the IP address and both "status" and "protocol" are UP.

```
Ruijie#show ip interface brief
Interface          IP-Address(Pri)                IP-Address(Sec)      Status      Protocol
Cellular 0/0   10.230.7.181/32                     no address           up               up
//The Cellular interface has obtained the IP address, indicating successful 4G dial-up.
```

2. The camera can access the public network.

```
Ruijie#ping 8.8.8.8
Sending 5, 100-byte ICMP Echoes to 192.168.0.111, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

3. The camera can be registered at the video server, and the video server can manage it and retrieve videos on it.

5.1.2.2 [Recommended] L2TP VPN Networking Solution (for Video or Data Transmission)

Features

The branch 4G router dials in the 4G public network and establishes an L2TP VPN connection with the central end to meet the requirement for communication between the branch intranet segment 192.168.1.0 and the headquarters intranet 192.168.2.0.

Scenario

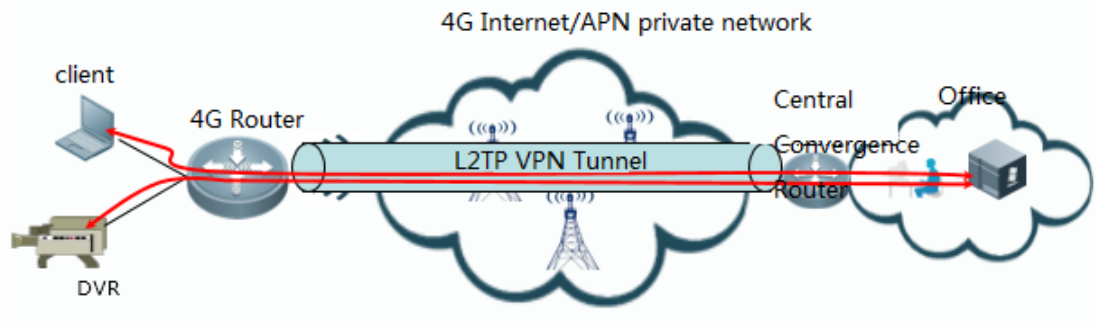
Branches and the headquarters of a company have the requirements for mutual access, for example:

1. The branches and headquarters can access data of each other via the internal private network.
2. The communication between the advertising service system and the central point can be established, so that the headquarters can push advertisements and other information to the service system.
3. Data communication between a financial branch and the headquarters can be established (if no production service is involved, 4G VPDN private network+L2TP+IPSec instead of the 4G Internet is recommended for transportation).

I.Networking Requirements

1. The 4G SIM card can be a common card which obtains the dynamic IP addresses.
2. The headquarters has an Internet egress with a fixed IP address.
3. If it is a dynamic address, an dynamic domain name should be deployed.
4. The egress router of the headquarters supports L2TP VPN

II. Network Topology



III. Configuration Steps

Part I Basic Configuration for the Branch 4G Router

1. Configure the router to dial in the 4G Internet/APN private network.

   After the 4G SIM card is inserted, the device performs automatic dial-up Internet access upon startup without manual configuration.

2. Configure the intranet gateway and DHCP.

```
interface vlan 1
 ip address 192.168.1.1 255.255.255.0       //Sets the IP address of the intranet gateway to 192.168.1.1.
  service dhcp
  ip dhcp pool ruijie
  network 192.168.1.0 255.255.255.0
  dns-server 8.8.8.8 114.114.114.114     //Configures the primary DNS (8.8.8.8) and secondary DNS
(6.6.6.6) based on the actual condition.
  default-router 192.168.1.1
  ip dhcp excluded-address 192.168.1.1
```

3. Configure routes for the 4G router.

```
ip route 0.0.0.0 0.0.0.0 cellular 0/0            //Configures a route to the external network interface of
the central end.
ip route 192.168.2.0 255.255.255.0 virtual-ppp 0 //Configures a route to the intranet interface of the
central end.
```

4. Configure L2TP VPN for branch routers and central aggregation routers.

```
l2tp-class l2x
authentication
password ruijie
pseudowire-class pw       // Note: Configure the same tunnel authentication password on the L2TP client as that on the server. Otherwise, L2TP negation fails.
    encapsulation l2tpv2    protocol l2tpv2 l2xinterface Virtual-ppp 1
    ppp pap sent-username test password test    ip address 100.0.0.2 255.255.255.  //If there are multiple branches, the IP addresses of other branches may be assigned in order. If the second solution is adopted, run the ip address negotiate command instead.
pseudowire 10.0.0.1 12 pw-class pw   //10.0.0.1 indicates the public address of the central aggregation router. If the central end uses a domain name, replace the IP address with the domain name and configure the DNS on the device, that is, set the IP name to server x.x.x.x (which indicates the IP address of the domain name server).
```

5. Configure TRACK support for the 4G interface. (Recommended)

```
ip rns 1
 icmp-echo 10.0.0.1 out-interface celluar0/0         //It is recommended to use the public address of the central aggregation router as the detection address so as to reduce delay and packet loss and ensure accurate link detection.
frequency 3000 //The detection frequency is 3 seconds. It can be lowered to increase the switchover speed in case of faults.
timeout 3000  //The detection interval of packet timeout is 10 seconds. It can be lowered to increase the switchover speed in case of faults.
track 1 rns 1
 delay up 5 down 5 //If all detection packets time out within 5 seconds, the track status is changed to DOWN and dial-up is triggered again. If all detection packets can be received from peer within 5 seconds, the track status is changed to UP.
exit
interface cellular 0/0
profile create master track 1
```

Note: Configuring TRACK support for link detection may incur extra traffic expenses. The following is the specific calculation formula.

Size of one ICMP request/reply packet = 100 (ICMP header + Load) + 20 (IP header) = 120 bytes

Traffic generated in one detection cycle = 120 (ICMP request) + 120 (ICMP reply) = 240 bytes

In case one detection cycle is 10 seconds, traffic generated in one day = 240*6*60*24 = 2073600 bytes = 2.07 MB.

In actual application, it is recommended to set the detection cycle to 10 seconds.

6. Enable the video transmission optimization function on the 4G router (required for video data transmission).

```
wan-ta enable    //Enables the video transmission optimization function.
ip access-list extended 101  //Defines the video data flow to be optimized from the camera 192.168.1.2 to the server.
10 permit ip host 192.168.1.2 192.168.2.0  0.0.0.255
wan-ta policy video  //Configures the video transmission optimization policy with TCP acceleration feature.
match-port all
interface Cellular 0/0  //Enables the video transmission optimization function on the interface.
wan-ta-policy video list 101
```

Part II Configuring the Central Aggregation Router (take Ruijie RSR routers as an example and see the configuration guides for other vendors' devices)

1. Configure the central aggregation router to access the Internet egress via the dedicated line.

```
inter gi0/0  //Configures the public network interface.
ip add 10.0.0.1 255.255.255.0
inter gi0/1 //Configures the intranet interface.
ip add 192.168.2.1 255.255.255.0
```

2. Configure routes for the central aggregation router.

```
ip route 0.0.0.0 0.0.0.0 gi0/0 10.0.0.2        //Configures a default route for the public network access.
ip route 192.168.1.0 255.255.255.0 100.0.0.2  //Configures a static route to the intranet of branch 1.
```

3. Configure L2TP VPN for the central aggregation router (taking the VPN 1.0 and local authentication as an example).

   1) (Optional) Configure the tunnel authentication user name, password and address pool on the 4G router.

```
ip local pool p1 100.0.0.2 100.0.0.100   //(Optional). If the virtual-ppp interface of the 4G router is set to a fixed IP address, it is not recommended to configure p1 address pool.
username test password test //Configures the user name and password for the 4G router to dial in VPDN, corresponding to the user name and password of the virtual-ppp interface of the 4G router.
```

   2) VPDN tunnel configuration

   ip add 192.168.2.1 255.255.255.0

```
interface loopback 1
   ip address 100.0.0.1 255.255.255.255
interface Virtual-Template 1
```

```
ppp authentication pap chap
ip unnumbered Loopback 1
peer default ip address pool p1       //(Optional). It is configured only when the second solution is adopted and the IP address of the virtual-ppp interface of 4G router is assigned dynamically. If the virtual-ppp interface is configured with a fixed IP address, it is not recommended to configure p1 address pool.
vpdn enable
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
l2tp tunnel authentication
l2tp tunnel password ruijie
```

4. Enable the video transmission optimization (WAN-TA+RTP shaping) function on the aggregation router. (Optional for aggregation routers of other vendors)

```
wan-ta enable //Enables the video transmission optimization function.
ip access-list extended 101 //Defines the video data flow to be optimized.
10 permit ip any any
wan-ta policy video
traffic classifier rtp or  //Enables the video shaping function.
  if-match acl 101
traffic behavior rtp
 rtp-shaping delay 2000 clock-rate 90000
traffic policy rtp
 classifier rtp behavior rtp precedence 1
interface GigabitEthernet 1/1/0
wan-ta-policy video list 101
traffic-policy rtp inbound
```

Note: For the detailed video transmission optimization configuration, see Video Transmission Optimization in Typical Configuration.

V. Verification

1. View the L2TP status on the branch 4G router.

1) After configuration, the branch router automatically initiates L2TP dial-up. If dial-up is successful, run the show ip interface brief command to confirm that the interface is UP and a correct IP address has been obtained.

