



Ruijie Networks – Innovation Beyond Networks



RG-Switch Implementation Cookbook

V1.3

Copyright Statement

Ruijie Networks©2013

Ruijie Networks reserves all copyrights of this document. Any reproduction, excerpt, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

 ,  ,  ,  ,  ,
 ,  ,  ,  ,  ,
 ,  are registered trademarks of Ruijie Networks. Counterfeit is strictly prohibited.

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.

Preface

This cookbook is applicable for RG-Switch Implementation Cookbook V1.1

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

- Ruijie Networks Websites : <http://www.ruijienetworks.com>
- Ruijie Service Portal : <http://case.ruijienetworks.com>

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

Revision History

| Date | Change contents | Reviser |
|------------|--------------------------|-------------|
| 2014.05.23 | Initial publication V1.0 | TAC Oversea |

| | | |
|------------|---|--|
| 2017.04.28 | <p>Add new chapter of 1.2.2 Firmware Upgrade for RGOS 11.X, 1.2.2 Reset Password for RGOS 11.X, 2.2.3 Log Filtering, 2.8.2 1X-Web Authentication, 2.8.5 L2 GRE, 2.8.6 VSD, 2.9.1.3 Super VLAN, 2.9.1.4 QinQ, 2.9.2.3 GRE Tunnel, 2.9.3.4 BGP, 2.9.3.5 Route Control, 2.9.3.6 Policy Routing, 2.9.3.7 GR, 3.9.6 QoS, 3.9.8.3 PIM-DM, 3.9.8.4 PIM-SM, 3.9.9 HPOE Function, 3.</p> <p>Hlightlight Function on publication V1.1</p> | |
|------------|---|--|

Contents

| | |
|---|------|
| Preface | 3-1 |
| Contents | 3-3 |
| 1 Installation and Device Management | 3-6 |
| 1.1 System Management | 3-6 |
| 1.1.1 Console Management | 3-6 |
| 1.1.2 Telnet Management | 3-7 |
| 1.1.3 SSH Management | 3-8 |
| 1.1.4 Creating a Management IP Address | 3-10 |
| 1.1.5 Configuring a Default Gateway | 3-11 |
| 1.2 Firmware Upgrade | 3-12 |
| 1.2.1 Firmware Upgrade for RGOS 10.x | 3-12 |
| 1.2.2 Firmware Upgrade for RGOS 11.x | 3-22 |
| 1.2 Password Recovery | 3-27 |
| 1.2.1 Reset Password for RGOS 10.X | 3-30 |
| 1.2.2 Reset Password for RGOS 11.X | 3-32 |
| 1.3 Restore Factory Default | 3-34 |
| 1.3.1 Restore Factory Default for RGOS 10.X | 3-34 |
| 2 Configuration Guide | 3-36 |
| 2.1 Initialization | 3-36 |
| 2.1.1 Overview (Must Read) | 3-36 |
| 2.1.2 Hostname | 3-36 |
| 2.2 Log | 3-37 |
| 2.2.1 Copying log to FLASH | 3-37 |
| 2.2.2 Copying log to Server | 3-39 |
| 2.2.3 Log Filtering | 3-40 |
| 2.3 Clock | 3-44 |
| 2.3.1 Local Clock | 3-44 |
| 2.3.2 NTP | 3-44 |
| 2.4 Configuring a Layer 2 Port | 3-47 |
| 2.4.1 Port Description | 3-47 |
| 2.4.2 Speed, Duplex and Flow control | 3-48 |
| 2.4.3 Combo Port | 3-49 |
| 2.4.4 Access or Trunk Port | 3-52 |
| 2.4.5 Storm Control | 3-54 |
| 2.5 SNMP | 3-55 |
| 2.5.1 SNMPV1/V2 | 3-55 |
| 2.5.2 SNMPV3 | 3-59 |
| 2.6 SPAN | 3-62 |
| 2.6.1 Many to one mirror | 3-62 |

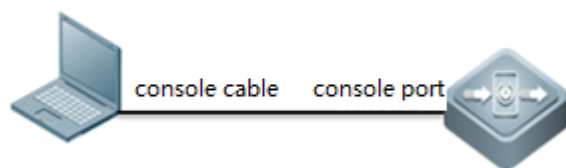
| | | |
|---------|---------------------------------------|-----------|
| 2.6.2 | One to Many Mirror | 3-64 |
| 2.6.3 | Flow-Based Mirroring | 3-67 |
| 2.7 | Featured commands | 3-70 |
| 2.8 | Typical Feature | 3-71 |
| 2.8.1 | VSU | 3-71 |
| 2.8.2 | 1X-Web Authentication | 3-82 |
| 2.8.3 | MSTP+VRRP | 3-89 |
| 2.8.4 | ARP Spoofing Protection | 3-112 |
| 2.8.5 | L2 GRE | 3-129 |
| 2.8.6 | VSD | 3-136 |
| 2.9 | Common Feature | 3-145 |
| 2.9.1 | Ethernet Switching | 3-145 |
| 2.9.2 | IP addressing and Application | 3-183 |
| 2.9.3 | IP Routing | 3-194 |
| 2.9.4 | IPv6 | 3-246 |
| 2.9.5 | Security | 3-261 |
| 3.9.6 | QoS | 3-309 |
| 3.9.7 | Reliability | 3-316 |
| 3.9.8 | Multicast | 3-340 |
| 3.9.9 | HPOE Function | 3-354 |
| 3 | Highlight Functions | 3-357 |
| 3.1 | Highlight Service Functions | 3-357 |
| 3.2 | Highlight Management Function | 3-357 |
| 4 | Best Practice Solution Guide | 4-358 |
| 4.9 | Preparation | 4-358 |
| 4.9.1 | Preparation before Installation | 4-358 |
| 4.9.2 | Check Switch Software/Hardware | 4-358 |
| 4.10 | Best Practic Scenario | 4-362 |
| 4.10.1 | Education | 4-362 |
| 4.11 | Appendix: Common Verification Command | 4-363 |
| 4.11.1 | Show version | 错误!未定义书签。 |
| 4.11.2 | Show run | 错误!未定义书签。 |
| 4.11.3 | Show CPU | 错误!未定义书签。 |
| 4.11.4 | Show memory | 错误!未定义书签。 |
| 4.11.5 | Show power | 错误!未定义书签。 |
| 4.11.6 | Show fan | 错误!未定义书签。 |
| 4.11.7 | Show temperature | 错误!未定义书签。 |
| 4.11.8 | Show clock | 错误!未定义书签。 |
| 4.11.9 | Show log | 错误!未定义书签。 |
| 4.11.10 | Verify flash | 错误!未定义书签。 |
| 4.11.11 | Verify local MAC address | 错误!未定义书签。 |

| | | |
|---------|---|-----------|
| 4.11.12 | Verify MAC table | 错误!未定义书签。 |
| 4.11.13 | Verify ARP table | 错误!未定义书签。 |
| 4.11.14 | Verify route table | 错误!未定义书签。 |
| 4.11.15 | Verify interface IP address | 错误!未定义书签。 |
| 4.11.16 | Verify interface status and description | 错误!未定义书签。 |
| 4.11.17 | Verify interface packets statistics | 错误!未定义书签。 |

1 Installation and Device Management

1.1 System Management

1.1.1 Console Management



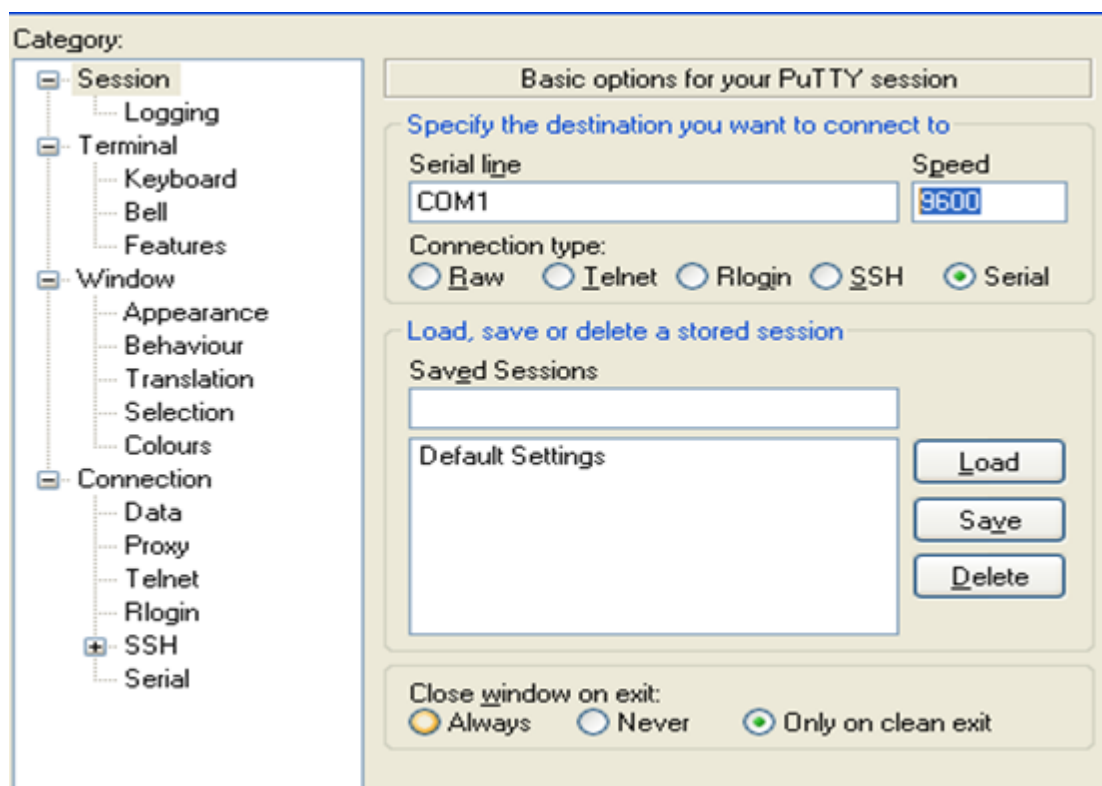
- **Cables**

Console cable, USB to RS232 cable



- **login the device**

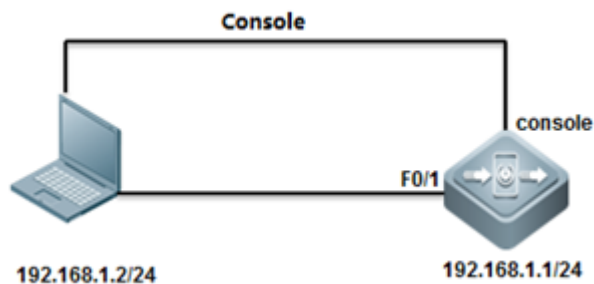
Open your software Putty, set baud rate to 9600



After system prompts "Ruijie>", you can start your configuration

1.1.2 Telnet Management

I. Network Topology



II. Configuration Steps

1. console connect to device and set passwords
2. set ip and gateway

```
ruijie(config)#interface vlan 1
```

```
ruijie(config-if-VLAN 1)#ip address 192.168.1.1 255.255.255.0
ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2
```

3. enable Telnet service

```
ruijie(config)# enable service telnet-server
```

4. set telnet password

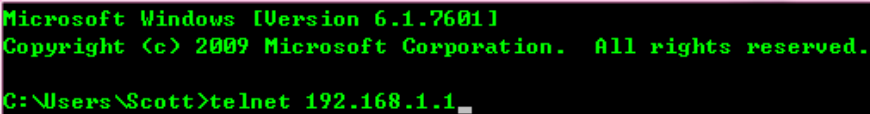
```
ruijie(config)#line vty 0 4
ruijie(config-line)#password ruijie
```

5. set enable password

```
Ruijie(config)#enable password ruijie
```

III. Verification

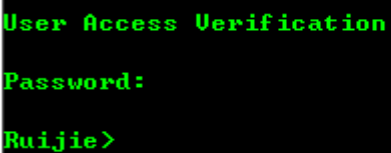
Telnet 192.168.1.1



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Scott>telnet 192.168.1.1_
```

Input telnet password

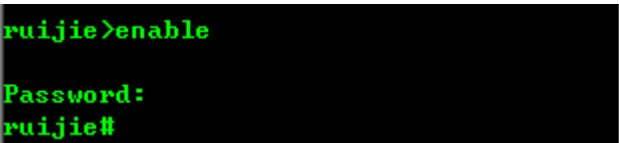


```
User Access Verification

Password:

Ruijie>
```

input enable password

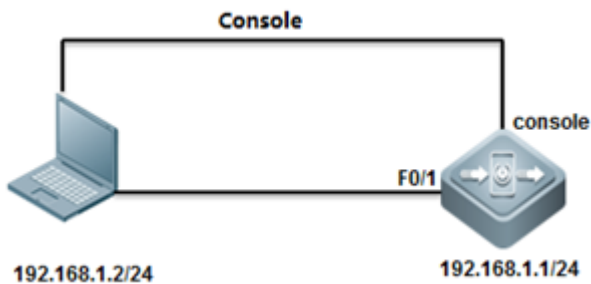


```
ruijie>enable

Password:
ruijie#
```

1.1.3 SSH Management

I. Network Topology



II. Configuration Steps

1. enable SSH service

```
Ruijie#configure terminal
Ruijie(config)#enable service ssh-server
```

2. generate key

```
Ruijie(config)#crypto key generate dsa
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus
greater than 512 may take a few minute
How many bits in the modulus [512]: //press enter
% Generating 512 bit DSA keys ...[ok]
```

3. configure IP address

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

Solution 1: password login

```
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login
Ruijie(config-line)#password ruijie
Ruijie(config-line)#exit
Ruijie(config)#enable password ruijie
Ruijie(config)#end
Ruijie#write
```

Solution 2: username & password login

```
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login local
Ruijie(config-line)#exit
Ruijie(config)#username admin password ruijie
Ruijie(config)#enable password ruijie
```

```
Ruijie(config)#end
Ruijie#write
```

III. Verification

Check SSH service

```
Ruijie#show service
ssh-server      : enabled
telnet-server   : enabled
web-server      : enabled
snmp-agent      : enabled
Ruijie#
```

Check SSH services

```
Ruijie#show ssh
Connection Version Encryption      Hmac      State      Username
      0      2.0 aes256-cbc      hmac-shal Session started admin
Ruijie#
```

Show users

```
Ruijie#show users
Line      User      Host(s)      Idle      Location
  0 con 0
*  1 vty 0      admin      idle      00:00:00      192.168.1.2
Ruijie#
```

1.1.4 Creating a Management IP Address

Creating a Management IP Address

The SVI and router port address can be used as the management address of the layer 3 switch.

Layer 3 Switch:

The address of a layer-3 switch can be configured for management or communication, for example, as the gateway for a user.

Configuration Method 1:

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.1.1 255.255.255.0
Ruijie(config-if-VLAN 10)#end
Ruijie#write
```

Note: To configure the address for VLANs other than VLAN 1 in interface configuration mode, create the corresponding VLAN first; otherwise, a failure prompt is displayed.

Configuration Method 2:

```

Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#int GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)#no switchport ----->configure the port as layer 3 port before configuring ip address
Ruijie(config-if-GigabitEthernet 1/1)#ip add 192.168.16.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 1/1)#end
Ruijie#write ----->save configuration after checking.

```

Verification

```

Ruijie#show ip int brief

```

| Interface | IP-Address(Pri) | IP-Address(Sec) | Status | Protocol |
|---------------------|------------------|-----------------|--------|----------|
| GigabitEthernet 1/1 | 192.168.16.1/24 | no address | up | up |
| VLAN 10 | 192.168.1.1/24 | no address | up | up |
| VLAN 100 | 192.168.100.1/24 | 192.168.10.1/24 | up | up |

1.1.5 Configuring a Default Gateway

Note: The default gateway of a layer 3 switch is provided by static routing. A device can also learn network routing through a dynamic routing protocol so as to implement remote management. For the configuration specification of other routing protocols, see [IP Route](#) (for the configuration method, see **Common Function Configuration > IP Route**).

Configuring the Default Gateway of a Switch

Configure the default gateway, that is, default route, of a layer 3 switch.

```

Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.254 ----->configure default gateway of switch as 192.168.1.254
Ruijie(config)#end
Ruijie#write ----->save configuration after checking.

```

Verification

```

Ruijie#show ip route
Codes:C - Connected, L - Local, S - Static
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
IA - Inter area, * - candidate default
Gateway of last resort is 192.168.1.254 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 192.168.1.254

```

1.2 Firmware Upgrade

1.2.1 Firmware Upgrade for RGOS 10.x

Notes (Must-Read)

I. TFTP Server

A TFTP server must be installed on a TCP/IP-ready workstation or PC. Once the application is installed, a minimal level of configuration must be performed.

1. First, the TFTP application must be configured to operate as a TFTP server as opposed to a TFTP client.
2. Second, the outbound file directory must be specified. This is the directory in which the Ruijie RGOS Software images are stored (see step 2 below). Most TFTP applications provide a setup routine to assist in these configuration tasks.

Note: A number of TFTP are available from independent software vendors or as shareware from public sources on the World Wide Web.

3. Third, download a TFTP Server. There are many TFTP servers available, and they can be easily found by searching for "tftp server" on your favorite Internet search engine. Ruijie does not specifically recommend any particular TFTP implementation.

II. Prerequisites

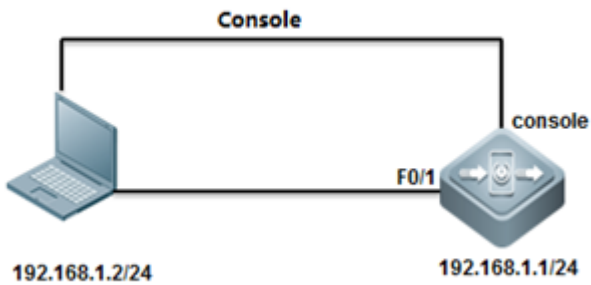
1. Download latest firmware at www.ruijienetworks.com
2. Backup running configuration to local harddrive
3. Prepare console cable in case of upgrade failure
4. Read firmware release notes, especially check "hardware supported" chapter
5. Log the whole upgrade process.