```
Ruijie#show ip interface brief
Interface                IP-Address(Pri)      IP-Address(Sec)      Status                    Protocol
FastEthernet 0/0         10.0.0.2/24          no address           up                        up
FastEthernet 0/1         no address           no address           down                      down
FastEthernet 5/0         no address           no address           up                        down
Virtual-ppp 1            100.0.0.2/32         no address           up                        up
```

2) View the routing table and confirm that an IP address of the LNS virtual-template interface directly connected to the virtual-ppp interface.

```
Ruijie#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.0.0.0/24 is directly connected, FastEthernet 0/0
C    10.0.0.2/32 is local host.
C    100.0.0.1/32 is directly connected, Virtual-ppp 1
C    100.0.0.2/32 is local host.
```

3) The L2TP client can ping the IP address of the virtual-template interface of the LNS.

```
Ruijie#ping 100.0.0.1
Sending 5, 100-byte ICMP Echoes to 100.0.0.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/10 ms
```

2. View the status of the central aggregation router.

Run the **show vpdn** command to view users that have dialed in.

```
Ruijie#show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name          State  Remote Address  Port  Sessions L2TP Class/
                                                                VPDN Group

77    2     branch               est    10.0.0.2        1701  1        1

LocID       RemID       TunID       Username, Intf/      State    Last Chg
                                    Vcid, Circuit
1           1           77          test, va0            est      02:09:56

%No active PPTP tunnels
```

Supplemental Note:

In the foregoing example, interconnection between intranets of both ends are implemented through a static route. The dynamic routing protocol can also be used. The following is an example:

Solution 2: Dynamic Routing Protocol (taking OSPF as an example)

//When the IP address of the virtual-ppp address of the 4G router is assigned by the central router, a dynamic route is applicable and easy for configuration.

1) Configure the OSPF routing protocol for the central aggregation router.

```
router ospf 1
network 192.168.2.1 0.0.0.0 area 0
network 100.0.0.1 0.0.0.0 area 0    //100.0.0.1 indicates the IP address of the virtual-template interface, namely, the IP address of the unnumber loopback interface in interface configuration mode. Based on the actual requirement, redistribute the central service segment to the OSPF domain via the network or the static route redistribution, so that a branch can learn the service route of the central service segment.
```

2) Configure the OSPF routing protocol for the branch 4G router.

```
router ospf 1
network 100.0.0.0 0.0.0.255  area 0 //Indicates the address segment of the virtual-ppp interface.
redistribute connected subnets 或 network 192.168.1.0 255.255.255.0 //Advertises the intranet address route of the 4G router.
```

5.1.2.3 IPSec VPN Networking Solution (for Video or Data Transmission)

Features

The branch 4G router dials in the 4G public network and establishes an IPSec VPN connection with the central end to provide encrypted data transmission for a branch and the central end.

Scenario

Branches and the headquarters have the requirements for mutual access. For example:

1. The branches and headquarters access data of each other via the internal private network.
2. The communication between the advertising service system and the central point can be established, so that the headquarters can push advertisements and other information to the service system.
3. Data communication between a financial branch and the headquarters can be established (if no production service is involved, 4G VPDN private network+L2TP+IPSec instead of the 4G Internet is recommended to carry it).

I.Networking Requirements

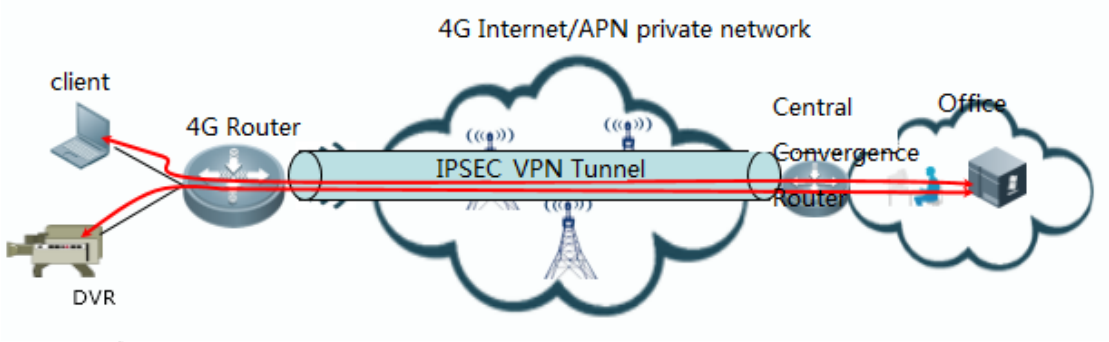
1. The 4G SIM card can obtain the public IP address.

2. The headquarters has an Internet egress with a fixed IP address.

3. If it is a dynamic address, the egress should support the dynamic domain name function.

4. The egress router of the headquarters support IPSec VPN.

II. Network Topology



Network Planning

Network design for the 4G Router	
Ip address of the 4G interface	Interface parameters are assigned by ISP
Internal network address	192.168.1.0/24, gw:192.168.1.1
Network design for the central router	
Ip address of External network interface	10.0.0.1/24, gw:10.0.0.2
Ip address of the internal server	192.168.2.0/24, internal network gw:192.168.2.1
Ip route plan for the internal network	Using reverse routing

IV. Configuration Steps

Part I Basic Configuration for the Branch 4G Router

1. Configure the router to dial in the 4G Internet/APN private network.

After the 4G SIM card is inserted, the device performs automatic dial-up Internet access upon startup without manual configuration.

2. Configure the intranet gateway and DHCP.

```
interface vlan 1
 ip address 192.168.1.1 255.255.255.0        //Sets the IP address of the intranet gateway to
192.168.1.1.
service dhcp
ip dhcp pool ruijie
network 192.168.1.0 255.255.255.0
```

```
dns-server 8.8.8.8 114.114.114.114   //Configures the primary DNS (8.8.8.8) and secondary DNS
(6.6.6.6) based on the actual condition.
default-router 192.168.1.1
ip dhcp excluded-address 192.168.1.1
```

3. Configure routes for the 4G router.

```
ip route 0.0.0.0 0.0.0.0 cellular 0/0       //Configures a route to the external network interface of
the central end.
```

4. Configure IPSec VPN for a branch.

1) Set IPSec interesting traffic to the traffic from the branch 192.168.1.0/24 to the headquarters 192.168.0.0/24.

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

2) Configure the ISAKMP policy.

```
crypto isakmp keepalive 5 periodic
crypto isakmp policy 1
authentication pre-share
encryption 3des
```

3) Configure the pre-shared key.

```
crypto isakmp key 0 ruijie address 10.0.0.1//10.0.0.1      //10.0.0.1 indicates the public address of the
egress of the central aggregation router. If the central end uses the domain name, replace the IP address
with a domain name and configure the DNS on the device, that is, set the IP name to server x.x.x.x (which
indicates the IP address of the domain name server).
```

4) Configure the IPSec encryption transform set.

```
crypto ipsec transform-set mysetesp-des esp-md5-hmac
```

5) Configure the IPSec crypto map.

```
crypto map mymap 5 ipsec-isakmp
set peer 10.0.0.1      //Specifies the IP address of the IPSec center. 10.0.0.1 indicates the public
address of the egress of the central aggregation router. If the central end uses the domain name,
replace the IP address with a domain name and configure the DNS on the device, that is, set the IP
name to server x.x.x.x (which indicates the IP address of the domain name server).
```

```
set transform-set myset
match address 101
set autoup
```

6) Apply the crypto map to the interface.

```
interface cellular 0/0
crypto map mymap
```

5. Configure TRACK support for the 4G interface. (Recommended)

```
ip rns 1
 icmp-echo 10.0.0.1 out-interface celluar0/0          //It is recommended to use the public address of the central aggregation router as the detection address so as to reduce delay and packet loss and ensure accurate link detection.
frequency 3000     //The detection frequency is 3 seconds. It can be lowered to increase the switchover speed in case of faults.
timeout 3000  //The detection interval of packet timeout is 10 seconds. It can be lowered to increase the switchover speed in case of faults.
track 1 rns
1 delay up 5 down 5   //If all detection packets fail to reach the peer end within 5 seconds, the track status is changed to DOWN and dial-up is triggered again. If all detection packets reach the peer end within 5 seconds, the track status is changed to UP.
exit
interface cellular 0/0
profile create master track 1
```

Note: Configuring TRACK support for link detection may incur extra traffic expenses. The following is the specific calculation formula.

Size of one ICMP request/reply packet = 100 (ICMP header + load) + 20 (IP header) = 120 bytes

Traffic generated in one detection cycle = 120 (ICMP request) + 120 (ICMP reply) = 240 bytes

In case one detection cycle is 10 seconds, traffic generated in one day = 240*6*60*24 = 2073600 bytes = 2.07 MB.

In actual application, it is recommended to set the detection cycle to 10 seconds.

6. Enable the video transmission optimization function on the 4G router (required for video data transmission).