III. Tips

1. System upgrade require rebooting, may cause network down , suggest to upgrade in offpeak hours.
2. Keep power on during the whole upgrade process, or firmware might be lost.
3. Double check firmware package before upgrade, (Verify MD5 hash value)
4. Backup config file before your upgrade.

1.2.1.1 User Mode Upgrade (Recommended)

I. Network Topology



II. Configuration Steps:

1. Configure MGMT IP

```
Ruijie>enable          ----->enable mode
Ruijie#configure terminal ----->enter global mode
Ruijie(config)#interface vlan 1 ----->interface mode
Ruijie(config-if)#ip address 192.168.1.1 255.255.255.0 ----->configure MGMT ip
Ruijie(config-if)#exit
```

2. Check ping connectivity

C:\Users\Scott>ping 192.168.1.1 ping from pc to switch

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

```
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

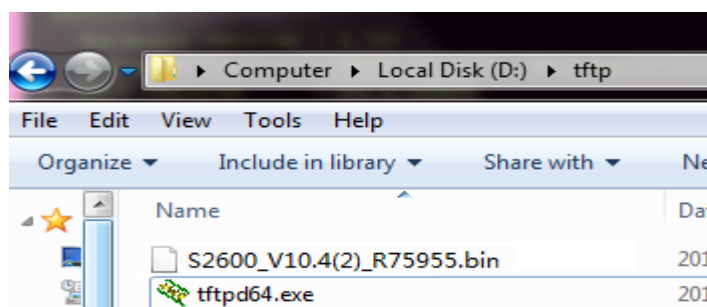
```
Ruijie#ping 192.168.1.2 From switch to PC
Sending 5, 100-byte ICMP Echoes to 192.168.1.2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Notice: disable PC firewall during the whole process.

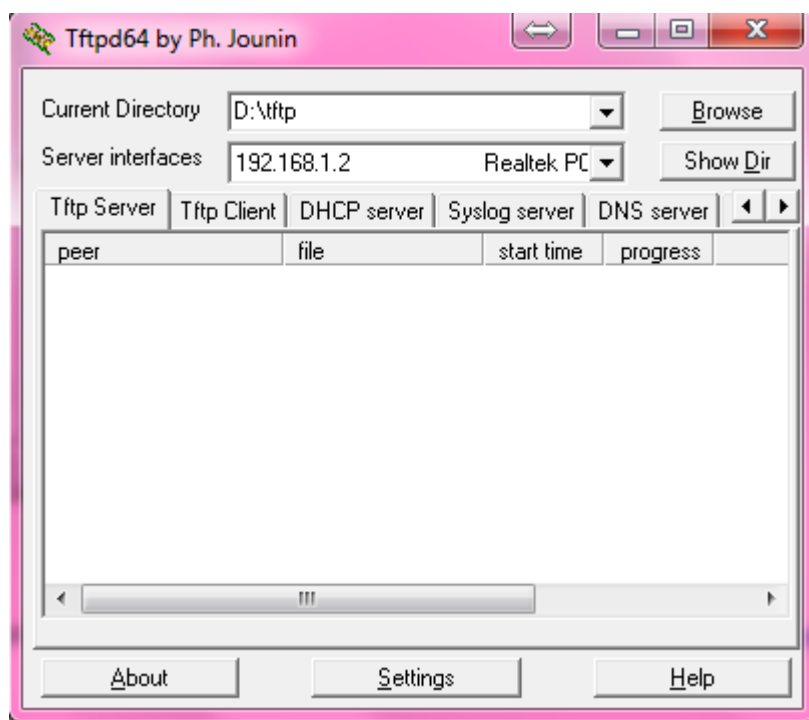
3. Check running firmware version

```
Ruijie#show ver
System description      : Ruijie Gigabit Security & Intelligence Acco
System start time       : 2013-2-27 15:9:17
System hardware version : 1.10 → hardware
System software version : RGOS 10.2(5), Release(67033) → software
System boot version     : 10.2.58430
System CTRL version     : 10.2.59999
Device information:
  Device-1
    Hardware version : 1.10
    Software version : RGOS 10.2(5), Release(67033)
    BOOT version     : 10.2.58430
    CTRL version     : 10.2.59999
```

4. Put tftp client and upgrade package in the same folder



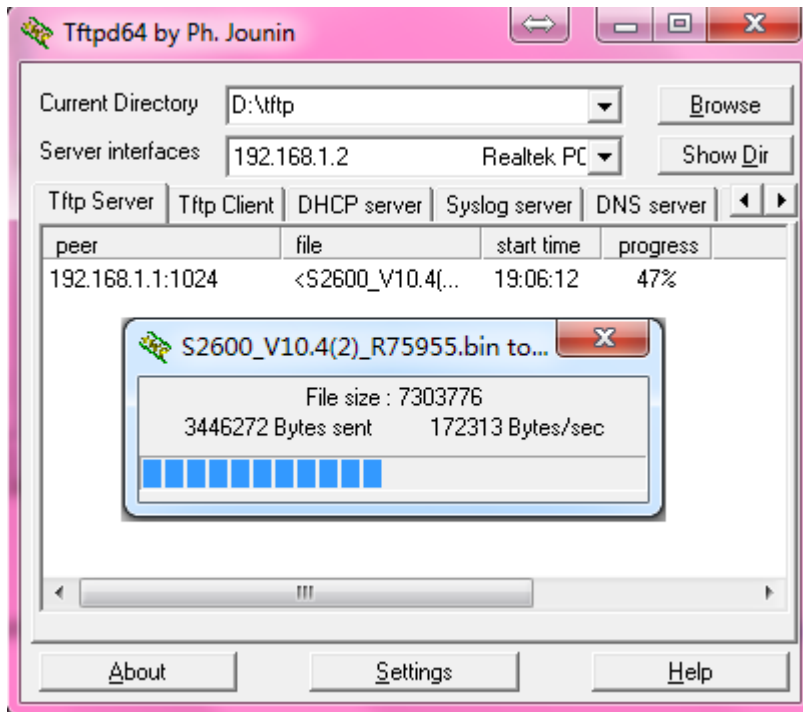
5. Enable TFTP server



6. Login the switch

```
Ruijie#show ip route Ruijie#copy tftp://192.168.1.2/S2600_V10.4(2)_R75955.bin flash:rgos.bin 192.168.1.2 -
->PC ; S2600_V10.4(2)_R75955.bin-->upgrade package ; rgos.bin --> firmware name
```

Copying firmware



7. File transfer finished

```
Ruijie#copy tftp://192.168.1.2/S2600_V10.4(2)_R75955.bin flash:rgos.bin
Accessing tftp://192.168.1.2/S2600_V10.4(2)_R75955.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Other members are not present, quit synchronize...
Checking file, please wait for a few minutes ....
Check file success.

Transmission finished, file length 7303776

THE PROGRAM VERSION: RGOS 10.4.*, Release(75955) -> version
Upgrade Master CM main program OK.

CURRENT PRODUCT INFORMATION :
PRODUCT ID: 0x20110010
PRODUCT DESCRIPTION: Ruijie Gigabit Security & Intelligence Access Switch (S2628G)

SUCCESS: UPGRADING OK -> Finished Model
```

8. Reboot the switch

```
Ruijie#reload
Processed with reload? [no]y → Input Y
```

9. Check rebooting process

```
Ruijie#show ver
System description      : Ruijie Gigabit Security & Intelligenc
System start time       : 2013-03-01 1:42:56
System uptime          : 0:0:2:9
System hardware version : 1.1
System software version : RGOS 10.4(2) Release(75955)
System BOOT version    : 10.4 Release(59831)
System CTRL version    : 10.4 Release(51419)
Device information:
  Device-1
    Hardware version : 1.1
    Software version : RGOS 10.4(2) Release(75955)
    BOOT version    : 10.4 Release(59831)
    CTRL version    : 10.4 Release(51419)
```

1.2.1.2 Monitor Mode Upgrade (for recovery)

Notice

1. Ctrl mode upgrade is designed for disaster recovery
2. If system prompts "send download request" , you have to follow these monitor mode upgrade steps.

I. Tips

1. Connect console cable to the switch
2. Connect Ethernet cable to the first copper port or MGMT port (physical port doesn't linked up until data transfer start, you also can not check ping connectivity during this process)

II. Upgrade Steps

1. Set pc IP address -->192.168.1.2 , enable TFTP server

Note: disable windows fireware during the whole upgrade process.

2. Connect switch console port
3. Console login to the system

1) Enter monitor mode

```
System bootstrap ...
Nor Flash ID: 0x01490000, SIZE: 2097152Bytes
Using 133.333 MHz high precision timer.
Press Ctrl+B to enter Boot Menu .....
Load Ctrl Program ...

Load CTRL with ECC.....
Executing program, launch at: 0x00010000

Load CTRL with ECC.....

Self decompressing the image :
#####
Ctrl Version: RGOS 10.4(2) Release(75955)
MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 33554432)
Press Ctrl+C to enter Ctrl .....

!!!NOTICE!!!
Main program (rgos.bin) is losted! —————> Firmware lost
Press F1 key to recover this problem step by step, or wait 2 s
Now begin to download all files through the FileList.

Host IP[192.168.64.1] Target IP[192.168.64.154] File name[FileList.txt]
%Now Begin Download File FileList.txt From 192.168.64.154

send download request. ■ —————> Auto download the firmware
```

2) Terminate this progress, enter Ctrl> mode

Note: during normal start-up process, Press "ctrl+C" to interrupt

```

send download request.
send download request. —————> Ctrl+C
User terminated!!!

Some i/o error was occurred while writing the file.
Can't download the FileList.txt!
Host IP[192.168.64.1] Target IP[192.168.64.154] File name[rgos
%Now Begin Download File rgos.bin From 192.168.64.154

User terminated!!!

Some i/o error was occurred while writing the file.
-----
download all files failed!
-----

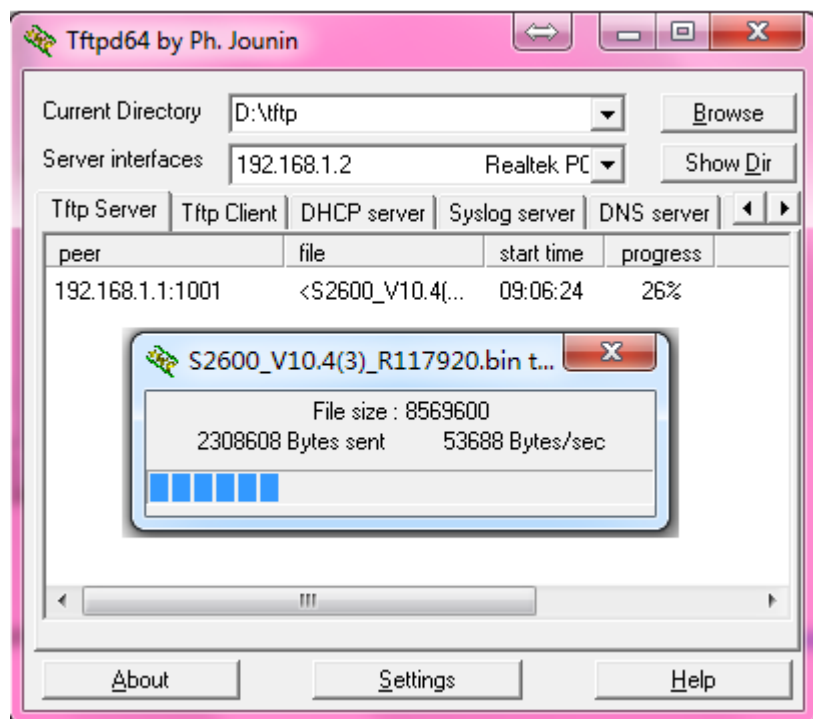
Hot Commands:
-----
-----
Ctrl>

```

3) Input command `ftfp 192.168.1.1 192.168.1.2 S2600_V10.4(3)_R117920.bin -main`

```
Ctrl>tftp 192.168.1.1 192.168.1.2 S2600_V10.4(3)_R117920.bin -main  
Switch PC Package keyword  
  
Now, begin download program through Tftp...  
  
Host IP[192.168.1.2] Target IP[192.168.1.1] File name[S2600_V10.4(3)_R117920.bin]  
%Now Begin Download File S2600_V10.4(3)_R117920.bin From 192.168.1.  
  
send download request.  
send download request. file transferring  
send download request.  
send download request.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
%Mission Completion. FILELEN = 8569600  
Tftp download OK, 8569600 bytes received!  
Verify the image ..[ok] total bytes  
  
CURRENT PRODUCT INFORMATION :  
PRODUCT ID: 0x20110020  
PRODUCT DESCRIPTION: Ruijie Gigabit Security & Intelligence Access Switch (S2652G)  
  
SUCCESS: UPGRADING OK.
```

4) File transferring



5) Check file size

```
Ctrl>dir.
```

| Mode | Link | Size | MTime | Name |
|-------|------|---------|---------------------|---------------------|
| | 1 | 512 | 2013-04-07 01:06:02 | Ctrl_hotcmd.cfg |
| | 1 | 1959 | 2013-03-12 05:11:15 | config.text |
| <DIR> | 1 | 0 | 1970-01-01 00:00:00 | dev/ |
| | 1 | 199 | 2013-03-08 01:44:16 | dhcp_snp.dat |
| <DIR> | 2 | 0 | 2013-03-04 03:39:20 | grtd/ |
| | 1 | 725 | 2013-03-04 03:39:37 | httpd_cert.crt |
| | 1 | 497 | 2013-03-04 03:39:37 | httpd_key.pem |
| <DIR> | 2 | 0 | 2013-03-04 03:39:22 | log/ |
| | 1 | 8 | 2013-03-12 05:11:15 | priority.dat |
| <DIR> | 0 | 0 | 1970-01-01 00:00:00 | proc/ |
| <DIR> | 1 | 0 | 2013-04-07 01:18:35 | ram/ |
| | 1 | 8569600 | 2013-04-07 01:09:07 | rgos.bin |
| | 1 | 7159 | 2013-03-12 09:13:01 | syslog.tx |
| <DIR> | 2 | 0 | 2013-03-12 05:12:50 | tmp/ |
| | 1 | 1215968 | 2013-03-07 01:12:56 | web_management_pack |

9 Files (Total size 9796627 Bytes), 6 Directories.
Total 31457280 bytes (30MB) in this device, 20320256 bytes (19M)

6) Load upgrade package

```

Ctrl>load——▶ Run upgrade package
Loading main program ...
Loading main program 'rgos.bin'.
Load main program successfully.
Executing program, launch at: 0x04000000
MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 33554432)

Self decompressing the image:
#####
Self decompressing the image succeed and will jump to 0x0001000
Ruijie General Operating System Software
Release Software (tm), RGOS 10.4(3) Release(117920), Compiled F

Copyright (c) 1998-2011s by Ruijie Networks.
All Rights Reserved.
Neither Decompiling Nor Reverse Engineering Shall Be Allowed.

*Apr  7 01:22:40: %MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(ch
*Apr  7 01:23:00: %UPGRADE-5-EXTITEM_INSTALLED: File /web_manag
*Apr  7 01:23:10: %DEVICE-5-CHANGED: Device S2652G (1) changed
000004: *Apr  7 01:23:21: Ruijie %GRTD-6-RUN_MINIMAL: Running m
000005: *Apr  7 01:23:22: Ruijie %GRTD-6-DIAG_OK: Passed boot-u
000006: *Apr  7 01:23:30: Ruijie %SYS-5-COLDSTART: System colds

```

7) Show version

```

Ruijie#show ver
System description      : Ruijie Gigabit Security & Intelligence
System start time       : 2013-04-07 1:22:40
System uptime           : 0:0:2:51
System hardware version  : 1.1
System software version : RGOS 10.4(3) Release(117920)
System BOOT version     : 10.4(2) Release(75955)
System CTRL version     : 10.4(2) Release(75955)
Device information:
  Device-1
    Hardware version : 1.1
    Software version  : RGOS 10.4(3) Release(117920)
    BOOT version     : 10.4(2) Release(75955)
    CTRL version     : 10.4(2) Release(75955)

```

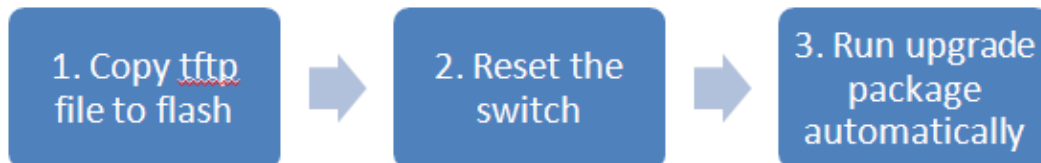
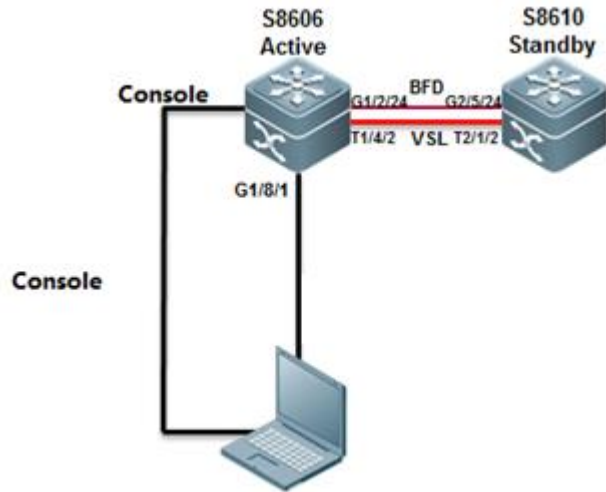
1.2.1.3 VSU Upgrade

Note : Applicable for all chassis/box switches

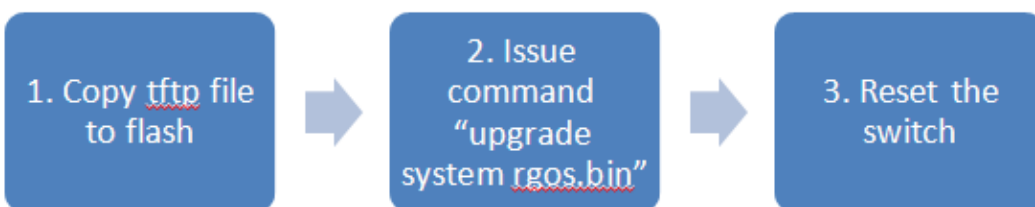
Scenario

One VSU group is consist of two S8600 VSU group, each of the chassis is loaded with dual control engine.

I. Network Topology



Auto upgrade: without any user interference .



Manually upgrade: 1. more reliable then auto mode
2.reduce service downtime.

II. Configuration Tips

1. Read release notes before the upgrade, especially the "supported hardware list"
2. VSU upgrade will cause network service down, plz researve at least TWO hours for the upgrade process.

III. Configuration Steps

1. Backup config file to local PC
2. Confirm hardware version before upgrade
3. Confirm with customer if service download is allowed;
4. Change chassis from VSU to standalone mode

Ruijie-ACTIVE#switch convert mode standalone

5. Follow chapter "firmware upgrade>User mode upgrade"
6. Show version on both chassis
7. Convert chassis back to VSU mode

Ruijie#switch convert mode virtual

Convert switch mode will automatically backup the "config.text" file and then delete it, and reload the switch. Do you want to convert switch to virtual mode? [no/yes]y

Do you want to recover "config.text" from "virtual_switch.text" (press 'ctrl + c' to cancel) [yes/no]:y

8. (show switch virtual), check network production

IV. Verification

1. Show version
2. Show switch virtual

1.2.2 Firmware Upgrade for RGOS 11.x

Overview

Two upgrade packages are available to 11.X switches, namely rack package and patch package.

A rack package contains main installation packages of the supervisor module and all line cards and is used to upgrade all line cards on a rack device at one time.

A hot patch package contains hot patches for several functional components and is generally used to fix minor bugs. The functional component package can be patched by upgrading the hot patch package. After the upgrade, the device can immediately have new features without being restarted.

Both the rack package and the hot patch package are upgraded with their configurations saved.

Notes (Must-Read)

The difference between an 11.X box-type switch and a rack-type switch lies in that the former restarts after the upgrade command is run while the latter restarts after the reload command is run.

```
Ruijie#upgrade flash:S2910_RGOS11.4(1)B1_02162700_install.bin
Upgrade the device must be auto-reset after finish, are you sure upgrading now?[Y/N]y
```

Upgrade in the Running Mode

Rack Package Upgrade Using a USB Flash Disk

Notes

1. To fix software bugs or get new features, upgrade the switch software version in the running mode.
2. A USB flash disk is recommended for 11.X switch upgrade because the installation package is big and upgrade using other methods is slow. Upgrade with a USB flash disk is easy and quick.
3. The CM supervisor module only has a capacity of 512 MB. Therefore, the rack package can be directly upgraded only with a USB flash disk.
4. If the CM supervisor module has a capacity of 1 GB, upgrade the device by copying the installation package from TFTP to the installation partition as well as by using a USB flash disk. Run the **dir install:** command to view the corresponding drive.
5. If the CMII supervisor module has a large capacity, upgrade the device by copying the installation package from TFTP to the data partition as well as using a USB flash disk. Run the **dir flash:** command to view the corresponding drive.

Patch Package Upgrade Using a USB Flash Disk

Notes

1. To fix software bugs or get new features, upgrade the switch software version in the running mode.
2. A hot patch package contains hot patches for several functional components and is generally used to fix minor bugs. The functional component package can be patched by upgrading the hot patch package. After the upgrade, the device can immediately have new features without being started.
3. There is a baseline version for the patch package upgrade. Upgrade the device to the corresponding baseline version before upgrading the patch package. The device may be upgraded compulsively to the corresponding baseline version but it may cause version incompatibility. Therefore, compulsive upgrade is not advised.
4. To permanently activate patches, run the **patch active** command to temporarily activate the patch before running the **patch running** command.

1.2.2.1 Upgrade with USB Drive

I. Configuration Tips

Run the **show version detail** command to display the current version, that is, system software number.

Verify the upgrade file used by checking Release Notes.

Copy the upgrade file from the PC to the root directory of the USB flash drive.

Insert the USB flash drive to the USB port of the supervisor engine. The USB flash drive is automatically identified.

Note: Before removing the USB flash drive from the switch, run the `show usb` command to check the USB ID, and then run the `usb remove xx` command to remove the USB flash drive.



II. Configuration Steps

1. On CLI, run the upgrade command.

```
Ruijie#dir usb0: Checks whether the upgrade file exists on the USB flash drive.
```

```
Ruijie#upgrade usb0: /xxxxx_install.bin (xxxx_install.bin is the upgrade file copied to the USB flash drive)
```

2. Wait until the upgrade progress reaches 100%, or run the `show upgrade status` command to check the upgrade progress.

```
S8600E-VSU#sh upgrade sta
[Slot 2/M1]
Device type      : ca-octeon-cm
Status           : ready
[Slot 2/3]
Device type      : ca-octeon-lc
Status           : ready
```

3. Wait until the upgrade process of all the line cards, FE cards, and supervisor engines reaches 100% and the result is success, run the `reload` command to restart the device. (The entire upgrade process generally takes four to five minutes and does not affect services. In this operation, the Flash file on the line card is upgraded, but the earlier version still runs on the memory.) After the device is restarted, the new version runs.
4. Wait three to five minutes until the device is restarted.

III. Verification

```
S8600E-VSU#sh version detail
```

1.2.2.2 Upgrade with FTP

Run the `show version detail` command to display the current version, that is, system software number.



Verify the upgrade file used by checking Release Notes.

II. Configuration Steps

1. Start the FTP server on the device, and designate the root directory as the USB0 root directory. (The space on the built-in Flash of CMI is small, and may be insufficient for storing the upgrade file. The CMII can be specified as the Flash root directory.) ,the reference commands are as follows:

```

Ruijie(config)#ftp-server username admin
Ruijie(config)#ftp-server password ruijie
Ruijie(config)#ftp-server topdir usb0: /           //The USB flash drive must be installed in advance on the main
engine.
Ruijie(config)#ftp-server timeout 300
Ruijie(config)#ftp-server enable
  
```

2. The local PC serves as the FTP client. Start the client software (such as FLASHFTP) and connect to the FTP server (N18K). Ensure that the PC can communicate properly with the S86E.
3. Use the FTP client on the PC to load the upgrade file to the FTP server.
4. Run the upgrade command. (The subsequent procedures and methods are the same as those in the USB upgrade mode.) The only difference between the FTP and USB onsite upgrade modes lies in the file transfer mode. In FTP upgrade mode, the upgrade file is transferred to the remote device through FTP to meet the remote upgrade requirement. In USB onsite upgrade mode, the upgrade file is directly copied from a PC to the USB flash drive.

The subsequent upgrade method is the same. That is, run the upgrade command to update the file and then restart the device to finish the upgrade.

1.2.2.3 Upgrade with TFTP

Run the show version detail command to display the current version, that is, system software number.



Verify the upgrade file used by checking Release Notes.

I. Configuration Steps

1. Start the TFTP server on the PC and specify the directory of the upgrade file. Ensure that the PC communicates properly with the S86E.

3. The S86E serves as the TFTP client. The upgrade method is the same as that in the common TFTP upgrade mode. Copy the upgrade file to the USB flash drive on the CMI, or to the built-in Flash on the CMII.

```
Ruijie#copy tftp://192.168.1.1/S86e_install.bin usb0:// S86e_install.bin
```

4. Run the upgrade command. (The subsequent procedures and methods are the same as those in the USB upgrade mode.) The only difference between the TFTP and USB onsite upgrade modes lies in the file transfer mode. In TFTP upgrade mode, the upgrade file is transferred to the remote device through TFTP to meet the remote upgrade requirement. In USB onsite upgrade mode, the upgrade file is directly copied from a PC to the USB flash drive.

The subsequent upgrade method is the same. That is, run the upgrade command to update the file and then restart the device to finish the upgrade.

The TFTP transmission rate is lower than the FTP transmission rate. Data is transmitted using TCP in FTP mode, and using UDP in TFTP mode. TFTP is simple and easy to use.

1.2.2.4 Install Patch

1. 11.X is a modular OS and the bug of a software function can be fixed by using a patch. After the patch is installed, the device can fix the bug and can run normally without being restarted. This OS is applicable to the scenario that imposes rigid requirements on the network interruption time during maintenance.

2. A patch is in the uninstalled, installed, or activated state, where:

The installed state indicates that the patch is installed on the memory of the device but the path function does not take effect yet.

Only a patch in the activated state takes effect.

I. Configuration Steps

1. Install a patch.

Copy the path file to a USB flash drive, and run the upgrade command to install the path. The reference command is as follows:

```
Ruijie#upgrade usb0: /N18K-octeon-cm_RGOS11.0(1b2)_20140708_patch.bin
```

2. Activate a patch.

The reference command is as follows:

```
Ruijie#patch active slot all
Ruijie#patch running slot all
```

Note: active means that the patch is currently effective and is ineffective after the device is restarted. running indicates that the patch is effective permanently.

3. Display the patch status.

The reference command is as follows:

```
Ruijie#show patch slot all
```

1.2.2.5 Monitor Mode Upgrade (for recovery)

Notice

3. Ctrl mode upgrade is designed for disaster recovery
4. If system prompts "send download request" , you have to follow these monitor mode upgrade steps.

I. Tips

1. Connect console cable to the switch
2. Connect Ethernet cable to the first copper port or MGMT port (physical port doesn't linked up until data transfer start, you also can not check ping connectivity during this process)

II. Upgrade Steps

Note: disable windows fireware during the whole upgrade process.

1. Connect switch console port
2. Console login to the system
- 1) Enter monitor mode, change the baudrate to 115200

```

System bootstrap ...
Nor Flash ID: 0x01490000, SIZE: 2097152Bytes
Using 133.333 MHz high precision timer.
Press Ctrl+B to enter Boot Menu .....
Load Ctrl Program ...

Load CTRL with ECC.....
Executing program, launch at: 0x00010000

Load CTRL with ECC.....

Self decompressing the image :
#####
Ctrl Version: RGOS 10.4(2) Release(75955)
MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 33554432)
Press Ctrl+C to enter Ctrl .....

!!!NOTICE!!!
Main program (rgos.bin) is losted! —————> Firmware lost
Press F1 key to recover this problem step by step, or wait 2 s
Now begin to download all files through the FileList.

Host IP[192.168.64.1] Target IP[192.168.64.154] File name[FileList.txt]
%Now Begin Download File FileList.txt From 192.168.64.1

send download request. ■ —————> Auto download the firmware

```

2) Terminate this progress, enter Ctrl> mode

Note: during normal start-up process, Press "ctrl+C" to interrupt, change the baudrate to 115200 first

```

===== BootLoader Menu("Ctrl+Z" to upper level) =====
TOP menu items.
*****
0. Tftp utilities.
1. XModem utilities.
2. Run main.
3. SetMac utilities.
4. Scattered utilities.
5. Set module serial
*****

```

```

===== BootLoader Menu("Ctrl+Z" to upper level) =====
Scattered utilities.
*****
0. Show the bootloader version.
1. Reload system
2. Set baudrate.
3. Advanced settings.
*****

```

```

===== BootLoader Menu("Ctrl+Z" to upper level) =====
Set baudrate.
*****
0. Change baudrate to 9600
1. Change baudrate to 57600
2. Change baudrate to 115200
*****
Press a key to run the command:

```

Relogin the CLI page of switch since the baudrate has been changed.

```

===== BootLoader Menu("Ctrl+Z" to upper level) =====
TOP menu items.
*****
0. Tftp utilities.
1. XModem utilities.
2. Run main.
3. SetMac utilities.
4. Scattered utilities.
5. Set Module Serial
*****
Press a key to run the command:

```

Choose 1 for Xmodem utilities, and then choose 1 for main program upgrading, then choose transmission mode as sendXmodem(N) for firmware transmission

```

===== BootLoader Menu("Ctrl+Z" to upper level) =====
TOP menu items.
*****
0. Tftp utilities.
1. XModem utilities.
2. Run main.
3. SetMac utilities.
4. Scattered utilities.
5. Set Module Serial
*****
Press a key to run the command: 1

===== BootLoader Menu("Ctrl+Z" to upper level) =====
XModem utilities.
*****
0. Upgrade bootloader.
1. Upgrade kernel and rootfs by install package.
*****
Press a key to run the command: 1
CCCCCCC
Starting xmodem transfer. Press Ctrl+C to cancel.
Transferring rgos.bin..
0%      174 KB      6 KB/s 04:33:44 ETA    0 Errors

```

3) Load upgrade package

```
===== BootLoader Menu("Ctrl+Z" to upper level) =====
TOP menu items.
*****
0. Tftp utilities.
1. XModem utilities.
2. Run main.
3. SetMac utilities.
4. Scattered utilities.
5. Set Module Serial
*****
Press a key to run the command:
```

7) Show version

```
Ruijie#show version
System description : Ruijie 10G Ethernet Switch(S5750C-48GT4XS-H) By Ruijie Networks
System start time : 2016-08-23 17:45:36
System uptime : 0:03:10:08
System hardware version : 1.00
System software version : S5700H_RGOS 11.4(1)B2P3
System patch number : NA
System serial number : 1234942570049
System boot version : 1.2
Module information:
Slot 0 : S5750C-48GT4XS-H
Cpu 0:
Hardware version : 1.00
Boot version : 1.2
Software version : S5700H_RGOS 11.4(1)B2P3
Serial number : 1234942570049
Ruijie# show
```

1.2 Password Recovery

1.2.1 Reset Password for RGOS 10.X

I. Configuration Tips

1. Recovery the password in monitor mode (Ctrl mode)
2. Rename previous config file instead of renaming config file

II. Configuration Steps

1. Connect console cable to the switch
2. Refer to chapter system management>console management
 - 1) Manually reboot the switch
 - 2) Press Ctrl+C when system rebooting

```
System bootstrap ...
Nor Flash ID: 0xC2CB0000, SIZE: 8388608Bytes
Press Ctrl+B to enter Boot Menu .....
Load Ctrl Program ...

Executing program, launch at: 0x00010000

Self decompressing the image :
#####
Ctrl Version: RGOS 10.4(2b2) Release(102500)
MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 134217728
1 nand chip(s) found on the target.
Press Ctrl+C to enter Ctrl ... → Press constantly
:
Hot Commands:
-----
F1. tftp 192.168.0.2 192.168.0.1 rgos.bin -main
-----
Ctrl>^C
Ctrl> → Ctrl mode
```

- 3) Rename config.text ---->config.bak

```
Ctrl>
Ctrl>rename config.text config.bak
Ctrl>
```

- 4) Load firmware

```
Ctrl>load
```

- 5) Recovery the previous config file

```
Ruijie#copy flash:config.bak flash:config.text
Ruijie#copy startup-config running-config
```

- 6) Set new password

```
Ruijie(config)#
Ruijie(config)#enable secret ruijie → New password
Ruijie(config)#line vty 0 4
Ruijie(config-line)#password ruijie → New telnet pwd
Ruijie(config-line)#login
Ruijie(config-line)#end
Ruijie#Feb 27 19:35:14: %SYS-5-CONFIG_I: Configured from console
Ruijie#wr → Save config file
Building configuration...
[OK]
```

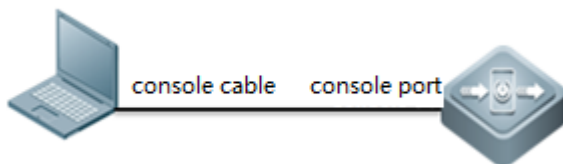
6) Verify new password

Login with the new password

1.2.2 Reset Password for RGOS 11.X

I. Configuration Tips

1. Prepare console cable before recovering
2. Password recovery require system rebooting and network downtime
3. Improper operation may cause config file lost.