```
wan-ta enable    //Enables the video transmission optimization function.
ip access-list extended 101    //Defines the video data flow to be optimized from the camera 192.168.1.2 to the server.
10 permit ip host 192.168.1.2 192.168.2.0  0.0.0.255  //Configures the video transmission optimization policy with TCP acceleration feature.
```

```
match-port all
interface Cellular 0/0  //Enables the video transmission optimization function on the interface.
wan-ta-policy video list 10
```

Part II Configuring the Central Aggregation Router (take Ruijie RSR routers as an example and see the configuration guides for other vendors' devices)

1. Configure the central aggregation router to access the Internet egress via the dedicated line.

```
inter gi0/0      //Configures the public network interface.
ip add 10.0.0.1 255.255.255.0
inter gi0/1       //Configures the intranet interface.
ip add 192.168.2.1 255.255.255.0
```

2. Configure routes for the central aggregation router.

```
ip route 0.0.0.0 0.0.0.0 gi0/0 10.0.0.2      //Configures a default route for the public network access.
```

3. Configure IPSec VPN for the central aggregation router.

1) Configure the ISAKMP policy.

```
crypto isakmp policy 1
 encryption 3des
 authentication pre-share
```

2) Configure the pre-shared key.

```
crypto isakmp key 0 ruijie address 0.0.0.0 0.0.0.0
```

3) Configure IPSec encryption transform set.

```
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

4) Configure the IPSec crypto map.

```
crypto dynamic-map dymymap 5
 set transform-set myset
 reverse-route       //Configures the reverse route injection (RRI) function. If this function is not configured (or not supported by devices of other vendors), deploy the static or dynamic routing protocol on both ends of the IPSec.
```

5) Map the dynamic IPSec crypto map to the static IPSec crypto map.

```
crypto map mymap 10 ipsec-isakmp dynamic dymymap
```

6) Apply the crypto map to the interface (for example, the dedicated line interface G0/0)

```
interface GigabitEthernet 0/0
 crypto map mymap
```

4. Enable the video transmission optimization function. (Recommended. Aggregation routers of other vendors do not have this function.)

```
wan-ta enable     //Enables the video transmission optimization function.
ip access-list extended 101     //Defines the video data flow to be optimized.
10 permit ip any any
wan-ta policy video
traffic classifier rtp or       //Enables the video shaping function.
  if-match acl 101
traffic behavior rtp
 rtp-shaping delay 2000 clock-rate 90000
traffic policy rtp
 classifier rtp behavior rtp precedence 1
interface GigabitEthernet 1/1/0
wan-ta-policy video list 101
traffic-policy rtp inbound
```

V. Verification

1. On the 4G client router, run the **show ip interface brief** command to confirm that the Cellular interface has obtained the IP address and both "status" and "protocol" are UP.

```
Ruijie#show ip interface brief
Interface        IP-Address(Pri)         IP-Address(Sec)      Status      Protocol
Cellular 0/0     10.230.7.181/32      no address                 up           up     //The Cellular
interface has obtained the IP address, indicating successful 4G dial-up.
```

2. Use the source address 192.168.1.1 on the router to ping the headquarters 192.168.2.1.

```
Ruijie#ping 192.168.2.1 source 192.168.1.1
Sending 5, 100-byte ICMP Echoes to 192.168.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

3. IPSec SA has been established on the router.

Successful IPSec tunnel negotiation goes through two stages: successful ISAKMP SA negotiation and IPSec SA negotiation.

```
Ruijie#show crypto isakmp sa
 destination       source              state        conn-id              lifetime(second)
 10.0.0.1         10.230.7.18       1IKE_IDLE        0                        84129    //ISAKMP
negotiation is successful, and the status is IKE_IDLE.
Ruijie#show crypto ipsec sa
......
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 //Indicates the number of packets successfully
encapsulated, encrypted and digested.
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4  //Indicates the number of packets successfully
decapsulated, decrypted and verified. When data is encrypted through IPSec for communication, repeatedly
run the show command.
       Inbound esp sas:
spi:0x2ecca8e (49072782)      //When the inbound esp sas and outbound esp sas are displayed, it indicates
that the IPSec SA negotiation is successful.
        Outbound esp sas:
spi:0x5730dd4b (1462820171)
```

5.1.2.4 4G Router-based Multi Links in Backup Mode

4G link as the backup for the wired dedicated line

Features

The 4G link serves as the backup for a wired line. When the wired line is abnormal, the router promptly switches to the 4G link and resumes services.

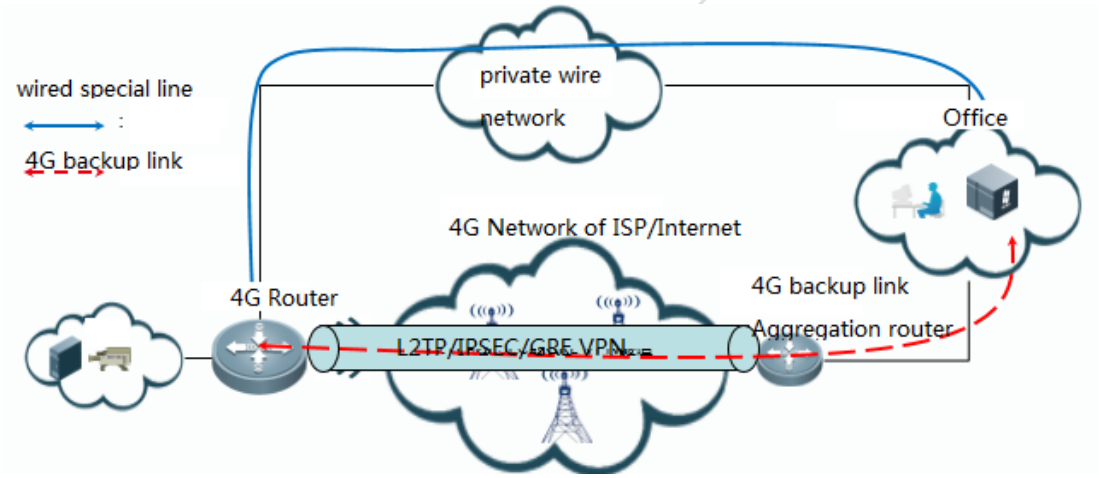
Scenario

Financial branches, chain hotels, and branches of other SMEs have the requirements for backup lines.

I.Networking Requirements

A 4G router wired link and 4G dual links are used for Internet access. The wired link serves as the active link and is connected to the wired network via the GE0 interface belonging to VLAN 2. 4G dual links serve as the backup link. Generally, all links are forwarded via the wired link. When the wired link is abnormal, services are automatically switched to 4G dual links; when the wired link is recovered, services are automatically switched back to the wired link.

II. Network Topology



III. Configuration Tips

1. Configure the central aggregation router as the VPN server.
2. Configure the branch 4G router as the VPN client.
3. Enable wired link connectivity detection on the 4G router.
4. Configure the active/standby routing protocol switch solution.

IV. Configuration Steps

1. Configure the central aggregation router as the VPN server.

Based on the VPN technology chosen, see 4G Typical Scenario Configuration Guide.

2. Configure the branch 4G router as the VPN client.

Based on the VPN technology chosen, see 4G Typical Scenario Configuration Guide.

3. Configure the active/standby routing protocol switch solution.

1) Routing Protocol Switch Solution for the 4G Router

a. Configure a RNS test.

```
 ip rns 10
icmp-echo 50.7.154.1 out-interface VLAN 2  next-hop 50.7.154.1 //Sends packets for detection from the wired interface to check the availability of the wired line. When the Ethernet interface performs a RNS test on a specified interface, detect the reachability of the next-hop address.
timeout 3000                //If an ICMP packet is received in response in 3 seconds, it indicates timeout of the packet.*
frequency 3000              //Indicates that detection packets are sent at intervals of 3s.
ntime 3             //Timeout for three times indicates that the RNS test fails.*
track 10 rns 10
```

```
delay down 3 up 3         /Associates TRACK with an RNS policy. If the RNS test fails, the TRACK status is changed to DOWN with a 3-second delay. If no delay time is configured, the TRACK status is changed to DOWN immediately.*
ip rns 20
icmp-echo 8.8.8.8 out-interface cellulaer 0/0         //Sends packets for detection from the wired interface to check the availability of the wired line. When the Ethernet interface performs an RNS test on a specified interface, detect the reachability of the next-hop address.
timeout 3000                 //If an ICMP packet is received in response in 3 seconds, it indicates timeout of the packet.*
frequency 3000             /Indicates that detection packets are sent in an interval of 3s.
ntime 3              //Timeout for three times indicates that the RNS test fails.*
track 20 rns 20
delay down 3 up 3  //Associates TRACK with an RNS policy. If the RNS test fails, the TRACK status is changed to DOWN with a 3 second delay. If no delay time is configured, the TRACK status is changed to DOWN immediately.*
```

b. Configure a floating default route on the 4G router to control data traffic switch between a wired link and a 4G link.

```
ip route 0.0.0.0 0.0.0.0 VLAN 2  50.7.154.1 track 10            //Configures a default route to direct traffic to the active link interface.
ip route 0.0.0.0 0.0.0.0  Cellular 0/0 100    //Configures a floating default route to direct the traffic to the 4G interface. Due to a low priority, the traffic is not sent from this link when the wired link is available.
```

c. Enable correlation between the wired interface and 4G interface.