II. Configuration Steps

1. connect console cable to the switch
2. Refer to chapter system management>console management
 - 1) manually reboot the switch
 - 2) Press Ctrl+C when system rebooting

```

Boot 1.2.7-ef4d454 (Build time: Jul 22 2014 - 17:14:28)

DRAM: 4 GiB
NAND: 512 MiB
Flash: 8 MiB
SETMAC: Setmac operation was performed at 2014-08-26 14:36:37 (version: 11.0)
Press Ctrl+C to enter Boot Menu -> press Ctrl+ C
Skipping PCIe port 0 BIST, reset not done. (port not configured)
Skipping PCIe port 1 BIST, reset not done. (port not configured)
BIST check passed.
CAOCTEONCM board revision major:1, minor:0
OCTEON CN6130-AAP pass 1.1, Core clock: 1000 MHz, IO clock: 600 MHz, DDR clock: 533 MHz (1066 Mhz data
rate)
Net: octmgmt0, octmgmt1, octeth0, octeth1, octeth2, octeth3, octeth4, octeth5, octeth6, octeth7
Entering simple UI....

===== BootLoader Menu("Ctrl+Z" to upper level) =====
TOP menu items.
*****
0. Tftp utilities.
1. XModem utilities.
2. Run main.
3. SetMac utilities.
4. Scattered utilities.
5. Set backplane info
6. Set Fan utilities
7. Set Power utilities
*****

```

3) Press CTRL + Q to enter uboot CLI mode

```

===== BootLoader Menu("Ctrl+Z" to upper level) =====
TOP menu items.
*****
0. Tftp utilities.
1. XModem utilities.
2. Run main.
3. SetMac utilities.
4. Scattered utilities.
5. Set backplane info
6. Set Fan utilities
7. Set Power utilities
*****
Press a key to run the command: Press CTRL+Q to enter uboot CLI
input command "main_config_password_clear"
ca-octeon-cm#main_config_password_clear->

```

4) then system will reboot automatically

```

Press a key to run the command:
ca-octeon-cm#main_config_password_clear
Bootloader: Done loading app on coremask: 0xf
Starting Devices Initializations... [ OK ]

*Sep 10 01:51:36: %LOCAL_DP-5-LC_PROB: Probing card in slot 1 of local chassis.
*Sep 10 01:51:36: %LOCAL_DP-5-LC_PROB: Probing card in slot FE3 of local chassis.
" # *Sep 10 01:51:56: %LOCAL_DP-5-LC_PROB: Probing card in slot 1 of local chassis.
*Sep 10 01:51:56: %LOCAL_DP-5-LC_PROB: Probing card in slot FE3 of local chassis.
*Sep 10 01:51:59: %LOCAL_DP-5-LC_PROB: Board information in this chassis has been collected.
*Sep 10 01:51:59: %SWITCH-6-INSTALL: Install chassis RG-N18010 on switch 1
*Sep 10 01:51:59: %DP-6-MASTER: Module in slot M1 has translated to master.
*Sep 10 01:51:59: %DP-6-POWER_OK: Power 4 ok.
*Sep 10 01:52:00: %DP-5-LC_PROB: Probing card in slot 1.
*Sep 10 01:52:00: %DP-5-LC_PROB: Probing card in slot FE3.
*Sep 10 01:52:00: %MODULE-6-INSTALL: Install Module M18000-24GT20SFP4XS-ED in slot 1.
*Sep 10 01:52:00: %DEV_MONITOR-4-CARD_POWER_ON: The power enough, card in slot 1 will be controlled to
power on automatically.
*Sep 10 01:52:00: %DEV_MONITOR-4-CARD_POWER_ON: The power enough, card in slot FE3 will be controlled
to power on automatically.
*Sep 10 01:52:00: %DEV_MONITOR-4-CARD_POWER_ON: The power enough, card in slot M1 will be controlled t
o power on automatically.
*Sep 10 01:52:02: %OIR-6-INSCARD: Card inserted in slot 1.
*Sep 10 01:52:02: %PKG_MGMT-4-NO_AUTO_UPGRADE: After uboot upgrade, auto sync upgrade halt!
*Sep 10 01:52:02: %OIR-6-INSCARD: Card inserted in slot FE3.
*Sep 10 01:52:02: %DP-5-PROB: Board probing has completed.
*Sep 10 01:52:02: %DEV_MONITOR-6-DEVICE_INIT: master role init.
*Sep 10 01:52:04: %REDUNDANCY-6-STATES_CHANGE: Redundancy states changed: role master, state alone.

Press RETURN to get started
*Sep 10 09:52:47: %TUN-4-CAPACITY_LOW: tunnel capability has changed from [1000] to [127], those tunne

```

- 5) At this moment, no password is required to enter CLI

```
Ruijie>en
Ruijie#
```

Note: The password is reset just temporarily .Once you quit privilege mode, password is required again. You have to reset the password quickly.

- 6) Reset new password

```
Ruijie(config)#
Ruijie(config)#enable secret ruijie → New password
Ruijie(config)#line vty 0 4
Ruijie(config-line)#password ruijie → New telnet pwd
Ruijie(config-line)#login
Ruijie(config-line)#end
Ruijie#Feb 27 19:35:14: %SYS-5-CONFIG_I: Configured from console
Ruijie#wr → Save config file
Building configuration...
[OK]
Ruijie#
```

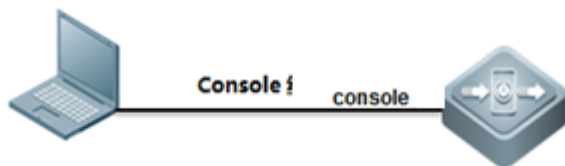
- 7) Verify new password

Login with the new password

1.3 Restore Factory Default

1.3.1 Restore Factory Default for RGOS 10.X

I. Network Topology



II. Configuration Steps

1. Connect console cable to the switch

2. Refer to chapter system management>console management

- 1) Manually reboot the switch
- 2) Press Ctrl+C when system rebooting

```
System bootstrap ...
Nor Flash ID: 0xC2CB0000, SIZE: 8388608Bytes
Press Ctrl+B to enter Boot Menu .....
Load Ctrl Program ...

Executing program, launch at: 0x00010000

Self decompressing the image :
#####
Ctrl Version: RGOS 10.4(2b2) Release(102500)
MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 134217728
1 nand chip(s) found on the target.
Press Ctrl+C to enter Ctrl ... → Press constantly
:
Hot Commands:
-----
F1. tftp 192.168.0.2 192.168.0.1 rgos.bin -main
-----
Ctrl>^C
Ctrl> → Ctrl mode
```

- 3) Delete config. txt

```
Ctrl>delete config.text
Are you sure you want to delete "config.text"?[No/yes]y → Press Y
File "config.text" is deleted.
```

- 4) Load firmware

```
Ctrl>load
```

III. Verification

Confirm if all previous config file has been earased.

2 Configuration Guide

2.1 Initialization

2.1.1 Overview (Must Read)

For Standardization reason, we strongly suggest you to initialize every new switch following the steps below:

1. Hostname (mandatory)
2. Access a device (mandatory , see Chapter Installation and Device Management --->System Management)
 - 2.1. Assign management IP address (mandatory)
 - 2.2. Set default gateway (optional for layer 3 switch, but mandatory for layer 2 switch)
 - 2.3. Telnet (optional)
 - 2.4. SSH (recommended)
 - 2.5. Web User interface (optional)
3. Log (mandatory , and choose one)
 - 3.1. Record log to FLASH (recommended)
 - 3.2. Send log to server (recommended)
4. Clock (mandatory , and choose one)
 - 4.1. Local clock (recommended)
 - 4.2. NTP (recommended)
5. Configuring a port (mandatory)
 - 5.1. Port description (mandatory)
 - 5.2. Speed, duplex and flowcontrol (optional)
 - 5.3. Combo port (optional)
 - 5.4. ACCESS or TRUNK port (mandatory)
 - 5.5. Storm control (recommended)
6. SNMP (recommended)
 - 6.1. SNMPV1/V2 (recommended)
 - 6.2. SNMPV3 (recommended)
7. SPAN (optional)
 - 7.1. Many to one mirror (Optional)
 - 7.2. One to many mirror (Optional)
 - 7.3. Flow-based mirror (Optional)

2.1.2 Hostname

Configuring Hostname

By default, system name is "Ruijie mostly, the example shows how to configure the system name:

```
Ruijie>en
Ruijie#configure terminal
Ruijie(config)#hostname Switch      ----->change name to "Switch"
Switch(config)#end
Switch#write                        ----->save configuration
```

Note: We suggest you to name a switch with these information physical location(AA), network location(BB) ,model(CC),serial number(DD), and the format is (AA_BB_CC_DD) , for example:

```
Ruijie(config)#hostname WLZX_Core_S8610_1
WLZX_Core_S8610_1(config)#
```

Verifying

```
Switch#show run
Building configuration...
Current configuration : 34129 bytes
```

2.2 Log

2.2.1 Copying log to FLASH

I. Requirements

1. Copy logs with a severity higher than debugging in the flash, then set size of each log file to 128Kbytes.
2. Set size of log buffer to 128Kbytes.
3. Record action when user logs in and operates.
4. Add system name, sequence number and time stamps to each log entry.

II. Network Topology



III. Configuration Tips

System doesn't copy logs from buffer to flash once finishing configuration, and it costs about half an hour to copy logs from buffer to flash, or the log buffer exceeds.

IV. Configuration Steps

```

Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#logging file flash:syslog 6 ----->set log file name to "syslog" and system copies all logs with
severity from 0 to 6 to flash
Ruijie(config)#logging file flash:syslog 131072 ----->set size of each log file in flash to 128K
Ruijie(config)#logging buffered 131072 ----->set log buffer size to 128K
Ruijie(config)#logging userinfo ----->record actions when user logs in
Ruijie(config)#logging userinfo command-log ----->record actions when user operates commands
Ruijie(config)#service sysname ----->add system name to each log entry
Ruijie(config)#service sequence-numbers ----->add sequence number to each log entry
Ruijie(config)#service timestamps ----->add time stamps to each log entry
Ruijie#wr

```

Note: We suggest you to set log buffer size to 128K because the buffer size is too small by default.

If the 1st log file is full, system copies logs to 2nd log file, then the 3th log filethere're 16 log files at most in the same time, and if all 16 log files are full, the new log entry overwrites the old one, **so Log file never takes up the whole flash room.**

Enter "more flash:xxx" privilege EXEC command to display log entries and "delete flash:xxx" privilege EXEC command to delete log file in flash.

v. Verification

1. This example shows how to display logs in buffer

```

Ruijie#show log -----> show logs in buffer
Syslog logging: enabled
Console logging: level debugging, 5 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 6 messages logged
File logging: level informational, 6 messages logged -----> log severity
File name:syslog.txt, size 1024 Kbytes, have written 1 files
Standard format: false -----> log file name in flash
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence-number log messages: enable -----> add sequence number
Sysname log messages: enable -----> add system name
Count log messages: disable
Trap logging: level informational, 6 message lines logged, 0 fail
Log Buffer (Total 131072 Bytes): have written 552, -----> buffer size
*Mar 12 05:12:30: %MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 33554432) de
*Mar 12 05:12:50: %DEVICE-5-CHANGED: Device S2652G (1) changed state to up.
000003: *Mar 12 05:13:07: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/3, changed
000004: *Mar 12 05:13:07: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface Fast

```

2. Enter "dir" privilege EXEC command to check log files in flash

```
Ruijie#dir
```

| Mode | Link | Size | MTime | Name |
|-------|------|---------|---------------------|-----------------|
| | 1 | 512 | 2013-03-04 03:27:42 | Ctrl_hotcmd.cfg |
| | 1 | 1959 | 2013-03-12 05:11:15 | config.text |
| <DIR> | 1 | 0 | 1970-01-01 00:00:00 | dev/ |
| | 1 | 199 | 2013-03-08 01:44:16 | dhcp_snp.dat |
| <DIR> | 2 | 0 | 2013-03-04 03:39:20 | grtd/ |
| | 1 | 725 | 2013-03-04 03:39:37 | httpd_cert.crt |
| | 1 | 497 | 2013-03-04 03:39:37 | httpd_key.pem |
| <DIR> | 2 | 0 | 2013-03-04 03:39:22 | log/ |
| | 1 | 8 | 2013-03-12 05:11:15 | priority.dat |
| <DIR> | 0 | 0 | 1970-01-01 00:00:00 | proc/ |
| <DIR> | 1 | 0 | 2013-03-12 05:12:33 | ram/ |
| | 1 | 7440800 | 2013-03-07 01:11:16 | rgos.bin |
| | 1 | 1550 | 2013-03-12 05:11:33 | syslog.txt |
| <DIR> | 2 | 0 | 2013-03-12 05:12:50 | tmp/ |

appear after half an hour
or system reload

3. This example shows how to display logs in flash

```
Ruijie# more flash:syslog.txt
000120: *Mar 12 13:03:23: Ruijie %CLI-5-EXEC_CMD: Configured from console command: ex
000121: *Mar 12 13:03:23: Ruijie %SYS-5-CONFIG_I: Configured from console by console
000122: *Mar 12 13:04:40: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN
000123: *Mar 12 13:04:41: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN
000124: *Mar 12 13:07:25: Ruijie %SYS-5-RELOAD: The device is reloading due to the ex
```

4. Enter "clear logging" privilege EXEC command to clear logs in buffer

```
Ruijie#clear logging
```

2.2.2 Copying log to Server

I. Requirements

Copy logs with severity from 0 to 7 to syslog server.

II. Network Topology



III. Configuration Tips

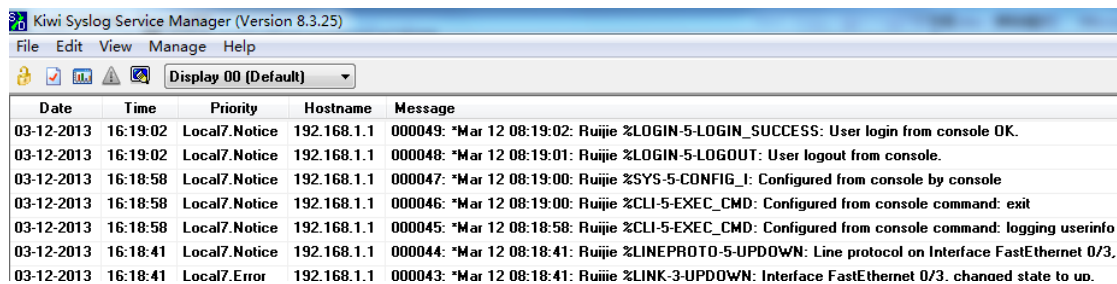
Timestamps and sequence number features must be enabled before system copys logs to log server

IV. Configuration Steps

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#service sequence-numbers ----->enable sequence number
Ruijie(config)#service timestamps ----->enable timestamps
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.1.1 255.255.255.0
Ruijie(config-if-VLAN 1)#exit
Ruijie(config)#logging server 192.168.1.2 ----->specify log server IP address
Ruijie(config)#logging source ip 192.168.1.1 ----->specify IP address on switch to communicate with log server
Ruijie(config)#logging trap 7 ----->copy all logs(severity from 0 to 7) to log server
Ruijie(config)#end
Ruijie#wr
```

V. Verification

This example shows how to verify the logs in a syslog server using "Kiwisyslog"



| Date | Time | Priority | Hostname | Message |
|------------|----------|--------------|-------------|---|
| 03-12-2013 | 16:19:02 | Local7.Notic | 192.168.1.1 | 000049: *Mar 12 08:19:02: Ruijie %LOGIN-5-LOGIN_SUCCESS: User login from console OK. |
| 03-12-2013 | 16:19:02 | Local7.Notic | 192.168.1.1 | 000048: *Mar 12 08:19:01: Ruijie %LOGIN-5-LOGOUT: User logout from console. |
| 03-12-2013 | 16:18:58 | Local7.Notic | 192.168.1.1 | 000047: *Mar 12 08:19:00: Ruijie %SYS-5-CONFIG_I: Configured from console by console |
| 03-12-2013 | 16:18:58 | Local7.Notic | 192.168.1.1 | 000046: *Mar 12 08:19:00: Ruijie %CLI-5-EXEC_CMD: Configured from console command: exit |
| 03-12-2013 | 16:18:58 | Local7.Notic | 192.168.1.1 | 000045: *Mar 12 08:18:58: Ruijie %CLI-5-EXEC_CMD: Configured from console command: logging userinfo |
| 03-12-2013 | 16:18:41 | Local7.Notic | 192.168.1.1 | 000044: *Mar 12 08:18:41: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/3, |
| 03-12-2013 | 16:18:41 | Local7.Error | 192.168.1.1 | 000043: *Mar 12 08:18:41: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/3. changed state to up. |

2.2.3 Log Filtering

Scenario

By default, the log information generated on the system can be output to various destinations. You can use the log filtering function to display required log information.

Features

- 1 The administrator can choose to hide some types of log information as required.
- 2 Generally, log information of all modules is displayed on the console or terminal. You can set log filter rules to enable log information printing on designated terminals or print only certain types of log information on designated terminals.
- 3 Two types of log information filtering are supported, including "contain only..." and "filter only...". Only one type of filtering is supported.

Working Principles & Configuration Details

Log filtering configuration mainly covers the filter rules, filter direction, and filter mode. During the configuration process:

- 1 If only the filter direction and filter mode are configured, the configuration does not take effect and log information is not filtered.
- 2 If only the filter rule is configured, the configuration takes effect. Log information in all directions is filtered and the filter mode is filter only.

1) Filter rule: sets the rule for filtering log information in global mode. Exact match and singular match are supported.

Filter rule in exact match mode: `logging filter rule exact-match [module module-name mnemonic mnemonic-name level level]`

Filter rule in singular match mode: `logging filter rule single-match [level level | mnemonic mnemonic-name | module module-name]`

Parameter description

exact-match Indicates an exact-match filter based on all three filter options. In exact match mode, all three filter options, including log module name (module module-name), log level (level level), and mnemonic character (mnemonic mnemonic-name), must be selected.

single-match Indicates a single-match filter based on all three filter options. In exact match mode, all three filter options, including log module name (module module-name), log level (level level), and mnemonic character (mnemonic mnemonic-name), must be selected.

module module-name indicates the name of the module about which the log information is to be filtered.

mnemonic mnemonic-name indicates the name of the mnemonic character for which the log information is to be filtered.

level level indicates the log level to be filtered.

Tips

1. In some scenarios, you may want to filter out certain types of log information. You can use the exact match mode and specify the module name, mnemonic character name, and log level in configuring the filter rule.
2. In some scenarios, you may want to filter out some types of log information. You can use the single match mode and specify the module name, mnemonic character name, or log level in configuring the filter rule.
3. If the configuration of the module name, mnemonic character name, or log level in a single-match filter rule is the same as that in an exact-match filter rule, the single-match filter rule is assigned with higher priority than the exact-match filter rule.

Configuration example

1. Set the filter rule to exact match, module name to LOGIN, log level to 5, and mnemonic character to LOGOUT.

```
Ruijie(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT level 5
```

2. Set the filter rule to **single-match** and module name to **SYS**.