```
interface Cellular 0/0
apply detect interface vlan 1 track 10   //Enable disaster recovery detection on the 4G interface. When the returned status of track object 10 is DOWN, the 4G interface automatically performs dial-up. When the returned status of track object 10 is UP, the 4G interface stops dial-up. Multiple detection statements can be configured. In this case, only when the returned status of the track object correlated to each statement is DOWN, the 4G interface performs dial-up. If the returned status of a track object correlated to a statement is UP, the 4G interface stops dial-up.
apply dial-on-demand    //Enables/disables correlation between the wired interface and 4G interface.
profile create master track 20    //Indicates correlation between the interface status and track object 2, which is similar to the keepalive function. When it is enabled, the status of track object 2 is DOWN and the interface performs dial-up again.
```

d. If an IPSec tunnel is configured on the 4G interface, run the following command to disconnect it from the device by force when the wired link is recovered.

```
crypto isakmp link-redundency backup Cellular 0/0 track 10     //When the returned status of track object 10 is UP, the IPSec tunnel on the 4G interface is disconnected by force.
```

e. If the SVI interface is used for wired link detection on the external network interface, it is recommended to run the following command to ensure that status of the SVI interface is changed to DOWN as the status of the layer-2 port is DOWN.*

```
ruijie(config)#svi-interface detecting
```

2) Route Switch Solution for the Headquarters Intranet

Switch the routes from the headquarters intranet to the branch intranet, so that the traffic is sent to the wired dedicated line when the wired link is available or the aggregation router with a 4G backup link when the wired link is abnormal. Multiple solutions are available. The following is a brief description of the configuration.

a. IPSec RRI Solution

The aggregation router with a 4G backup link and the lower end establish an IPSec VPN, and use the RRI function to inject branch routes into the aggregation router. The aggregation router and the intranet run the dynamic routing protocol to advertise branch routes to the headquarters intranet. The priority of a redistributed route should be lower than that of a route from the headquarters intranet to a branch. Priorities can be subject to the weight of a route.

b. Dynamic Routing Protocol for the Whole Network

The aggregation router with a 4G backup link and the 4G router establish an L2TP/GRE VPN, and run the dynamic routing protocol. The aggregation router and the intranet also run the dynamic routing protocol to advertise branch routes to the headquarters intranet. The priority of a redistributed route should be lower than that of a route from the headquarters intranet to a branch. Priorities can be subject to the weight of a route.

V. Verification

1. Generally all services are forwarded via the wired link.
2. Shut down the wired interface or disconnect the wired link. Services are automatically switched to the 4G link.
3. When the wired link is recovered, services are automatically switched back to the wired link.
4. 4G Dual Link Dial-up in Backup Mode

这里漏了标题

Features

One 4G link serves as the backup for the other 4G link. When the active 4G link is abnormal, the router promptly switches to the standby 4G link and resumes services.

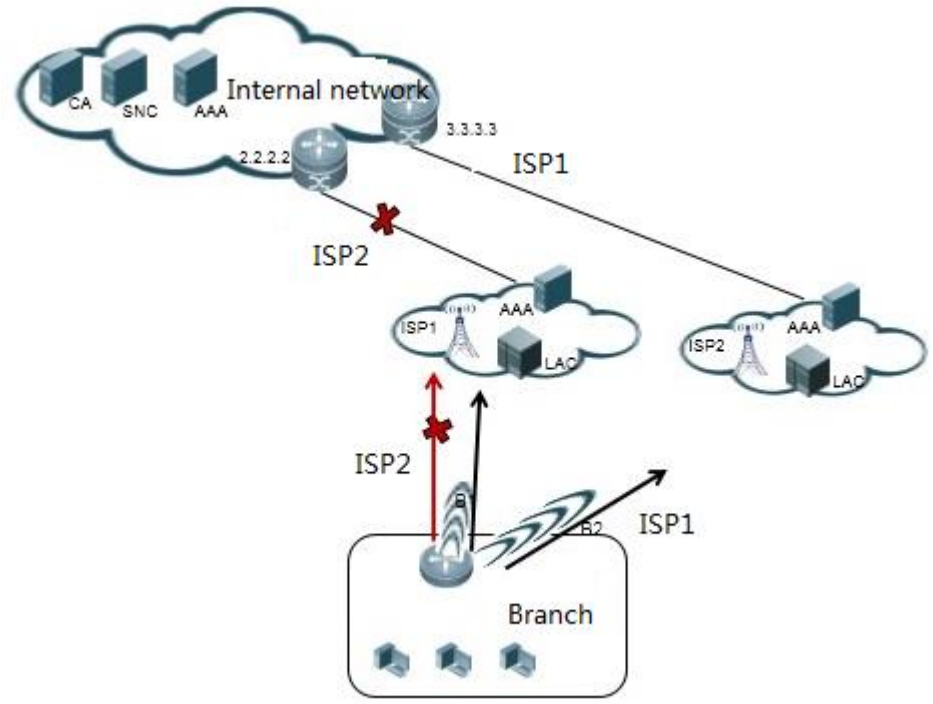
Scenario

Financial branches, chain hotels, and branches of other SMEs have the requirements for backup 4G links.

I.Networking Requirements

The 4G router is connected to the financial aggregation network using dual 4G SIM cards. The active Unicom 4G SIM card Unicom is used to access the network while the standby Mobile 4G SIM card is in backup mode. When the active Unicom link is abnormal, the data is switched to the backup 4G Mobile link; when it is recovered, services are switched back.

II. Network Topology



III. Configuration Tips

1. Configure dual card dial-up for the 4G router.
2. Configure the access mode switch solution for the 4G router.
3. Configure the central aggregation router as the VPN server.

IV. Configuration Steps

1. Configure dual card dial-up for the 4G router.

```
ip rns 1      //Indicates detection of the active Unicom card.
icmp-echo 100.0.0.1 out-interface Cellular  2/0    //100.0.0.1 indicates the IP address of the virtual-template interface on the LNS.
timeout 3000         //The detection timeout interval is 3 seconds.
frequency 3000          //The detection frequency is 3 seconds.
ntime 3              //Status change for three consecutive times is synchronized with the track status.
```

```
ip rns 2       //Indicates detection of the standby Mobile link.
icmp-echo 2.2.2.2 out-interface Cellular 3/0    //2.2.2.2 indicates the IP address of the virtual-template interface on the LNS.
timeout 3000
frequency 3000
ntime 3
track 1 rns 1        //Correlates track object 1 with the status of RNS1.
track 2 rns 2         //Correlates track object 2 with the status of RNS2.
interface Cellular 2/0      //Configures the active card. The cell interface number is identical with the show slot number.
plmn mode manual lte-pref    //Enables 4G priority mode.
profile create master track 1  //Indicates the interface traffic keepalive. When the track status is DOWN, dial-up is performed.
profile create master apn liantong  //Sets the APN to liantong. The APN is provided by customers and ISPs.
profile create master username ruijie@liantong password 0 123  //Configures the user name and password.
interface Cellular 3/0       //Configures the standby card. The cell interface number is identical with the show slot number.
plmn mode manual lte-pref    //Enables 4G priority mode.
profile create master track 2  //Indicates the interface traffic keepalive. When the track status is DOWN, dial-up is performed.
profile create master apn yidong //Sets the APN to yidong. The APN is provided by customers and ISPs.
profile create master username ruijie2@yidong password 0 123  //Configures the user name and password.
```

2. Configure the access mode switch solution for the 4G router.

```
interface Cellular 3/0      //Configures the standby card. The cell interface number is identical with the show slot number.
apply detect interface cellular 2/0 track 1    //Correlates the status of the active interface. When track object 1 of the active interface is DOWN, the standby interface performs dial-up. When track object 1 is UP, the standby stand is changed to the standby status.
apply dial-on-demand       //Enables/disables correlation between the wired interface and 4G interface.
ip route 0.0.0.0 0.0.0.0 Cellular 2/0 track 1     //Correlates the default route of the active link with the status of track object 1. When the status of track object 1 is DOWN, the router does not take effect.
ip route 0.0.0.0 0.0.0.0 Cellular 3/0 100     //Sets the route priority of the backup link to 100.
crypto isakmp link-redundency backup Cellular 3/0 track 1 //When the active link is recovered, the status of track object 1 changes from DOWN to Up. Delete the IPSec on the cell interface to ensure
```

```
that the IPSec inverse route on the aggregation end does not affect a user's selection of the return route.
```

3. Configure the central aggregation router as the VPN server (taking Unicom as an example).

1) Configure the tunnel authentication user name, password and address pool on the 4G router. (Optional)

```
ip local pool p1 100.0.0.2 100.0.0.100  //(Optional) If the virtual-ppp interface of the 4G router is configured set to a fixed IP address, it is not recommended to configure p1 address pool.
username test password test       //Configures the user name and password for the 4G router to dial in VPDN, corresponding to the user name and password of the virtual-ppp interface of the 4G router.
```

2) Configure the VPDN tunnel.

```
interface loopback 1
ip address 100.0.0.1 255.255.255.255
interface Virtual-Template 1
ppp authentication pap chap
ip unnumbered Loopback 1
peer default ip address pool p1     //(Optional) If the intranet AAA server is used to assign IP addresses, configuration for the address pool is optional.
crypto map mymap          //Configures the IPSec map.
vpdn enable
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
l2tp tunnel authentication
l2tp tunnel password ruijie
```

5.1.3 Other Function Configuration for a 4G Router

Video Transmission Optimization Function

Video Transmission Optimization Principle

Features of Video Stream:

Video data features massive data and information and traffic irregularity.

These features pose challenges to its transmission through WiFi. As known to all, the WiFi connection is poor, featuring unstable bandwidth, high delay, jitter, and packet loss ratio. A video server at the sending end sends video frames at regular intervals (one video frame may consist of one or more packets). After transmission through an unstable network, long or short

and irregular delay occurs when video packets reach the receiving end, causing pause or stutter of decoded video images and even reconnection after play interruption.

Problems and Solutions:

Problem			Solution	
Phenomenon	Cause	Technology	Principle	Application
Pixilation, pause, or disconnection	The standard TCP implementation is restricted by the maximum window size (MWS) of 64 or 256 KB. A network with high bandwidth and high delay can make full use of the bandwidth.	TCP window extension (Use the default maximum segment size (MSS) 1460.)	It uses TCP proxy, and extends the MWS. The MSS is 1460.	Access device (Sending end)
	In case of packet loss, the standard TCP implementation is forced to re-transmit the whole windows where packets are lost, causing low efficiency.	Selective recognition and extension (Sack enable is enabled by default.)	It only transmits the lost TCP segments so as to efficiently recover the lost data packets.	Access device (Sending end)
	TCP has a built-in recovery mechanism handling congestion. In case of congestion, the connection throughput rate is immediately lowered by 50%.	Congestion control for delay (Low-bandwidth-delay is enabled by default.)	It uses TCP proxy, and optimizes the congestion control algorithms. Five algorithms are available now.	Access device (Sending end)
Video retrieval, slow start, or timeout occasionally	Many applications use extremely short-term TCP connections. Due to slow TCP start, new TCP connections may be inhibited.	Large initiation window (Use the default init-cwnd 10.)	It enlarges the MSS of the TCP connection, and maximizes the use of the WAN throughput rate. The initial value	Access device (Sending end)

Problem			Solution	
Phenomenon	Cause	Technology	Principle	Application
			of the congestion window is 10 by default.	
Video stutter and disorder	After transmission through a ISP's link, the arrival interval of data packets may be inconsistent and even disorderly.	RTP shaping and caching technology	RTP shaping uses the delay technology to ensure that RTP service packets reach the monitoring end at regular intervals.	Aggregation device (Receiving end)

The complete video transmission optimization solution consists of two parts:

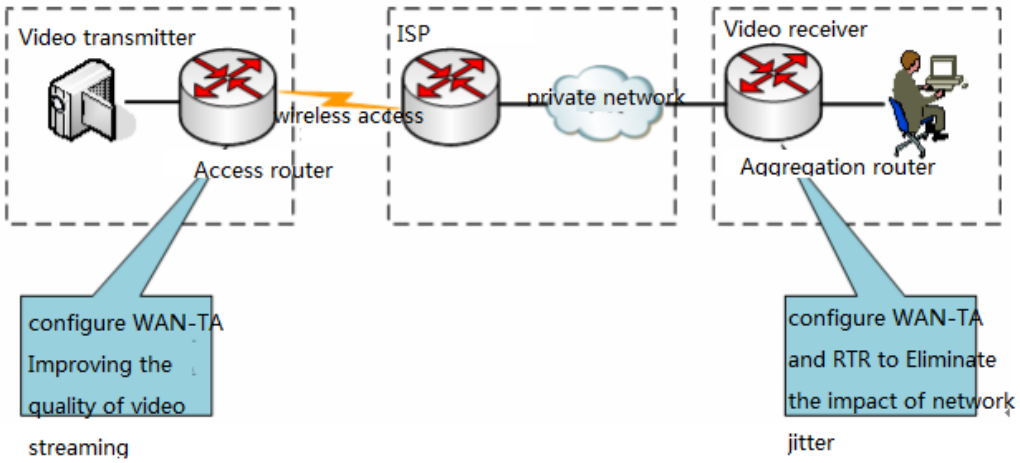
Access Port: WAN-TA

Enable WAN-TA on the access router at the sending end to improve the quality of video transmission.

Receiving End: WAN-TA+RTP

Enable WAN-TA+RTP shaping at the receiving end to eliminate video pause and stutter caused by network jitter.

This solution enables transmitted videos to be played more smoothly without video pause or stutter, improving the video experience.



WAN-TA

WAN Transmission Accelerate (WAN-TA) is a general term for technologies used to improve the efficiency of TCP transmission over a WAN link. To improve the TCP transmission efficiency in the video network transmission environment (video packets are encapsulated in TCP in the online video surveillance system), Ruijie routers introduce some new TCP features based on WAN-TA and apply them to the forwarded data flow so as to improve the performance of TCP transmission over a WAN link.

WAN-TA divides a TCP connection through a Ruijie router into two connections, so that the Ruijie router is used as the terminal device to participate in the TCP session, and the TCP data flow is controlled through the WAN-TA optimization policy configured on the Ruijie router. WAN-TA can eliminate almost all TCP performance bottlenecks without changing the client, server or network features.

RTP Shaping

Adopting the delay technology, RTP shaping is used at the aggregation receiving end to ensure that RTP service packets reach the video client at regular intervals. Based on the WAN-TA function, RTP shaping retrieves packets from the WAN-TA incoming queue, caches video frames in the RTP queue, and sends them one by one in the original timing sequence at regular intervals after a delay (from hundreds of milliseconds to several seconds), so that the video client can receive stable video streams.

Note:

Both WAN-TA and RTP shaping functions are used to improve transmission efficiency rather than increase the link bandwidth. Therefore, neither functions can solve unsmooth video transmission caused by insufficient bandwidth (for example, a 6 Mbps HD video is transmitted over a bandwidth of 4 Mbps).

Configuration for Video Transmission Optimization

Features:

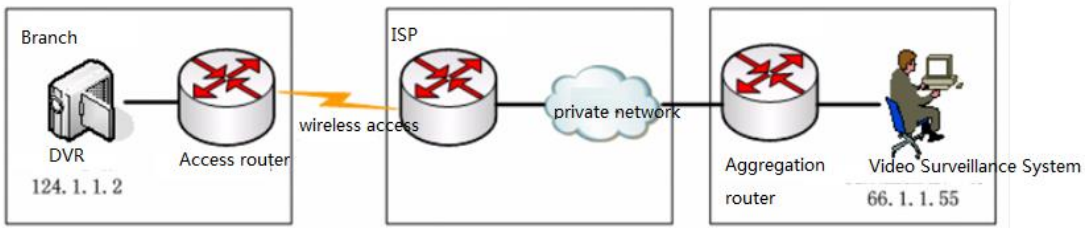
The video transmission optimization solution is mainly used in online video surveillance scenario.

The complete video transmission optimization solution consists of two parts. First, enable WAN-TA on the access router at the sending end to improve the quality of video transmission. Second, enable WAN-TA+RTP at the receiving end to eliminate video pause and stutter caused by network jitter. This solution enables transmitted videos to be played more smoothly without video pause or stutter, improving the video experience.

I.Networking Requirements

1) As shown in the following figure, in the wireless video surveillance scenario, the access router is connected to the digital video server (DVR) in the branch, and the aggregation router is connected to the video client in the headquarters.
2) The access router is connected to the headquarters via the 3G/4G line.
3) The video surveillance client is connected to the branch and headquarters via TCP.

II. Network Topology



III. Configuration Tips

1. Enable WAN-TA on the access port.
2. The video optimization policy is built in the system. Choose **wan-ta policy** video without changing any parameter.
3. Enable WAN-TA+HQOS_RTP on the aggregation port.

IV. Configuration Steps

1. Configuration for the access port (WAN-TA): (basic configuration for 3G dial-up is omitted)

1) Enable video transmission optimization in global configuration mode.

```
wan-ta enable
```

2) Define the video data flow to be optimized.

```
ip access-list extended 101
 10 permit ip host 124.1.1.2 66.1.1.0 0.0.0.255      //Video transmission optimization can be only performed for traffic matching the ACL. Do not set the ACL range to any any. Precisely define the video stream.
```

3) Enable the video transmission optimization policy.

```
wan-ta policy video  //Enables a system-defined policy named "video", which is a default policy without detailed configuration.
match-port xx yy zz.....  //xx yy zz..... indicates the port number used by the manufacturer's device for video transmission. If the port number is unidentified, run the match-port all command, which however affects the device performance because all data connections (both video and non-video) are accelerated.
```

4) Apply the video transmission optimization policy on the interface.

```
interface Async 1
wan-ta-policy video list 101
```

5) Create an empty port-queue rule. (Optional)

```
port-queue 1
```

6) Apply the port-queue rule on the interface. (Optional)

```
interface Async 1
port-queue 1    //Deploys HQOS port-queue, which prevents service interruption during video on demand (VOD) and enables video transmission optimization.
```

2. Configuration for the aggregation port (WAN-TA+RTP): (L2TP configuration is omitted)

1) Enable WAN-TA.