```
Ruijie(config)# logging filter rule single-match module SYS
```

FAQs

1. To filter logs 046188: *Aug 13 08:36:16: 401-C1&D1-RG-N18010 %SPANTREE-6-RCVDTCBPDU: (*2/M1) Received tc bpd on port AggregatePort 256 on MST0

Command: ruijie(config)#logging filter rule exact-match module SPANTREE mnemonic RCVDTCPDU level 6

2. To filter logs *Jul 30 12:35:51: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host 185.94.111.1

Command: ruijie(config)#logging filter rule exact-match module SNMP mnemonic AUTHFAIL level 3

3. To filter logs %PARAM-6-CONFIG_SYNC: Sync'ing the startup configuration to the standby supervisor

Command: ruijie(config)#logging filter rule exact-match module PARAM mnemonic CONFIG_SYNC level 6

2) Filter direction: sets the direction for filtering log information in global mode.

logging filter direction { all | buffer | file | server | terminal } //By default, the filter direction is set to **all**, that is, to filter log information in all directions.

default logging filter direction // The filter direction for the log information restoration command is **all**.

Parameter description

all Indicates to filter log information in all directions, including the console, virtual type terminal (VTY), log buffer area, log file, and log server.

buffer Indicates to filter logs sent to the log buffer area that is the logs configured in the show logging command.

file Indicates to filter the logs sent to the log files.

server Indicates to filter the logs sent to the log server.

terminal Indicates to filter logs sent to the console and VTY (including via Telnet and SSH).

Tips

1. Generally, you may filter the logs meeting the filter rule in all directions (including to the console, VTY terminal, log buffer area, log file, and log server) after the log filter function is configured. In some cases, you may want to filter logs only for certain destinations. For example, you may need the logs filtered out for the terminal on the log file or log server. In these cases, you need to set log filter rules for the terminal direction.

2. You can set the filter direction to multiple destinations by separating each other with a vertical line "|" or only one destination.

3) Filter type: sets the log information filter type. The configuration takes effect globally.

logging filter type { contains-only | filter-only } //The default value is **filter-only**, indicating that only filter is used.

Parameter description

contains-only Indicates that only logs containing keywords specified in the filter rule are output.

filter-only Indicates that logs containing keywords specified in the filter rule are filtered out and not output.

Tips

1. In some scenarios, a module may output too much log information that it may causes screen downpour on the terminal with few valuable information being displayed. In this case, you can use the filter-only mode to filter out undesired log information.
2. In some scenarios, you may want to check whether a certain type of log information is generated only. In this case, you can use the contain-only mode to output logs matching the filter rule to the terminal for observation.
3. In actual application, the two filter modes are mutually exclusive. Choose one filter mode only.

Configuration example

[Example 1]

[Requirement]

Assume there are following log information filtering requirements on the live network:

1. Set the filter direction to **terminal** and **server**.
2. Set the filter mode to **filter-only**.
3. Set the filter rule to **single-match** and module name to **SYS**.
2. Set the filter mode to **filter-only**.
3. Set the filter rule to **single-match** and module name to **SYS**.
3. Set the filter rule to **single-match** and module name to **SYS**.

[Configuration method]

Configure log information filter on the system.

```
Ruijie# configure terminal
Ruijie(config)# logging filter direction server
Ruijie(config)# logging filter direction terminal
Ruijie(config)# logging filter type filter-only
Ruijie(config)# logging filter rule single-match module SYS
```

[Verification method]

1. Run the **show running-config | include logging** command to check the parameter configuration.
2. Check the output log information on the system by entering and quitting the global configuration mode

```
Ruijie#configure
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#exit
```

2.3 Clock

2.3.1 Local Clock

I. Requirements

System time plays a very important role for troubleshooting and logs .We suggest you to deploy local clock to a scenario in which there're only a few nodes with a small maintenance.

II. Configuration Steps

```
Ruijie>enable
Ruijie#configure terminal          ----->enter global configuration mode
Ruijie(config)#clock timezone beijing 8 ----->set timezone to UTC +8
Ruijie(config)#exit
Ruijie#clock set 18:00:00 12 3 2013 ----->set clock in format "hh:mm:ss month day year"
Ruijie(config)#end
Ruijie#write                      ----->double confirm and save configuration
```

III. Verification

```
Ruijie#show clock
18:01:03 beijing Tue, Dec 3, 2013
```

2.3.2 NTP

Overview

Network Time Protocol (NTP) is designed for time synchronization on network devices. A device can synchronize its clock source and the server. Moreover, the NTP protocol can provide precise time correction (less than one millisecond on the LAN and dozens of milliseconds on the WAN, compared with the standard time) and prevent from attacks by means of encryption and confirmation.

To provide precise time, NTP needs precise time source, the Coordinated Universal Time (UTC). The NTP may obtain UTC from the atom clock, observatory, satellite or Internet. Thus, accurate and reliable time source is available.

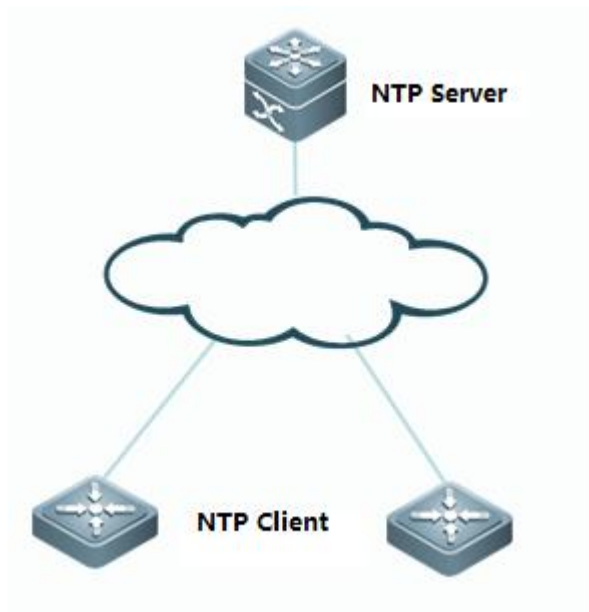
To prevent the time server from malicious destroying, an authentication mechanism is used by the NTP to check whether the request of time correction really comes from the declared server, and check the path of returning data. This mechanism provides protection of anti-interference.

Ruijie switches support the NTP client and server. That is, the switch can not only synchronize the time of server, but also be the time server to synchronize the time of other switches. But when the switch works as the time server, it only support the unicast server mode.

I. Requirements

Switch synchronizes system clock to NTP Server in order to keep system clock more accurate.

II. Network Topology



III. Configuration Tips

1. Basic network routes setting
2. (Optional) Configuring a switch as NTP Server
3. Configuring a switch as NTP client
4. (Optional) Specifying an interface on switch to communicate with NTP Server

IV. Configuration Steps

NTP configuration without authentication

1. Basic network routes setting

Ensure that NTP client can communicate with the NTP server

2. (Optional) Configuring a switch as NTP Server

Note:

Mostly NTP server is a particular server rather than a switch in production network. This example shows how to configure a switch as a NTP server:

```
Ruijie(config)#ntp master
```

3. Configuring a switch as NTP client

```
Ruijie(config)#ntp server 192.168.2.1 ----->set NTP server IP address
Ruijie(config)#ntp update-calendar ----->allow system to save clock in hardware even power interruption
```

4. (Optional) Specifying a interface on switch to communicate with NTP Server

```
Ruijie(config)#ntp server 192.168.1.2 source loopback 0 -----> specify interface loopback 0 to communicate with NTP
Server
```

NTP configuration with authentication

1. Basic network routes setting

Ensure that NTP client can communicate with the NTP server

2. (Optional) Configuring a switch as NTP Server

Note:

Mostly NTP server is a particular server rather than a switch in production network. This example shows how to configure a switch as a NTP server and how to configure NTP authentication on a switch NTP Server

```
Ruijie(config)#ntp master
Ruijie(config)#ntp authenticate ----->enable NTP authentication
Ruijie(config)#ntp authentication-key 6 md5 ruijie ----->NTP key id is "6" , and password is "ruijie"
Ruijie(config)#ntp trusted-key 6
```

4. Configuring a switch as NTP client

```
Ruijie(config)#ntp update-calendar ----->allow system to save clock in hardware even power interruption
Ruijie(config)#ntp authenticate ----->enable NTP authentication
Ruijie(config)#ntp authentication-key 6 md5 ruijie ----->NTP key id is "6" , and password is "ruijie"
Ruijie(config)#ntp trusted-key 6
Ruijie(config)#ntp server 192.168.2.1 key 6 ----->apply key id 6 to corresponding NTP server 192.168.2.1
```

5. (Optional) Specifying a interface on switch to communicate with NTP Server

```
Ruijie(config)#ntp server 192.168.1.2 source loopback 0 ----->specify interface loopback 0 to communicate with
NTP Server
```

V. Verification

1. This example displays the clock on NTP server

```
Switch-A#show clock
10:53:23 UTC Tue, Mar 12, 2013 → NTP Server clock
```

2. This example displays the clock on NTP client before synchronization

```
Switch-B#show clock
02:40:19 UTC Tue, Mar 12, 2013
```

→ NTP client clock

3. This example displays NTP status on NTP client before synchronization

```
Switch-B#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 0.000000 sec
reference time is 0.0 (00:00:00.000 UTC Thu, Jan 1, 1970)
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00000 msec, peer dispersion is 0.00000 msec
```

4. System returns a message after synchronizing successfully:

*Mar 12 10:55:04: %SYS-6-CLOCKUPDATE: System clock has been updated to 10:55:04 UTC Tue Mar 12 2013.

This example displays NTP status on NTP client before synchronization

```
Switch-B#show ntp status
Clock is synchronized, stratum 13, reference is 192.168.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 0.000000 sec
reference time is D4E98804.A92CF0F9 (10:55:00.000 UTC Tue, Mar 12, 2013)
clock offset is 29575.68187 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

2.4 Configuring a Layer 2 Port

2.4.1 Port Description

Function Overview

Port description is very important for daily maintenance and trouble shooting. We suggest you to use the format "**Link-peer name-peer port**" to define port description. For example:

```
Ruijie(config-if-GigabitEthernet 0/1)#description Link-to-WLZX_Core_S8610_1-G1/2
```

I. Configuration Steps

Configuring port description on G0/1

```
Ruijie#configure terminal
```

```
Ruijie(config)#interface gigabitEthernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)#description Link-to-Core-S8610_1-G2/3
```

```
Ruijie(config-if-GigabitEthernet 0/1)#end
Ruijie#write
```

II. Verification

```
Ruijie#show interfaces description
```

| Interface | Status | Administrative | Description |
|---------------------|--------|----------------|---------------------------|
| GigabitEthernet 0/1 | down | up | Link-to-Core-S8610_1-G2/3 |
| GigabitEthernet 0/2 | down | up | |
| GigabitEthernet 0/3 | down | up | |

2.4.2 Speed, Duplex and Flow control

Overview

By default, speed and duplex negotiate automatically. You can also set speed and duplex manually to ensure that both ends of a link have the same speed and duplex. Usually we keep the default setting for flow control.

I. Configuration Steps

In the following example, the "speed" config-interface command with the keyword 100 is used to manually set speed on Giga0/24 to 100M

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#int gigabitEthernet 0/24
Ruijie(config-if-GigabitEthernet 0/24)#speed 100
Ruijie(config-if-GigabitEthernet 0/24)#end
Ruijie#write
```

In the following example, the "duplex" command config-interface with the keyword full is used to manually set duplex on Giga0/24 to full duplex

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#int gigabitEthernet 0/24
Ruijie(config-if-GigabitEthernet 0/24)#duplex full
Ruijie(config-if-GigabitEthernet 0/24)#end
Ruijie#write
```

This example shows how to disable flow control feature on Giga0/1

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#flowcontrol off
```

```
Ruijie(config-if-GigabitEthernet 0/1)#end
Ruijie#write
```

Note: By default flow control feature is enabled, but different switches vary, and you can enter "**show interface**" privilege EXEC command to verify.

II. Verification

This example shows how to display interface status including duplex and speed.

```
Ruijie#show interfaces status
Interface      Status  Vlan  Duplex  Speed  Type
-----
GigabitEthernet 0/1    down    1     Unknown Unknown copper
GigabitEthernet 0/2    up      1     Full    1000M  copper
GigabitEthernet 0/3    down    1     Unknown Unknown copper
```

2.4.3 Combo Port

I. Configuration Steps

Following example shows how to convert combo mode on Giga0/23 to fiber

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/23
Ruijie(config-if-GigabitEthernet 0/23)#medium-type fiber ----->convert combo mode to fiber
Ruijie(config-if-GigabitEthernet 0/23)#end
Ruijie#write ----->confirm and save
```

Following example shows how to convert combo mode on Giga0/23 to copper

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/23
Ruijie(config-if-GigabitEthernet 0/23)#medium-type copper ----->convert combo mode to copper
Ruijie(config-if-GigabitEthernet 0/23)#end
Ruijie#write
```

II. Verification

1. To display combo mode status, enter "show interface status" privilege EXEC command

```
Ruijie#show interfaces status
Interface      Status  Vlan  Duplex  Speed  Type
-----
GigabitEthernet 0/22    down    1     Unknown Unknown copper
GigabitEthernet 0/23    up      1     Full    1000M  fiber
GigabitEthernet 0/24    down    1     Unknown Unknown copper
```

2. This example shows how to display the transceiver information of Giga0/23

```
Ruijie#show interfaces g0/23 transceiver
Transceiver Type      : 1000BASE-LX-SFP
Connector Type        : LC
Wavelength(nm)       : 1310
Transfer Distance     :
    SMF fiber
        -- 10km
    50/125 um OM2 fiber
        -- 550m
    62.5/125 um OM1 fiber
        -- 550m
Digital Diagnostic Monitoring : NO ----->This transceiver doesn't support DDM . DDM provides you the
light intensity of receiving and sending direction.
Vendor Serial Number      : LP201093226676
```

3. This example shows how to display the light intensity of a 10G transceiver which supports DDM

```
Ruijie#show interfaces tenGigabitEthernet 1/25 transceiver diagnosis
Current diagnostic parameters[AP:Average Power]:
Temp(Celsius)  Voltage(V)      Bias(mA)          RX power(dBm)      TX power(dBm)
26(OK)         3.26(OK)         5.22(OK)         -3.65(OK)[AP]     -2.09(OK)
```

4. This example shows how to display the transceiver alarm

```
Ruijie#show interfaces tenGigabitEthernet 1/25 transceiver alarm -----> if the transceivers is plugged in , but the
port doesn't come up , system returns the following warning message
RX power low
RX loss of signal
Module not ready
RX not ready
RX CDR loss of lock

Ruijie#show interfaces tenGigabitEthernet 1/25 transceiver alarm ----->if the transceivers is plugged in and the
port comes up , system returns no warning message
```

Ruijie transceivers specification

1. MINI-GBIC transceiver:

| GBIC/SFP | Wavelength (nm) | Fiber Type | Support DDM (Yes/No) | Transmitting Sensitivity/dBm | | Receiving Sensitivity/dBm | |
|------------------------|-----------------|-------------|----------------------|------------------------------|-----|---------------------------|-----|
| | | | | MIN | MAX | MIN | MAX |
| FE-SFP-LX-MM1310 | 1310 | Multimode | Yes | -22 | -14 | -30 | -14 |
| FE-SFP-LH15-SM1310 | 1310 | Single-mode | Yes | -15 | -8 | -28 | -8 |
| Mini-GBIC-SX | 850 | Multimode | No | -9.5 | -3 | -17 | 0 |
| Mini-GBIC-LX | 1310 | Single-mode | No | -9.5 | -3 | -20 | -3 |
| GE-eSFP-SX-MM850 | 850 | Multimode | Yes | -9.5 | -3 | -17 | 0 |
| GE-eSFP-LX-SM1310 | 1310 | Single-mode | Yes | -9.5 | -3 | -20 | -3 |
| Mini-GBIC-LH40 | 1310 | Single-mode | Yes | -2 | 3 | -22 | -3 |
| Mini-GBIC-ZX50 | 1550 | Single-mode | Yes | -5 | 0 | -22 | -3 |
| Mini-GBIC-ZX80 | 1550 | Single-mode | Yes | 0 | 4.7 | -22 | -3 |
| Mini-GBIC-ZX100 | 1550 | Single-mode | Yes | 0 | 5 | -30 | -9 |
| SDH155-SFP-SX-MM850 | 850 | Multimode | No | -10 | -4 | -25 | 0 |
| SDH155-SFP-SX-MM1310 | 1310 | Multimode | No | -20 | -14 | -30 | -14 |
| SDH155-SFP-LH15-SM1310 | 1310 | Single-mode | No | -15 | -8 | -28 | -8 |
| SDH155-SFP-LH40-SM1310 | 1310 | Single-mode | No | -5 | 0 | -34 | -8 |

MINI-GBIC cabling specification:

| GBIC/SFP | Wavelength (nm) | Fiber Type | Core Size(μm) | Maximum Cabling Distance |
|------------------------|-----------------|-------------|---------------|--------------------------|
| FE-SFP-LX-MM1310 | 1310 | Multimode | 62.5/125 | 2km |
| FE-SFP-LH15-SM1310 | 1310 | Single-mode | 9/125 | 15km |
| Mini-GBIC-SX | 850 | Multimode | 62.5/125 | 275m |
| | | | 50/125 | 550m |
| Mini-GBIC-LX | 1310 | Single-mode | 9/125 | 10km |
| GE-eSFP-SX-MM850 | 850 | Multimode | 62.5/125 | 275m |
| | | | 50/125 | 550m |
| GE-eSFP-LX-SM1310 | 1310 | Single-mode | 9/125 | 10km |
| Mini-GBIC-LH40 | 1310 | Single-mode | 9/125 | 40km |
| Mini-GBIC-ZX50 | 1550 | Single-mode | 9/125 | 50km |
| Mini-GBIC-ZX80 | | | | 80km |
| Mini-GBIC-ZX100 | | | | 100km |
| SDH155-SFP-SX-MM850 | 850 | Multimode | 62.5/125 | 500m |
| SDH155-SFP-SX-MM1310 | 1310 | | | 2km |
| SDH155-SFP-LH15-SM1310 | 1310 | Single-mode | 9/125 | 15km |
| SDH155-SFP-LH40-SM1310 | | | | 40km |
| SDH155-SFP-LH80-SM1550 | 1550 | Single-mode | 9/125 | 80km |

2. 10G XFP

| Model | Wave length (nm) | Fiber Type | Core Size (μm) | Modular Bandwidth (MHz • km) | Maximum Cabling Distance | Sending Optical Density (dBm) | | Receiving Optical Density (dBm) | |
|--------------------|------------------|----------------------------|----------------|------------------------------|--------------------------|-------------------------------|-----|---------------------------------|-----|
| | | | | | | MIN | MAX | MIN | MAX |
| 10GBASE-SR-XFP | 850 | Multimode (Lc connector) | 62.5 | 200 | 33m | -5 | -1 | -7.5 | 0.5 |
| | | | | 160 | 22m | | | | |
| | | | 50 | 2000 | 300m | | | | |
| | | | | 500 | 82m | | | | |
| | | | | 400 | 66m | | | | |
| 10GBASE-LR-XFP | 1310 | Single-mode (Lc connector) | 9 | N/A | 10km | -4.8 | 0.5 | -10.3 | 0.5 |
| 10GBASE-ER-XFP | 1550 | Single-mode (Lc connector) | 9 | N/A | 40km | -1 | 2 | -11.3 | -1 |
| XG-XFP-ZR80-SM1550 | 1550 | Single-mode (Lc connector) | 9 | N/A | 80km | 0 | 4 | -23 | -7 |

3. 10G SFP+

| Model | Wave length (nm) | Fiber Type | Core Size (μm) | Modular Bandwidth (MHz • km) | Maximum Cabling Distance | Sending Optical Density (dBm) | | Receiving Optical Density (dBm) | |
|------------------|------------------|----------------------------|----------------|------------------------------|--------------------------|-------------------------------|-----|---------------------------------|-----|
| | | | | | | MIN | MAX | MIN | MAX |
| XG-SFP-SR-MM850 | 850 | Multimode (Lc connector) | 62.5 | 200 | 33m | -5 | -1 | -7.5 | 0.5 |
| | | | | 160 | 26m | | | | |
| | | | 50 | 2000 | 300m | | | | |
| | | | | 500 | 82m | | | | |
| | | | | 400 | 66m | | | | |
| XG-SFP-LR-SM1310 | 1310 | Single-mode (Lc connector) | 9 | N/A | 10km | -8.2 | 0.5 | -10.3 | 0.5 |
| XG-SFP-ER-SM1550 | 1550 | Single-mode (Lc connector) | 9 | N/A | 40km | -4.7 | 4 | -11.3 | -1 |

2.4.4 Access or Trunk Port

Note: By default, trunk port carries traffic for all vlans that is created, and we strongly recommend you to prune every trunk port to allow only the traffic of useful vlan pass through in case that unknown unicast, broadcast and multicast packets floods through the overall network, leading to a heavier CPU burden and useless consumption of system resource.

I. Configuration Steps

1. Configuring access port

The following example shows how to configure interface F0/1 as an access port and assign interface F0/1 to VLAN 100

```
Ruijie>en
Ruijie#conf t
Ruijie(config)#interface fastEthernet 0/1
```

```
Ruijie(config-if)#switchport mode access
Ruijie(config-if)#switchport access vlan 100
Ruijie(config-if)#end
Ruijie#wr
```

Note: By default, all ports are access mode and belongs to VLAN 1

Enter "show vlan" privilege EXEC command to verify that interface F0/1 belongs to VLAN 100

```
Ruijie# show vlan
VLAN Name                Status    Ports
-----
 1 VLAN0001              STATIC    Fa0/3, Fa0/4, Fa0/5
                               Fa0/6, Fa0/7, Fa0/8, Fa0/9
                               Fa0/10, Fa0/11, Fa0/12, Fa0/13
                               Fa0/14, Fa0/15, Fa0/16, Fa0/17
                               Fa0/18, Fa0/19, Fa0/20, Fa0/21
                               Fa0/22, Fa0/23, Fa0/24, Fa0/25
                               Fa0/26, Fa0/27, Fa0/28, Fa0/29
                               Fa0/30, Fa0/31, Fa0/32, Fa0/33
                               Fa0/34, Fa0/35, Fa0/36, Fa0/37
                               Fa0/38, Fa0/39, Fa0/40, Fa0/41
                               Fa0/42, Fa0/43, Fa0/44, Fa0/45
                               Fa0/46, Fa0/47, Fa0/48, Gi0/49
                               Gi0/50
100 VLAN0100             STATIC    Fa0/1,Fa0/2
```

2. Configuring trunk port

The following example shows how to configure interface G0/49 as a trunk port

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/49
Ruijie(config-if)#switchport mode trunk
Ruijie(config-if)#end
```

In the following example, "show interface trunk" privilege EXEC command is used to verify all trunk port status

```
Ruijie# show interfaces trunk
Interface                Mode    Native VLAN VLAN lists
-----
FastEthernet 0/48        Off    1          ALL
GigabitEthernet 0/49      On     1          ALL
GigabitEthernet 0/50      Off    1          ALL
```

3. Pruning a Trunk port (Mandatory)

This example shows how to prune a trunk port to carry traffic only for vlan 5, 10 and 20-30

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)#switchport trunk allowed vlan remove 1-4,6-9,11-19,31-4094
Ruijie(config-if-GigabitEthernet 0/1)#end
Ruijie#wr
```

2.4.5 Storm Control

Overview

1. We suggest you to apply storm-control on edge port on access switch and don't apply storm-control on uplink port.
2. If access switch doesn't support storm-control, we suggest you to apply storm-control on distribution switch.
3. The limitation of 100 pps to 300 pps for unknown unicast/broadcast/multicast packets is proper.

I. Configuration Steps

To configure storm control on a port with keyword level, perform this task:

```
Ruijie>enable
Ruijie#configure termina
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#storm-control broadcast level 1 ----->storm-control limits the number of
broadcast packets to 1% of the bandwidth that is 1G*1%=10M
Ruijie(config-if-GigabitEthernet 0/1)#storm-control unicast level 1 ----->storm-control limites the number of
unknown unicast packets to 1% of the bandwidth that is 1G*1% =10M
Ruijie(config-if-GigabitEthernet 0/1)#storm-control multicast level 1
```

To configure storm control on a port with keyword pps, perform this task:

```
Ruijie>enable
Ruijie#configure termina
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#storm-control broadcast pps 200 ----->storm-control limits the number of
broadcast packets to 200 packets per seconds
Ruijie(config-if-GigabitEthernet 0/1)#storm-control unicast pps 200 ----->storm-control limits the number of
unknown unicast packets to 200 packets per seconds
Ruijie(config-if-GigabitEthernet 0/1)#storm-control multicast 200
Ruijie(config-if-GigabitEthernet 0/1)#end
```

II. Verification

```
Ruijie#show storm-control
Interface          Broadcast Control Multicast Control Unicast Control Action
```

| | | | | | | | |
|---------------------|----------|---|----------|---|----------|---|------|
| GigabitEthernet 0/1 | 1 | % | 1 | % | 1 | % | none |
| GigabitEthernet 0/2 | Disabled | | Disabled | | Disabled | | none |
| GigabitEthernet 0/3 | Disabled | | Disabled | | Disabled | | none |

2.5 SNMP

2.5.1 SNMPV1/V2

Overview

SNMP: As the abbreviation of Simple Network Management Protocol, SNMP has been a network management standard (RFC1157) since the August, 1988. So far, the SNMP becomes the actual network management standard for the support from many manufacturers. It is applicable to the situation of interconnecting multiple systems from different manufacturers. Administrators can use the SNMP protocol to query information, configure network, locate failure and plan capacity for the nodes on the network. Network supervision and administration are the basic function of the SNMP protocol.

SNMP versions:

SNMPv1 : The first formal version of the Simple Network Management Protocol, which is defined in RFC1157

SNMPv2C: Community-based Administrative Framework for SNMPv2, an experimental Internet protocol defined in RFC1901.

SNMPv3: Offers the following security features by authenticating and encrypting packets:

1. Ensure that the data are not tampered during transmission;
2. Ensure that the data come from a valid data source;
3. Encrypt packets to ensure the data confidentiality;

| Model | Level | Authentication | Encryption | Description |
|---------|--------------|------------------|------------|--|
| SNMPv1 | noAuthNoPriv | Community string | None | Ensures the data validity through community string. |
| SNMPv2c | noAuthNoPriv | Community string | None | Ensures the data validity through community string. |
| SNMPv3 | noAuthNoPriv | User name | None | Ensures the data validity through user name. |
| SNMPv3 | authNoPriv | MD5 or SHA | None | Provides HMAC-MD5 or HMAC-SHA-based authentication mechanism. |
| SNMPv3 | authPriv | MD5 or SHA | DES | Provides HMAC-MD5 or HMAC-SHA-based authentication mechanism and CBC-DES-based encryption mechanism. |

Both the SNMPv1 and SNMPv2C use a community-based security framework. They restrict administrator's operations on the MIB by defining the host IP addresses and community string. With the Get Bulk retrieval mechanism, SNMPv2C sends more detailed error information type to the management station. Get Bulk allows you to obtain all the information or a great volume of data from the table at a time, and thus reducing the times of request and response. Moreover, SNMPv2C improves the capability of handing errors, including expanding error codes to distinguish different kinds of errors, which are represented by one error code in SNMPv1. Now, error types can be distinguished by error codes. Since there may be the management workstations supporting SNMPv1 and SNMPv2C in a network, the SNMP agent must be able to recognize both SNMPv1 and SNMPv2C messages, and return the corresponding version of messages.

I. Requirements

1. Only SNMP network manager (IP:192.168.1.2/24) can access switch SNMP service with community string "ruijie"
2. SNMP agent on switch sends SNMP trap to SNMP manager actively
3. SNMP manager can get basic information of switch ---location, contact method and chassis id

II. Network Topology



III. Configuration Tips

1. Set Read-Only community string and Read-Write community string on switch independently
2. Define ACL to allow authorized SNMP manager to access SNMP agent of switch only
3. Enable SNMP trap
4. Configure SNMP manager

IV. Configuration Steps

1. Define an access-list named "abc" and an entry to permit IP address of SNMP manager

```
Ruijie(config)#ip access-list standard abc
Ruijie(config-std-nacl)#permit host 192.168.1.2
Ruijie(config-std-nacl)#exit
```

2. Set read-write community string to "ruijie" and read-only community string to "public", then associate both community strings with ACL to allow only the SNMP manager to access SNMP agent of switch only

```
Ruijie(config)#snmp-server community ruijie rw abc
Ruijie(config)#snmp-server community public ro abc
```

3. SNMP agent on switch actively sends trap to SNMP network manager

```
Ruijie(config)#snmp-server host 192.168.1.2 traps ruijie ----->by default , SNMP trap version is version 1
Ruijie(config)#snmp-server host 1.1.1.1 version 2c ruijie ----->set SNMP trap version to version 2c
```

4. Enable trap feature

```
Ruijie(config)#snmp-server enable traps
```

5. Set SNMP optional parameters

Set location

```
Ruijie(config)#snmp-server location fuzhou
```

Set contact method

```
Ruijie(config)#snmp-server contact ruijie.com.cn
```

Set chassis-id

```
Ruijie(config)#snmp-server chassis-id 1234567890
```

6. Assign a management IP address to SVI 1

```
Ruijie(config)#interface vlan 1
```

```
Ruijie(config-if-VLAN 1)#ip address 192.168.1.1 255.255.255.0
```

7. Save configuration


```
Ruijie(config-if-VLAN 1)#end
```

```
Ruijie#wr
```

V. Verification

1. This example shows how to verify SNMP agent status

```
Ruijie# show service
ssh-server      : disabled
telnet-server   : enabled
web-server      : enabled
snmp-agent      : enabled
```




Following example provides how to disable SNMP agent if snmp agent issue leads to heavy load of CPU :

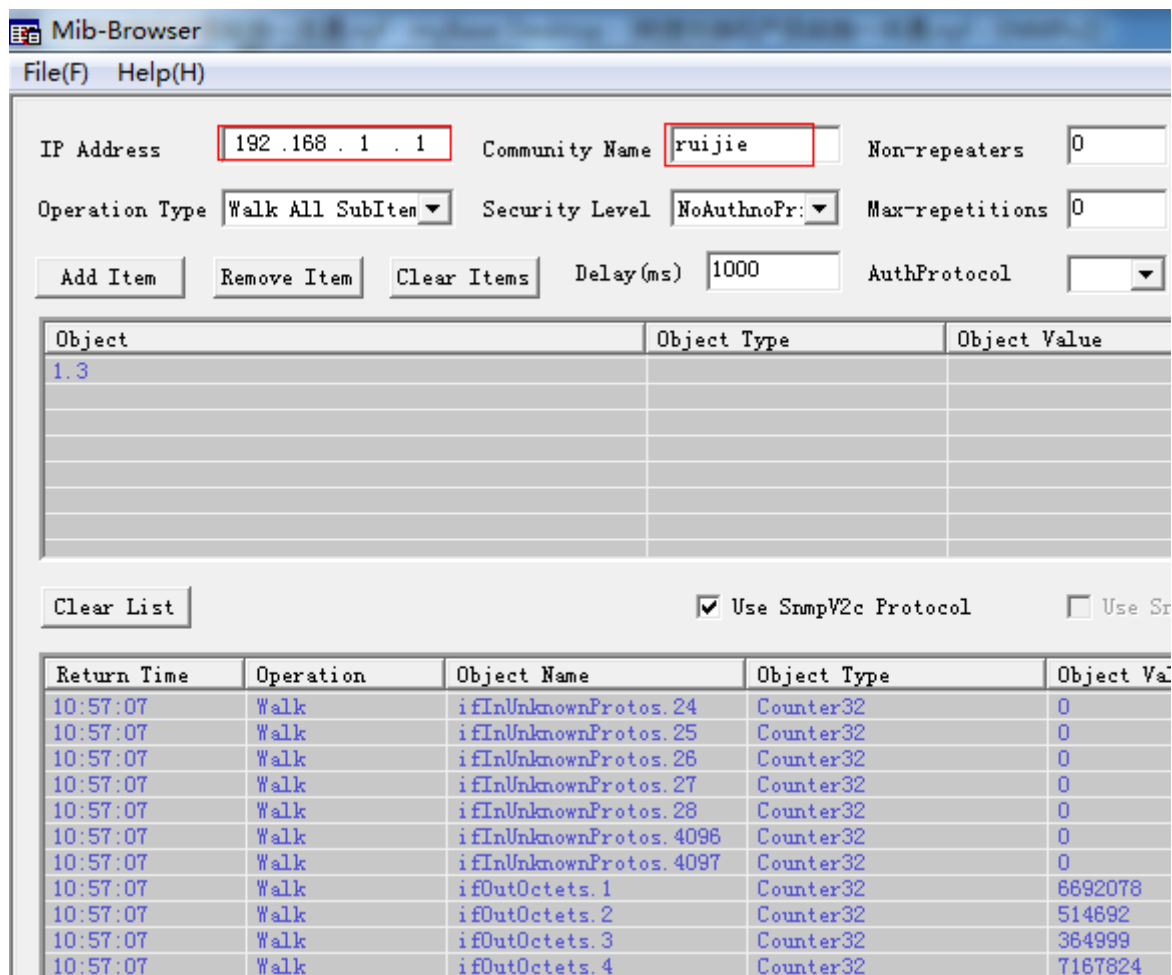
```
Ruijie(config)#no enable service snmp-agent
```

2. This examples shows how to display SNMP host information

```
Ruijie#show snmp host
Notification host: 192.168.1.2
udp-port: 162
type: trap
user: ruijie
security model: v1
```



3. This example shows how to access the SNMP agent in a SNMP manager using "Mib-Browser"



4. Other SNMP manager except for 192.168.1.2 cannot access SNMP agent at the same time.

2.5.2 SNMPV3

I. Requirements

- 1) The SNMP manager can access the SNMP agent on switch by applying user-based security model. The user name is "admin", authentication mode is MD5, authentication key is "ruijie", encryption algorithm is DES56, and the encryption key is "123"
- 2) User "admin" can read the MIB objects under System (1.3.6.1.2.1.1) node, and can only write MIB objects under SysContact (1.3.6.1.2.1.1.4.0) node.
- 3) The switch can actively send authentication and encryption messages to the SNMP manager

II. Network Topology



III. Configuration Tips

1. Create MIB view and specify the included or excluded MIB objects.
2. Create SNMP group and set the version to "v3"; specify the security level of this group, and configure the read-write permission of the view corresponding to this group.
3. Create user name and associate the corresponding SNMP group name in order to further configure the user's permission to access MIB objects; meanwhile, configure the version number to "v3" and the corresponding authentication mode, authentication key, encryption algorithm and encryption key.
4. Configure the address of SNMP manager, configure the version "3" and configure the security level to be adopted.

IV. Configuration Steps

Configuring switch:

```
Ruijie(config)#no enable service snmp-agent Ruijie(config)#snmp-server view view1 1.3.6.1.2.1.1 include
-----> Create a MIB view of "view1" and include the MIB object of 1.3.6.1.2.1.1
Ruijie(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include -----> Create a MIB view of
"view2" and include the MIB object of 1.3.6.1.2.1.1.4.0
Ruijie(config)#snmp-server group group1 v3 priv read view1 write view2 ----->Create a group named
"g1" ,using SNMPv3 ; configure security level to "priv" ,and can read "view1" and write "view2"
Ruijie(config)#snmp-server user admin group1 v3 auth md5 ruijie priv des56 ruijie123 ----->Create a user
named "admin", which belongs to group "group1"; using SNMPv3 and authentication mode is "md5", authentication
key is "ruijie", encryption mode is "DES56" and encryption key is "123".
Ruijie(config)#snmp-server host 192.168.1.2 traps version 3 priv admin ----->Configure the SNMP server
address as 192.168.1.2 , using SNMPv3,then configure security level to "priv" and associate the corresponding
user name of "admin"
Ruijie(config)#snmp-server enable traps ----->Enable
the Agent to actively send traps to NMS
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.1.1 255.255.255.0
Ruijie(config-if-VLAN 1)#end
```

Set SNMP optional parameters