```
wan-ta enable      //Enables WAN-TA (video transmission optimization).
ip access-list extended 101 //Defines the video stream to be optimized using the ACL.
10 permit ip host 124.1.1.2 66.1.1.0 0.0.0.255
wan-ta policy video              //Creates a video transmission optimization policy.
```

2) Define the classfier policy and correlate it with the ACL.

```
traffic classifier rtp or
  if-match acl 101       //Use the same ACL as that used by WAN-TA.
```

3) Define the behavior and configure a RTP shaping policy.

```
traffic behavior rtp
 rtp-shaping delay 2000 clock-rate 90000      //Sets the cache time of RTP video stream to 2 seconds
and the clock frequency to 90000.
```

4) Correlate classfier and behavior and configure an HQOS policy.

```
traffic policy rtp
 classifier rtp behavior rtp precedence 1
```

5) Apply the RTP policy for WAN-TA and HQOS to the interface.

```
interface GigabitEthernet 1/1/0
   wan-ta-policy video list 101
    traffic-policy rtp inbound
```

Note: RTP shaping takes effect only after WAN-TA is enabled, that is, enabling WAN-TA is a prerequisite for RTP shaping.

V. Verification

1. Call the real-time video to compare video effects before and after transmission optimization.
2. Check the configuration of the WAN-TA policy.

```
Ruijie#show wan-ta policy video
wan-ta policy: video
    Congestion Control : low-bandwidth-delay
    SACK Support: TRUE
    Initial Congest Window: 10 MSS
    Maxitum Segment Size: 1460
```

```
    Keepalvie Interval(retry): 120(9)

apply on interfaces:
interface name                              list
GigabitEthernet 2/1/0                    101
```

3. Check the current session.

```
Ruijie#sh wan-ta  policy session  vtty 2/1
session_id  pair     flow                                tcp_state          uptime      service
391         392      [124.1.1.2:554->66.1.1.55:1776]     TCP_ESTABLISHED    0:00:06     RTSP
392         391      [66.1.1.55:1776->124.1.1.2:554]     TCP_ESTABLISHED    0:00:06     RTSP    //The
session ID 392 acts as a proxy for LAN communication between an onsite ATM and an offsite ATM. The session
ID 391 acts as a proxy for WAN communication between a branch and the headquarters.
WiFi Configuration for the 4G Router
```

5.1.4 Configuring WiFi for the 4G Router

4G router supports WLAN 2.4 G frequency band only. The WiFi access terminal belongs to an independent VLAN by default

The configurations are shown as follow:

1) Create VLAN 100 for WiFi.

```
vlan 100
```

2) Configure WLAN ID and SSID.

```
dot11 wlan 1
 wlan-type ap // Set AP configuration mode.
ssid ruijieruijie      //Set SSID to ruijie.
vlan 100        //Correlate it with VLAN 100.
no l2_isolate      //Allow users connected to WiFi to access each other.
```

3) Configure the gateway for the WiFi network segment.

```
interface Dot11radio 2/0.1
 encapsulation dot1Q 100
 ip address 192.168.2.1 255.255.255.0
```

4) Configure a wireless interface and correlate it with a WLAN ID.

```
interface Dot11radio 2/0
```

```
 wlan-id 1
```

5) Set the WiFi password to 12345678 (using WAP2 encryption).

```
wlansec 1
 security rsn enable
 security rsn akm psk set-key ascii 12345678
 security rsn akm psk enable
 security rsn ciphers aes enable
```

6) Configure the DHCP server connected to WiFi.

```
ip dhcp pool AP1_NET_POOL
 network 192.168.2.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.2.1
ip dhcp excluded-address 192.168.2.255
ip dhcp excluded-address 192.168.2.1
```

Note:

For RSR10-01G-T (W) series, if the network segments of WLAN users and LAN users should be in the same subnet, upgrade the router version to RGOS 10.4 (3b64) p1, Release (202782) or a later version. Change the following configuration: WLAN configuratios just keep the same.

```
interface VLAN 2
 ip address 10.7.250.209 255.255.255.240    //Set the IP addresses of the wired and wireless interfaces.
transparent
transparent manage-interface VLAN 2   //Set VLAN2 as the active interface.
interface Dot11radio 2/0.1
 encapsulation dot1Q 2
 transparent
```

5.1.5 4G FAQs and Faults

FAQs

4G FAQs

For RSR10-01G-T series, how to restore factory settings?

As the series have no console port, log in through Web or Telnet. The following are methods for restoring factory settings.

1. Restore factory settings through the Web page.

2. If Web login fails, use the FUNC button on the dashboard to restore factory settings in the following steps:

After the device is powered on, immediately press the FUNC button and release it 10 seconds later. When the device is restarted (the system indicator on the dashboard is steadily on in yellow for two to three seconds), the configuration is cleared. Log in to 192.168.1.1 through Web and enter the password admin. In the pop-up page, choose Clear Configuration to completely clear the configuration of the device.

Note: RGOS 10.4 (3b47), Release (193205) and later versions support this method. For earlier versions, use the FUNC button to upgrade the device to the required version.

6 Device Status Detection

6.1 Check Clock

I. Basic Check

Correct time ensures correct logging time and facilitates fault location. CA certificate and other applications also call for correct time.

Run the **show clock** command to check time:

```
Ruijie#show clock
02:24:23 UTC Thu, Jan 17, 2013
```

II. Check Criteria

Check router time against Beijing time. In case of inconsistency, configure the NTP server or correct time.

6.2 Check Log

I. Basic Check

1) Save logs in the flash

Logs are saved in the memory by default. Due to small memory cache and potential log loss after device restart, save logs in the flash instead. Thus it is easy to find historical logs in case of a fault.

Ruijie(config)#logging file flash:log 2000000 7 //Saves logs in the flash with 2M memory at the level of 7 (all logs including debug messages).

2) Run the **show log** command in privileged EXEC mode to display logs:

```
Ruijie#show logging
Syslog logging: enabled
Console logging: level debugging, 71 messages logged
Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 71 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Count log messages: disable
  Trap logging: level informational, 71 message lines logged,0 fail
Log Buffer (Total 262144 Bytes): have written 6507,
```

3) Run the **more flash:xxx** command to display logs saved in the flash.

II. Check Criteria

Check exceptions in logs, such as, frequent interface UP/DOWN, dynamic protocol DOWN and other high level alarms or tips. If you have any problems, call 4008-111-000.

6.3 Check Hardware Status

I. Basic Check

Run the **show environment** command to check the working status of hardware:

RSR77 routers are taken as an example below. This process is also applicable to other middle-range and high-end devices.

```
RSR7708#show environment
  Environmental status update at 23:4:53 2013-01-16.
  Data is 5 second old, refresh in 30 second(s).
  Power Supplies:                              //working status of power supplies: "on" indicates
normal.
        Power supply 1 is present. Unit is on.
        Power supply 2 is present. Unit is on.
        Power supply 3 is not present. Unit is off.
  Fans working status: OK.                 //working status of fans: "OK" indicates normal.
  Temperature readings:                 //temperature inside the chassis: Pay attention if the
temperature is above 45°C.
        measured at 23 ℃
  Hardware:
        CPU name : Freescale MPC85xx.
        CPU Speed: 1320M
```

II. Check Criteria

1) If the power module displayed is different from the inserted power module, check whether there are any exceptions.

2) If any exceptions occur to the operating environment (for example, temperature), an alarm is displayed. If you have any problems, call 4008-111-000.

6.4 Check CPU Utilization

I. Basic Check

Run the **show cpu** command to check CPU utilization.

```
Ruijie#show cpu
=====================================
     CPU Using Rate Information
CPU utilization in five seconds: 12.12%
CPU utilization in one minute  : 12.07%
CPU utilization in five minutes: 12.07%
```

II. Check Criteria

1) In the normal state, “CPU utilization in five minutes” must remain below 30%. Pay attention if the CPU utilization is above 60%.

2) Extensive configurations, display of extensive information or debugging may result in high CPU utilization. You can stop operations or disable debugging.

3) Heavy network traffic or network attacks may also result in high CPU utilization. Traffic exceptions may result from network attacks.

6.5 Check Memory Utilization

I. Basic Check

Run the **show memory** command to check memory utilization.