```
Ruijie(config)#snmp-server location fuzhou
Ruijie(config)#snmp-server contact ruijie.com.cn
Ruijie(config)#snmp-server chassis-id 1234567890
```

Note: If you don't create a new SNMP view, Ruijie switch uses the default SNMP view named "default", including MIB object of 1

Minimum SNMPv3 configuration example:

```
snmp-server group group1 v3 priv read default write default
snmp-server user admin group1 v3 auth md5 ruijie priv des56 ruijie123
snmp-server host 192.168.1.2 traps version 3 priv admin
snmp-server enable traps
```

V. Verification

1. This example shows how to verify SNMP agent status

```
Ruijie# show service
ssh-server      : disabled
telnet-server   : enabled
web-server      : enabled
snmp-agent      : enabled
```

Following example provides how to disable SNMP agent if snmp agent issue leads to heavy load of CPU :

```
Ruijie(config)#no enable service snmp-agent
```

2. Following examples show how to display snmp view, snmp group and snmp user individually

```
Ruijie#show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1
```

```
Ruijie#show snmp group
groupname: group1
securityModel: v3
securityLevel:authPriv
readview: view1
writeview: view2
notifyview:
```

```
Ruijie#show snmp user
User name: admin
Engine ID: 800013110314144b1b546c
storage-type: permanent      active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: group1
```

2.6 SPAN

2.6.1 Many to one mirror

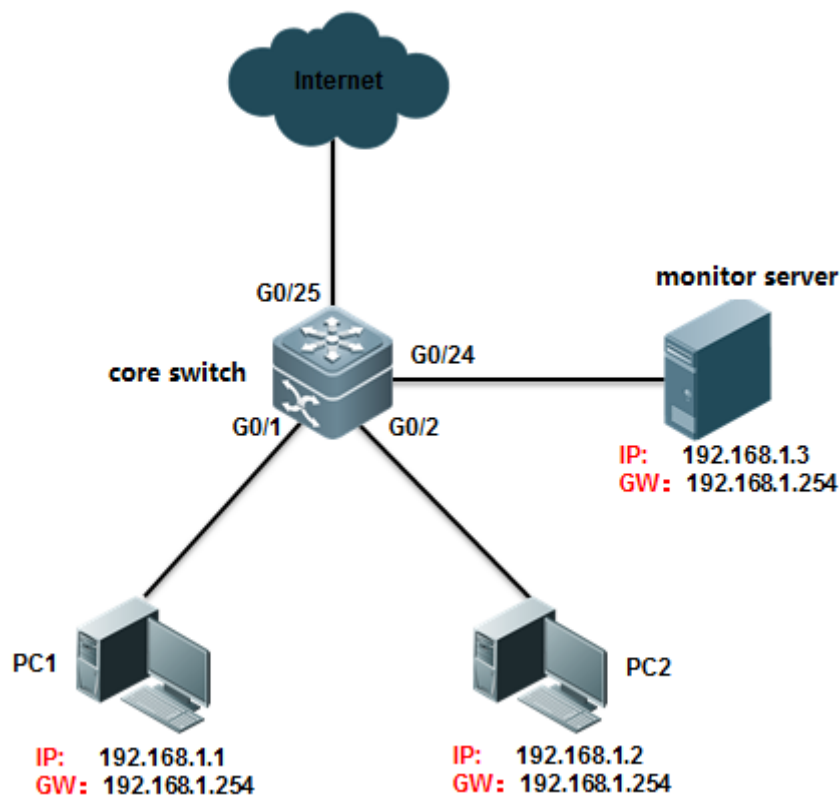
Overview

With SPAN, you can analyze the communications between ports by copying a frame from one port to another port connected with a network analysis device or RMON analyzer. The SPAN mirrors all the packets sent/received at a port to a physical port for analysis. SPAN does not affect the exchange of packets between the source and destination ports. Instead, it copies the frames incoming/outgoing the source port to the destination port. However, the frames may be discarded on an overflowed destination port, for example, when a 100Mbps port monitors an 1000Mbps port.

I. Requirements

Core switch copies traffic of G0/1 and G0/2 on both directions to Monitor Server and Monitor Server can also visit Internet at the same time

II. Network Topology



III. Configuration Tips

Enter "monitor session" global configuration command with "**switch**" keyword to allow mirror destination port to forward additional traffic more than mirroring traffic

IV. Configuration Steps

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#monitor session 1 source interface gigabitEthernet 0/1 both ----->define G0/1 as source port in
monitor session , and both traffic directions are monitored. If you want to monitor income or outcome traffic only ,
you can use keyword rx or tx instead of both , such as "monitor session 1 source interface gigabitEthernet 0/1 rx"
Ruijie(config)#monitor session 1 source interface gigabitEthernet 0/2 both
Ruijie(config)#monitor session 1 destination interface gigabitEthernet 0/24 switch
Ruijie(config)#end
Ruijie#wr
```

V. Verification

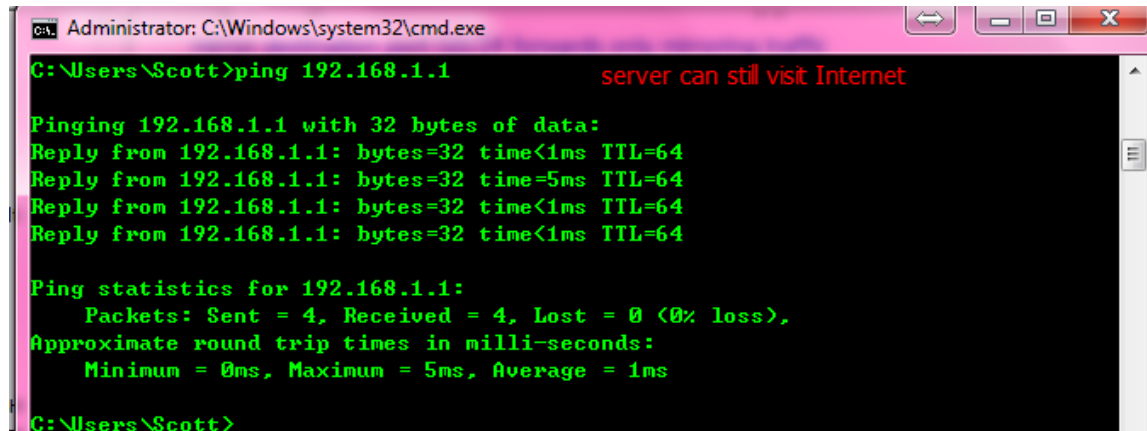
1. This example shows how to verify status of monitor session

```

Ruijie#show monitor
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/2      frame-type Both
src-intf:
GigabitEthernet 0/1      frame-type Both
dest-intf:
GigabitEthernet 0/24 mirror dst port can forward traffic after enable "switch" keyword
ntp switch on →

```

2. This examples verifies that the Monitor Server can visit Internet while monitoring



```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Scott>ping 192.168.1.1      server can still visit Internet

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms
C:\Users\Scott>

```

2.6.2 One to Many Mirror

Note: Only S8600E and N18000 series switch support one to many (or many to many) SPAN so far.

Tips: For those switches that do not support one to many SPAN, you can apply another fallback method as below:

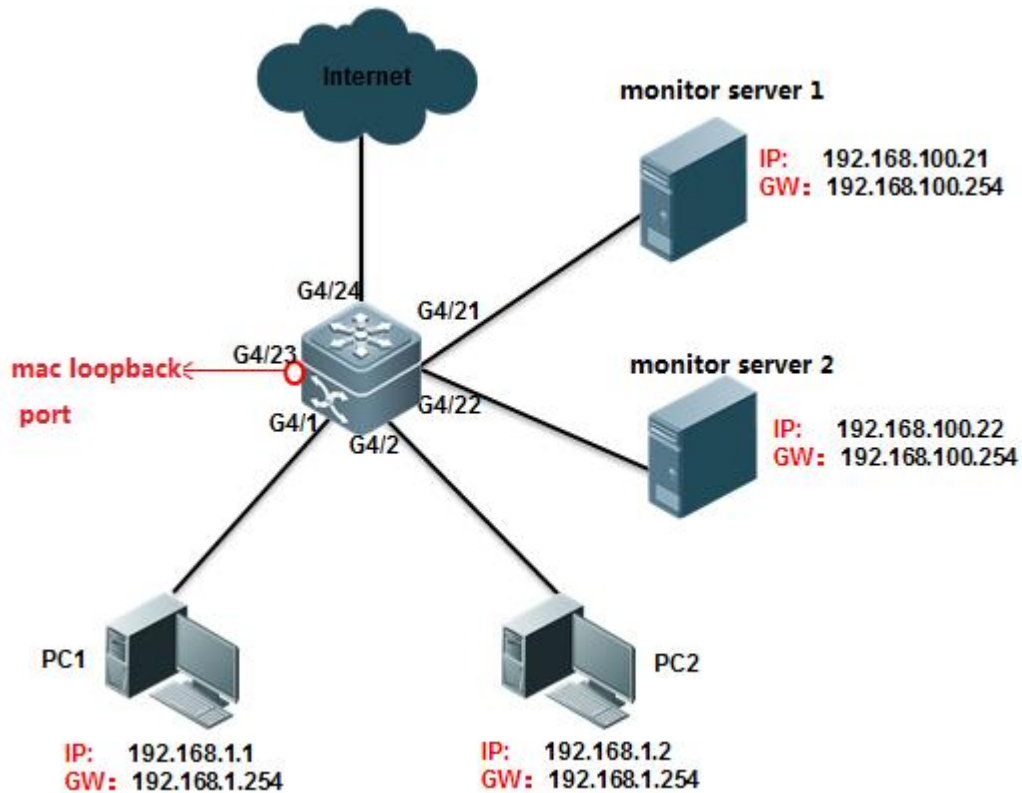
1. Configure the ordinary many to one SPAN
2. Connect a HUB to the mirror destination port, so packets floods through the HUB
3. Connect your Monitor Server to the HUB.

HUB can also be a default setting switch. You must assign ports to the remote-vlan and disable the mac-learning feature (enter "no mac-address-learning" config-interface command) and storm-control feature.

I. Requirements

Core switch copies traffic of G4/1 and G4/2 on both directions to Monitor Server 1 connected to port G4/21 and Monitor Server 2 connected to port G4/22

II. Network Topology



III. Configuration Tips

- 1) Create VLAN 100 as remote-vlan on switch
- 2) Define G4/1 and G4/2 as source port in monitor session, and both traffic directions are monitored
- 3) Create a mac-loopback port, assign this mac-loopback port to Remote vlan and define it as destination port in monitor session
- 4) Assign ports G4/21 and G4/22 to Remote vlan 100

Note:

- 1) Utilize an unused port as mac-loopback port. You cannot connect cable to this port, even so switch puts link status of mac-loopback port to up status and port LED is green
- 2) Don't configure any other commands to the mac-loopback port and don't specify "switch" keyword when configuring monitor session (monitor session 1 destination remote vlan 100 interface gigabitEthernet 4/23 no switch keyword)

IV. Configuration Steps

1. Create VLAN 100 as remote-vlan on switch

```
Ruijie#configure terminal
Ruijie(config)#vlan 100 -----> VLan 100 must be dedicated for mirroring
Ruijie(config-vlan)#remote-span
Ruijie(config-vlan)#exit
```

2. Define G4/1 and G4/2 as source port in monitor session, and both traffic directions are monitored

```
Ruijie(config)#monitor session 1 remote-source
Ruijie(config)#monitor session 1 source interface gigabitEthernet 4/1 both
Ruijie(config)#monitor session 1 source interface gigabitEthernet 4/2 both
```

3. Configure G4/23 as mac-loopback port, assign this mac-loopback port to Remote vlan and define it as destination port in monitor session

```
Ruijie(config)#interface gigabitEthernet 4/23
Ruijie(config-if-GigabitEthernet 4/23)#switchport access vlan 100
Ruijie(config-if-GigabitEthernet 4/23)#mac-loopback ----->Don't configure any other commands or
connect cable to this port
Ruijie(config-if-GigabitEthernet 4/23)#end
Ruijie(config)#monitor session 1 destination remote vlan 100 interface gigabitEthernet 4/23 switch
Ruijie# clear mac-address-table dynamic interface gigabitEthernet 4/23 -----> clear mac-address-table of this
port when finish configuring
```

4. Assign ports G4/21 and G4/22 to Remote vlan 100

```
Ruijie(config)#interface range gigabitEthernet 4/21-22
Ruijie(config-if-range)#switchport access vlan 100
Ruijie(config-if-range)#end
Ruijie#wr
```

V. Verification

1. This example shows how to verify status of monitor session

```
Ruijie#show monitor
sess-num: 1
span-type: SOURCE_SPAN
src-intf:
GigabitEthernet 4/2      frame-type Both
src-intf:
GigabitEthernet 4/1      frame-type Both
dest-intf:
GigabitEthernet 4/23
remote vlan 100
ntp_switch on
```

2. This example shows how to display configuration of port G4/23

```

Ruijie#show run int g4/23 → View configuration of G4/23
Building configuration...
Current configuration : 102 bytes
!
interface GigabitEthernet 4/23
  switchport access vlan 100
  mac-loopback
  no mac-address-learning
Ruijie#show int g4/23 status → View port status
Interface                               Status    Vlan    Duplex    Speed    Type
-----
GigabitEthernet 4/23                   up        100     Full      1000M    copper

```

VI. Script

```

conf t
vlan 100
remote-span
exit
monitor session 1 remote-source
monitor session 1 source interface gigabitEthernet 4/1 both
monitor session 1 source interface gigabitEthernet 4/2 both
monitor session 1 destination remote vlan 100 interface gigabitEthernet 4/23 switch
interface gigabitEthernet 4/23
switchport access vlan 100
mac-loopback
interface range gigabitEthernet 4/21-22
switchport access vlan 100

```

2.6.3 Flow-Based Mirroring

Scenario

Flow-based mirroring: During network troubleshooting, when the traffic on the port is high, a common mirroring analysis solution may lead to analysis failure due to limited PC performance, and it would be difficult for the system to capture required traffic packets (for example, a traffic packet of a certain MAC address, or a traffic packet originated by a designated IP address and destined for another designated IP address). In this case, you can use the flow-based mirroring analysis function. If the traffic on the port is too high for the monitoring server or log auditing server deployed on the network to carry out all the data analysis tasks, you can choose to capture specified traffic packets only.

Function Overview

Port mirroring: You can use the switched port analyzer (SPAN) to replicate packets on a specified port to the port that connects a network surveillance device on the switch for network monitoring and traffic analysis. You can monitor packets flow in and out of a source port through SPAN for fast and packet replication.

The SPAN does not change packet information or affect packet transmission. In addition, the SPAN does not have requirement on the media type for the source and destination ports. Port mirroring can be optical ports to electrical ports or electrical ports to optical ports. The SPAN has no requirement on the property of the source and destination ports. It supports mirroring from an access port to a trunk port or a trunk port to an access port.

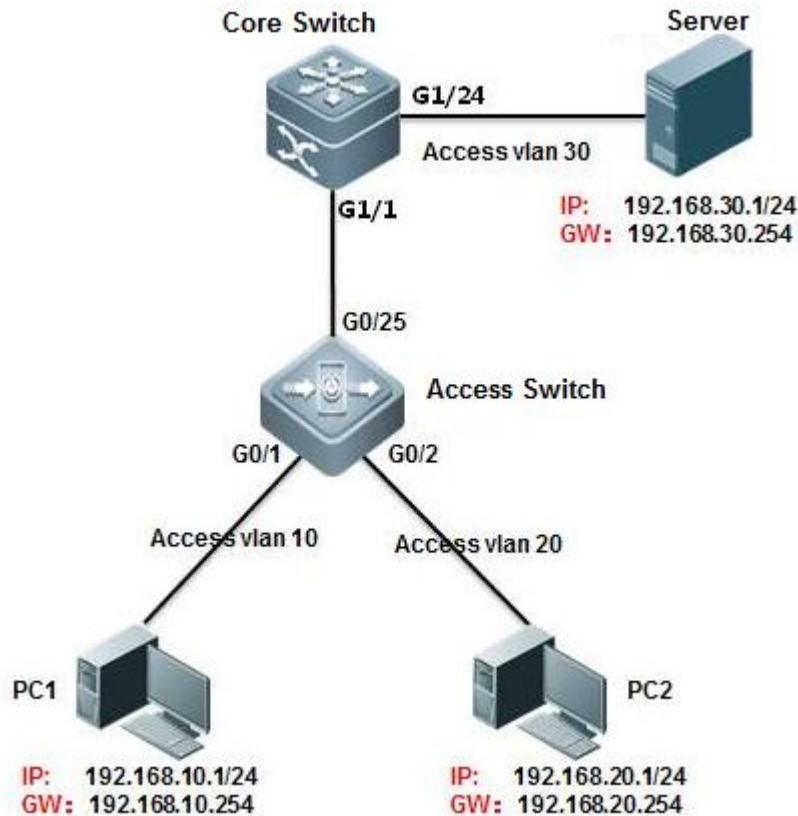
Flow-based mirroring: You can define the desired types of traffic packets (for example, PPPOE packets, IP packets on a specified network segment, and HTTP packets on TCP 80) using the ACL. Ruijie switches provide rich ACL functions, and support traffic packet matching by L2 frame types, MAC addresses, IP addresses, TCP/UDP ports, and ACL80 (the first 80 bytes of a packet). The SPAN captures traffic packets on the source port according to the defined ACL, and mirrors the traffic packets to the destination port. Traffic packets not matching the defined ACL are not mirrored.

Note: The switch supports flow-based mirroring in the RX direction (inbound on the port) only. Monitoring on the TX (outbound on the port) direction or bi-direction are not supported.

I. Networking Requirements

1. The monitoring server monitors traffic consumption on the core server by users on the 192.168.10.0/24 network segment.
2. The monitoring server monitors the traffic from the core server to the access server.