```
Ruijie#show memory
System Memory Statistic:
  Free pages: 54998
    watermarks : min 2140, lower 4025, low 5910, high 7795
  System Total Memory : 512MB, Current Free Memory : 225428KB
Used Rate : 57%
```

II. Check Criteria

In the normal state, memory utilization must remain below 60%. The memory utilization rises with an increase in the service load. Pay attention if the memory utilization is above 80%.

NOTE: Due to small memory of RSR10-01G and RSR10-02 routers, the memory utilization may reach 80%-90% in case of service loading. But if the memory utilization remains stable, the device runs normally.

6.6 Check Flow Table Status

I. Basic Check

Note:

The RSR77 router is a distributed system with an independent flow table capacity for every line card. Enter every line card to check flow table statistics.

Run the **show ip fpm statistics** command to check the flow table capacity:

```
Ruijie#show ip fpm statistics
Flow table capacity: 262143      //Indicates flow table capacity
Flow number: 0                   //Indicates the number of flow tables
Nat-flow number: 0               //Indicates the number of entries in the NAT flow table
User number: 0                   /Indicates the number of users
Defragment context number:0      //Indicates the number of fragmented IP packets to be reassembled
Defragment packet number: 0      //Indicates the number of fragmented packets to be reassembled
Event count: 57
```

II. Check Criteria

1) Flow table information may indicate the load state of a device.
2) If the number of entries in the flow table is close to the flow table capacity, traffic or session attacks may exist in the network. Attack sources must be found.

If there are too many fragmented packets in a flow table, fragmented packet attacks may exist in the network. Attack sources must be found.

6.7 Check Interface Status

I. Basic Check

Run the **show interface** command to display the interface status:

```
Ruijie#show interfaces gigabitEthernet 0/0
Index(dec):1 (hex):1
GigabitEthernet 0/0 is UP  , line protocol is UP  //Indicates physical status and protocol status of the interface
Hardware is PQ3 TSEC GIGABIT ETHERNET CONTROLLER GigabitEthernet, address is 001a.a93c.c9f6 (bia 001a.a93c.c9f6)
Interface address is: 10.0.0.3/24
ARP type: ARPA, ARP Timeout: 3600 seconds
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queueing strategy: FIFO
Output queue 0/40, 0 drops; //Indicates packets dropped in output direction
```

```
Output queue 0/75, 0 drops; //Indicates packets dropped in input direction
Link Mode: 100M/Full-Duplex, media-type is twisted-pair.    //Indicates rate, duplex mode, and media type of the interface
  Output flowcontrol is off;Input flowcontrol is off.
5 minutes input rate 79 bits/sec, 0 packets/sec    //Indicates average traffic in input direction in 5 minutes
5 minutes input rate 107 bits/sec, 0 packets/sec    //Indicates average traffic in output direction in 5 minutes
31 packets input, 1860 bytes, 0 no buffer, 0 dropped   //Indicates the traffic and the number of packets dropped in the inbound direction
    Received 31 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort //Indicates error packets in the inbound direction
54 packets input, 2652 bytes, 0 no buffer, 0 dropped   //Indicates the traffic and the number of packets dropped in the outbound direction
0 output errors, 0 collisions, 5 interface resets   //Indicates error packets in the outbound direction
```

II. Check Criteria

1) Check whether traffic on the interface is normal. If the traffic is close to or completely occupy the bandwidth, check whether the bandwidth can meet the existing application or whether any attacks has used up the bandwidth.

2) Check whether the number of CRC errors and the number of dropped packets are large and continuously increase. It may result from poor cable contact or cable aging, or the rate/duplex mode mismatching.

6.8 Basic Fault Information Collection

If a fault cannot be located, you are advised to acquire the following basic information and then call 4008-111-000 for technical support:

```
show version
show run
show clock
show cpu (Run this command once every 5 seconds for 3 times.)
show memory (Run this command once every 5 seconds for 3 times.)
show memory protocols (Run this command once every 5 seconds for 3 times.)
show logging
show slot
show version slot
show arp (Run this command once every 5 seconds for 3 times.)
```

```
show interface (Run this command once every 5 seconds for 3 times.)
show ip route count (Run this command once every 5 seconds for 3 times.)
show ip fpm counters (Run this command once every 5 seconds for 3 times.)
show ip fpm statistics (Run this command once every 5 seconds for 3 times.)
show ip ref adj (Run this command once every 5 seconds for 3 times.)
```

Run the **debug support** command in privileged EXEC mode to enter the support mode.

```
Ruijie#debug support
Ruijie(support)#show exception (Run this command once every 5 seconds for 3 times.)
Ruijie(support)#exit    (NOTE: Exit after running the show exception command.)
```

7 Detailed Case Study

7.1 Detailed Configuration for Internet Access

7.1.1 Internet Access Configuration Guide

RG-RSR10 Router Configuration

RSR10-02E Internet Access Configuration

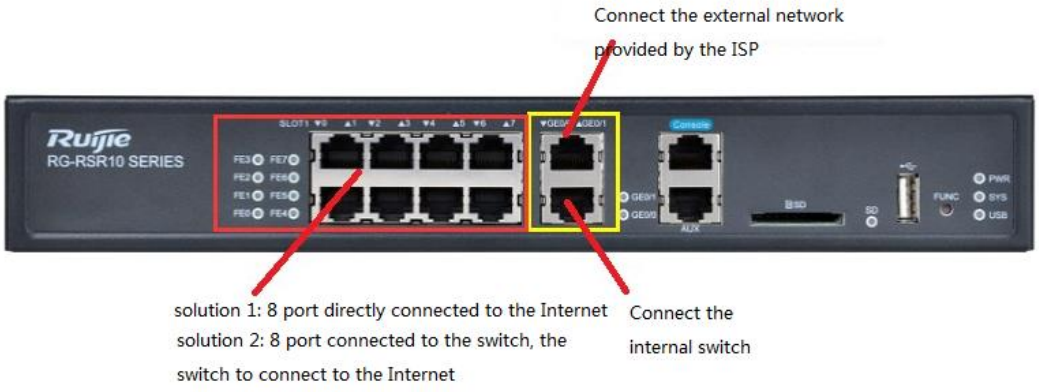
RSR10-02E Device Appearance

Internet Access via a Fixed IP Address Provided by an ISP

Common Networking Scenario:

With a Ruijie router as the egress, the internal PCs access the Internet via a fixed public IP address provided by an ISP.

Network Topology Example:



Configuration Example:

Information provided by the ISP:

The public IP address is 211.11.83.2. The subnet mask is 255.255.255.224. The IP address of the gateway is 211.11.83.1.

The IP address of the primary DNS is 111.11.1.1. The IP address of the secondary DNS is 8.8.8.8.

IP address segment planning for intranet PCs:

1) IP address segment planning for PCs connected to the GE0/0 interface

The address segment is 192.168.10.0/24. The IP address of the gateway is 192.168.10.1.

The IP address of an Intranet PC is automatically obtained via the intranet with the range from 192.168.10.2 to 192.168.10.254.

2) IP address segment planning for PCs connected to eight switching interfaces

The address segment is 192.168.20.0/24. The IP address of the gateway is 192.168.20.1.

The IP address of an Intranet PC is automatically obtained via the intranet with the range from 192.168.20.2 to 192.168.20.254.

Configuration Steps

Log in to device through the console port (see Device Login Method).

1) Configure the external network interface and intranet interface of the router. (Mandatory)

```
inter gi0/1
    ip address 211.11.83.2 255.255.255.224
    ip nat outside
    inter gi0/0
    ip nat inside
    ip add 192.168.10.1 255.255.255.0
    inter vlan 1
    ip nat inside
    ip address 192.168.20.1 255.255.255.0
```

2) Configure NAT. (Mandatory)

```
access-list 100 permit ip any any
    ip nat inside source list 100 interface gi0/1 overload
```

3) Configure a default route. (Mandatory)

```
ip route 0.0.0.0 0.0.0.0 211.11.83.1
```

4) Configure DHCP-based automatic IP address assignment. (Optional)

```
ser dhcp
    ip dhcp pool g0
```

```
    network 192.168.10.0 255.255.255.0
    dns-server 114.114.114.114  8.8.8.8
    default-router 192.168.10.1
  ip dhcp pool vlan1
    network 192.168.20.0 255.255.255.0
    dns-server 114.114.114.114  8.8.8.8
    default-router 192.168.20.1
```

5) Configure the Telnet login password. (Optional)

```
enable password ruijie
    line vty 0 4
    password ruijie
```

6) Save the configuration. (Optional)

```
end
    wr
```

To copy the configuration steps, modify the part in red based on the actual condition and copy them in ruijie> mode.

Internet Access via User Name and Password in PPPoE Mode Provided by an ISP

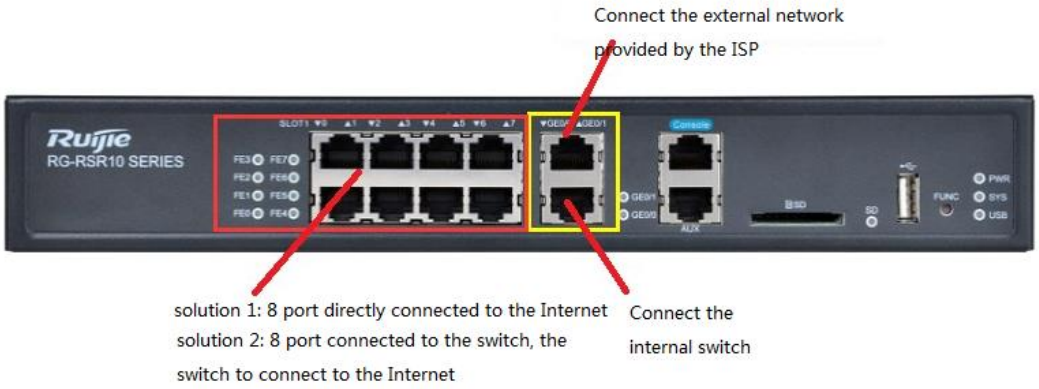
```
en
    conf t

    inter gi0/1
    ip address 211.11.83.2 255.255.255.224
    ip nat outside



    inter gi0/0
    ip nat inside
    ip add 192.168.10.1 255.255.255.0



    inter vlan 1
    ip nat inside
    ip address 192.168.20.1 255.255.255.0
    access-list 100 permit ip any any
    ip nat inside source list 100 interface gi0/1 overload
```

```
   ip route 0.0.0.0 0.0.0.0 211.11.83.1

   ser dhcp
   ip dhcp pool g0
   network 192.168.10.0 255.255.255.0
   dns-server 114.114.114.114  8.8.8.8
   default-router 192.168.10.1
  ip dhcp pool vlan1
   network 192.168.20.0 255.255.255.0
   dns-server 114.114.114.114  8.8.8.8
   default-router 192.168.20.1

enable password ruijie
   line vty 0 4
   password ruijie

   end
   wr
```

Common Networking Scenario:

With a Ruijie router as the egress, the internal PCs access the Internet via a fixed account and password in PPPoE mode provided by an ISP.

Network Topology Example:



Configuration Example:

Information provided by the ISP:

The PPPoE account name is abcd. The password is 1234567.

The IP address of the primary DNS is 111.11.1.1. The IP address of the secondary DNS is 8.8.8.8.

IP address segment planning for intranet PCs:

1) IP address segment planning for PCs connected to the GE0/0 interface

The address segment is 192.168.10.0/24. The IP address of the gateway is 192.168.10.1.

The IP address of an Intranet PC is automatically obtained via the intranet with the range from 192.168.10.2 to 192.168.10.254.

2) IP address segment planning for PCs connected to eight switching interfaces

The address segment is 192.168.20.0/24. The IP address of the gateway is 192.168.20.1.

The IP address of an Intranet PC is automatically obtained via the intranet with the range from 192.168.20.2 to 192.168.20.25.

Configuration Steps

Log in to device through the console port (see Device Log-in Method).

1. Configure the external network interface and intranet interface of the router. (Mandatory)

```
inter gi0/0
    ip add 192.168.10.1 255.255.255.0
    ip nat inside



    inter vlan 1
    ip nat inside
    ip address 192.168.20.1 255.255.255.0



    interface dialer 0
    encapsulation ppp
    ppp chap hostname abcd
    ppp chap password 1234567
    ppp pap sent-username abcd password 1234567
    ip address negotiate
    dialer pool 5
    ip nat outside
    mtu 1492

    inter g0/1
    pppoe enable
    pppoe-client dial-pool-number 5 no-ddr
```

2. Configure NAT. (Mandatory)

```
access-list 100 permit ip any any
    ip nat inside source list 100 interface dialer 0  overload
```

3. Configure a default route. (Mandatory)

```
ip route 0.0.0.0 0.0.0.0 dialer 0
```

4. Configure DHCP-based automatic IP address assignment. (Optional)

```
ser dhcp
    ip dhcp pool g0
    network 192.168.10.0 255.255.255.0
    dns-server 114.114.114.114  8.8.8.8
    default-router 192.168.10.1
  ip dhcp pool vlan1
    network 192.168.20.0 255.255.255.0
    dns-server 114.114.114.114  8.8.8.8
    default-router 192.168.20.1
```

5. Configure the Telnet login password. (Optional)

```
enable password ruijie
    line vty 0 4
    password ruijie
```

6. Save the configuration. (Mandatory)

```
end
    wr
```

To copy the configuration steps, modify the part in red based on the actual condition and copy them in ruijie> mode.

Internet Access via DHCP-based Automatic IP Address Assignment

```
en
    conf t

    inter gi0/0
    ip add 192.168.10.1 255.255.255.0
    ip nat inside
```

```
   inter vlan 1
   ip nat inside
   ip address 192.168.20.1 255.255.255.0


   interface dialer 0
   encapsulation ppp
   ppp chap hostname abcd
   ppp chap password 1234567
   ppp pap sent-username abcd password 1234567
   ip address negotiate
   dialer pool 5
   ip nat outside
   mtu 1492

   inter g0/1
   pppoe enable
   pppoe-client dial-pool-number 5 no-ddr


   access-list 100 permit ip any any
   ip nat inside source list 100 interface dialer 0  overload

   ip route 0.0.0.0 0.0.0.0 dialer 0

   ser dhcp
   ip dhcp pool g0
   network 192.168.10.0 255.255.255.0
   dns-server 114.114.114.114  8.8.8.8
   default-router 192.168.10.1
 ip dhcp pool vlan1
   network 192.168.20.0 255.255.255.0
   dns-server 114.114.114.114  8.8.8.8
   default-router 192.168.20.1

enable password ruijie
   line vty 0 4
   password ruijie

   end
```

```
wr
```

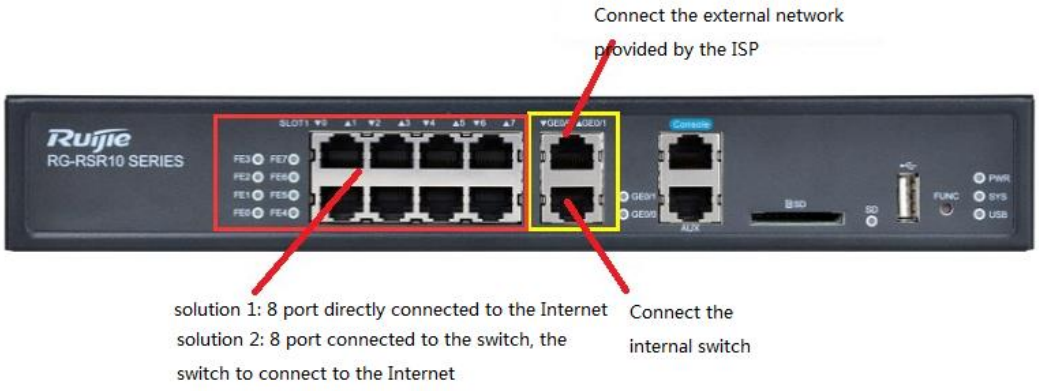
Common Networking Scenario:

Scenario 1: A Ruijie router as the egress is connected to a device of an ISP (which automatically assigns the IP address for the router). Intranet PCs access the Internet via a fixed account and password in PPPoE mode provided by the ISP.

Scenario 2: A Ruijie router as the secondary router is connected to the switch interface of the primary router (which automatically assigns the IP address for the router). Intranet PCs access the Internet via a fixed account and password in PPPoE mode provided by the ISP.

Note: Configuration steps for Scenario 1 and Scenario 2 are the same. Insert the uplink line directly to the PC on which the network card is configured to obtain an IP address automatically, and check whether the PC can access the Internet.

Network Topology Example:



Configuration Example:

An ISP provides a device that can access the Internet (downlink PC that is configured to obtain an IP address automatically to directly access the Internet).

Alternatively,

A shopping mall has a router that can access the Internet, in which a store needs to use Ruijie router for Internet access.

IP address segment planning for intranet PCs:

The address segment is 192.168.10.0/24. The IP address of the gateway is 192.168.10.1.

The IP address of an Intranet PC is automatically obtained via the intranet with the range from 192.168.10.2 to 192.168.10.254.

Configuration Steps

Log in to device through the console port (see Device Log-in Method).

1) Configure the external network interface and intranet interface of the router. (Mandatory)

```
inter gi0/0
    ip add 192.168.10.1 255.255.255.0
```

```
    ip nat inside

    inter vlan 1
    ip address 192.168.20.1 255.255.255.0
    ip nat inside

    inter gi0/1
    ip address dhcp
    ip nat outside
```

2) Configure NAT. (Mandatory)

```
access-list 100 permit ip any any
    ip nat inside source list 100 interface gi0/1  overload
```

3) Configure DHCP-based automatic IP address assignment. (Optional)

```
ser dhcp
    ip dhcp pool g0
    network 192.168.10.0 255.255.255.0
    dns-server 114.114.114.114  8.8.8.8
    default-router 192.168.10.1
  ip dhcp pool vlan1
    network 192.168.20.0 255.255.255.0
    dns-server 114.114.114.114  8.8.8.8
    default-router 192.168.20.1
```

4) Configure the Telnet login password. (Optional)

```
enable password ruijie
    line vty 0 4
    password ruijie
```

5) Save the configuration. (Optional)

```
end
    wr
```

To copy the configuration steps, modify the part in red based on the actual condition and copy them in ruijie> mode.

```
en
    conf t
```

```
  inter gi0/0
  ip add 192.168.10.1 255.255.255.0
  ip nat inside

  inter vlan 1
  ip address 192.168.20.1 255.255.255.0
  ip nat inside

  inter gi0/1
  ip address dhcp
  ip nat outside



  access-list 100 permit ip any any
  ip nat inside source list 100 interface gi0/1  overload

  ser dhcp
  ip dhcp pool g0
  network 192.168.10.0 255.255.255.0
  dns-server 114.114.114.114  8.8.8.8
  default-router 192.168.10.1
  ip dhcp pool vlan1
  network 192.168.20.0 255.255.255.0
  dns-server 114.114.114.114  8.8.8.8
  default-router 192.168.20.1

enable password ruijie
  line vty 0 4
  password ruijie

  end
  wr
```