II. Network Topology



III. Configuration Tips

1. On the core server, configure the ACL to allow users on the network segment 192.168.10.0/24.
2. On the core server, configure the port mirroring function. Set the g1/1 port that connects the access server as the source port of port mirroring and enable the ACL association.
3. Set the port connecting the monitoring server (port g1/24) as the destination port of port mirroring.

IV. Configuration Steps

Configure the core server.

```
Ruijie#configure terminal
Ruijie(config)#ip access-list extended ruijie          ----->Create ACL, named as ruijie
Ruijie(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
Ruijie(config-ext-nacl)#exit
Ruijie(config)#monitor session 1 source interface gigabitEthernet 1/1 tx
Ruijie(config)#monitor session 1 source interface gigabitEthernet 1/1 rx acl ruijie -----> Set the g1/1 port that
connects the access server as the source port of port mirroring and enable the ACL association.
Ruijie(config)#monitor session 1 destination interface gigabitEthernet 1/24 switch -----> Set the port
connecting the monitoring server (port g1/24) as the destination port of port mirroring and enable switching on the
mirroring destination port.
Ruijie(config)#end
Ruijie#wr
```

V. Verification

1. Check the port mirroring state.

```
Ruijie(config)#show monitor
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 1/1          frame-type Both
rx acl id 2900
acl name ruijie
dest-intf:
GigabitEthernet 1/24
mtp_switch on                -----> Allow mirroring port forwarding data stream
```

2. Check the ACL.

```
Ruijie#show access-lists  
  
ip access-list extended ruijie  
10 permit ip 192.168.10.0 0.0.0.255 any
```

3. Capture

2.7 Featured commands

1. switchport trunk allowed vlan only x-x

Previously in 10.x version, all vlans are able to pass through trunk port by default. Engineers have to remove all vlans first, then permit vlan one by one.

By command "switchport trunk allowed vlan only x-x", only allowed vlans are able to pass through trunk port, you don't need to remove all vlan anymore.

For example:

```
Ruijie(config-if-GigabitEthernet 1/1)#show this  
Building configuration...  
switchport mode trunk  
switchport trunk allowed vlan only 1-2  
end
```

2. show this

Previously in 10.x version, engineers have to execute commands "show run" or "show run | include xxx" to check configurations. By command "show this", you can display configurations under current mode directly:

For example:

```
Ruijie(config)#int mgmt 0  
Ruijie(config-if-Mgmt 0)#show this  
Building configuration...  
!  
ip address 172.18.10.62 255.255.255.0  
gateway 172.18.10.1
```

3. show upgrade history

Previously in 10.x version, engineers have to rename firmware as "rgos.bin" before upgrading. In addition, there is no historical upgrade records.

Currently, you can give any name to firmware for convenient management purpose and system might record historical upgrade.

For example:

```
Ruijie#show upgrade history
Last Upgrade Information:
  Time:      2015-04-20 03:02:05
  Method:    LCOAL
  Package Name: N18000_RGOS11.0(2)B1_CM_install.bin
  Package Type: Distribution
```

4. debug syslog limit

Previously in 10.x version, at worst, massive system logs printing might crash device after debug is enable.

By command "debug syslog limit time seconds numbers numbers ", system logs printing is limited,

For example:

```
Ruijie#debug syslog limit ?
numbers  Syslog limited by numbers
reset    Syslog reset limit statistics
time     Syslog limited by time
```

5. one key collection

Previously in 10.x version, usually engineers have to collect information multiple times while trouble shooting which might miss the best opportunity.

By one key collection, system collects all relevant information in one time.

For example:

```
Ruijie#debug support
Ruijie(support)#tech-support ?
console  Tech-support information to terminal
package  Tech-support information to package
```

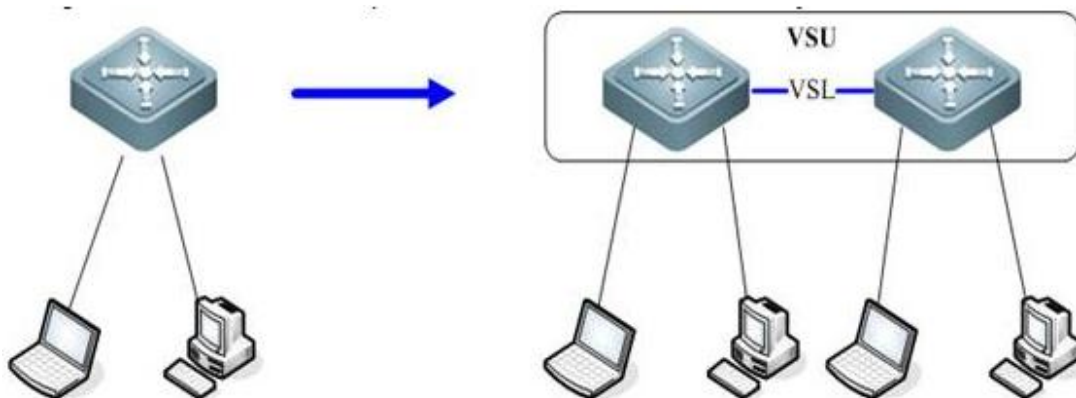
2.8 Typical Feature

2.8.1 VSU

Overview

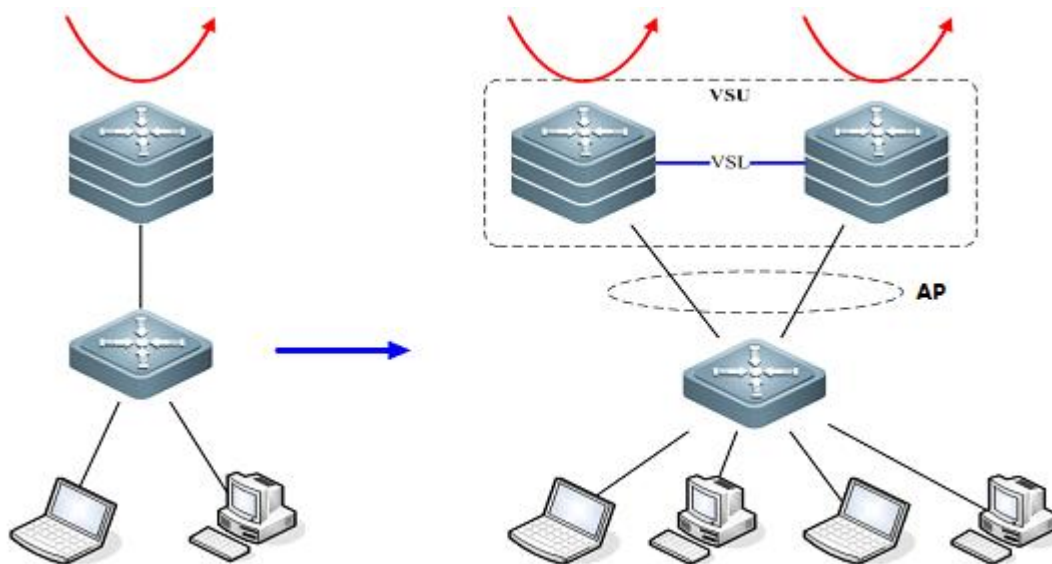
VSU expands the Port Numbers

As figure shown below, when port number on a switch runs out, you can add one more switch to the VSU to expand port numbers



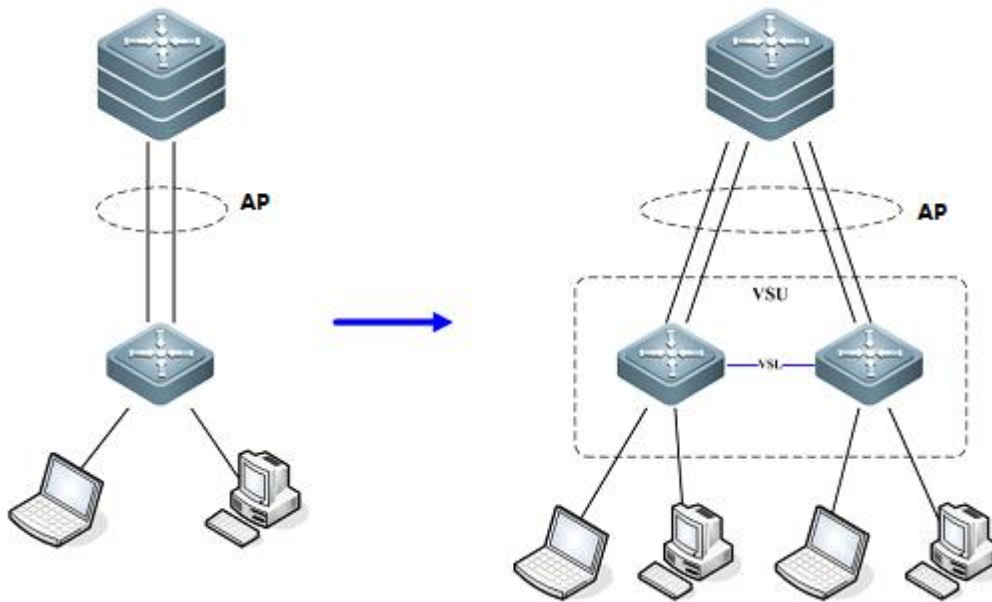
VSU expands Forwarding Capacity

As figure shown below, you can add one more switch to the VSU to expand the global forwarding capacity. For example, forwarding capacity of one switch is 128M pps, and the global forwarding capacity expands up to 256 M pps when two switches join in a VSU.



VSU expands Uplink Bandwidth

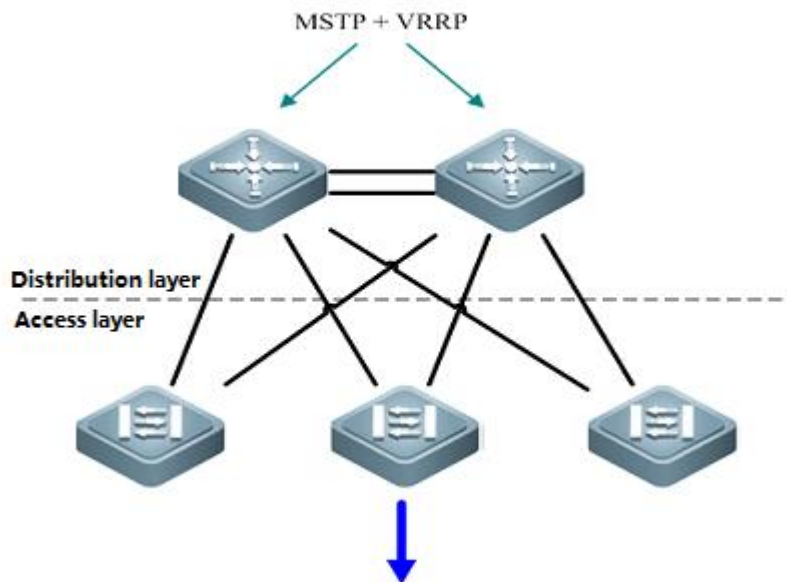
As figure shown below , you can add one more switch to VSU to expand uplink bandwidth to the core switch with the minimum impact for network topology and configuration.

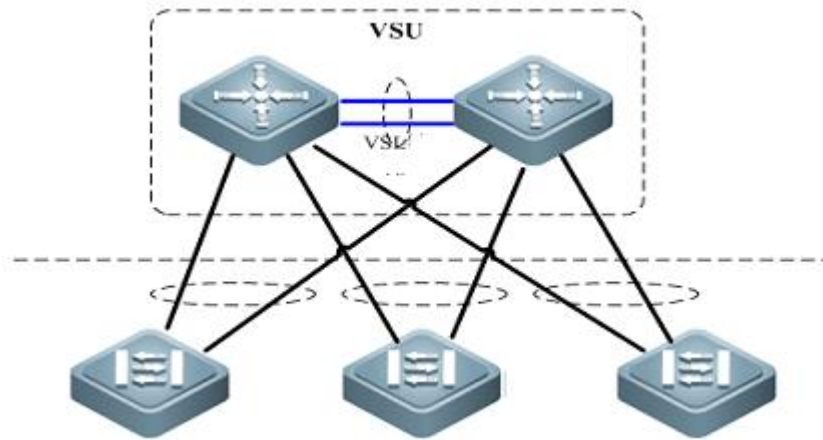


VSU simplifies the Network Topology

As the first figure shown below, this is a common scenario consisted of MSTP and VRRP features to ensure high available, and redundant ports are blocked to prevent loops.

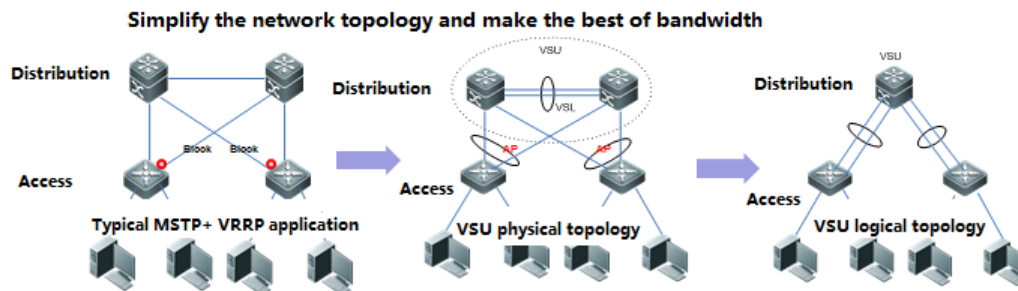
As the second figure shown below, VSU reduces the complexity of network and enhance the utilization ratio of network resources. All ports are occupied in the same time.



**Note:**

In the traditional network, in order to strengthen network reliability, the core layer or distribution layer will generally configure two devices into the dual-core system to allow redundant standby, with neighboring devices connecting two links to reach the dual-core redundant system. Such typical traditional network architecture is shown in the following figure. The redundant network architecture increases the complexity of network design and operations, while the enormous standby links also reduce the utilization ratio of network resources and decrease the rate of return on investment.

VSU (Virtual Switching Unit) is a common network virtualization technology combining two switches into a single virtual switch, thus reducing the complexity of network and enhancing the utilization ratio of network resources.



MSTP+VRRP : Complicate configuration and maintainance . Block link exists and can't make the best of bandwidth

VSU : Simple configuration and maintainance , associate with aggregate ports to make the best of bandwidth

Role of Chassis:

Each switch in a VSU are called VSU member and there're three VSU roles for VSU member based on different features:

- 1) Active: The active chassis controls the entire VSU system
- 2) Standby: The standby chassis take charge of the control if the main chassis fails

VSU Domain ID:

VSU Domain ID ranges from 1 to 255, and the default value is 100. Only VSU members with the same Domain ID can establish a VSU.

VSU Chassis ID:

The value of Chassis id can be 1 or 2. The default value is 1.

In standalone mode, port number takes 2-dimension format (for example, GigabitEthernet 2/3); In VSU mode, port number takes 3-dimension format (for example, GigabitEthernet 1/2/3).

The first number (GigabitEthernet~~1~~/2/3) indicates the chassis ID and the last two numbers (GigabitEthernet1/~~2~~/3) indicate the slot number and port number. So chassis ID of each VSU member must be different.

In addition, if two VSU chassis have the same chassis ID, VSU system recalculates a new chassis ID for them.

VSU Chassis Priority:

The value of chassis priority ranges from 1 to 255, and the default value is 100. A higher priority indicates a higher priority to become the active chassis.

In addition, chassis priority consists of configuring priority and running priority. Running priority doesn't change when administrator changes the configuring priority when VSU is running. Running priority changes when administrator saves configuration and reloads the VSU.

VSL

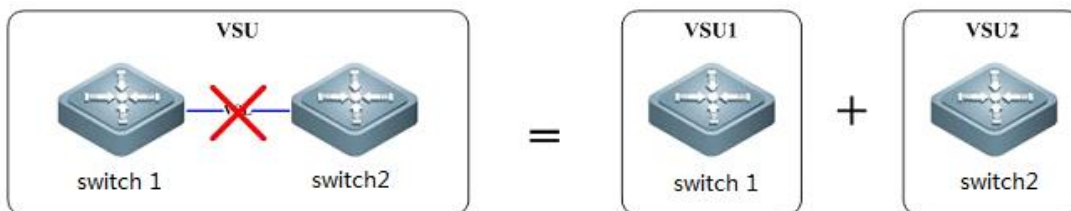
Since two chassis jointly forms a network entity in VSU system, they need to share control information and partial data streams. VSL (Virtual switching link) is a special link between two chassis for transmitting control information and data streams.

The VSL acts as an aggregation port. Its member port count is unlimited, and these member ports can reside on line cards in different slots. For the VSL transferred traffic, load balancing is performed among these member ports according to the traffic balancing algorithm.

Currently, 10-GB or 40-GB ports can become member ports of the VSL, while 1-GB ports cannot. Besides, a line card can hold physical member ports of the VSL as well as common data service ports.

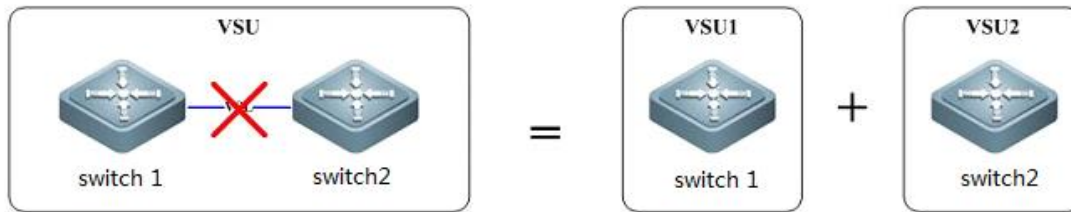
VSL Interruption:

As figure shown below, VSL Interruption occurs when the VSL fails and both VSU members disconnect



VSU Combination:

As figure shown below, VSU Combination occurs when both VSU members with the same Domain ID establish a VSU

**Switch Working Mode:**

Switch working mode includes: standalone mode and VSU mode, and the default mode is standalone mode

VSU VSL Connection medium:

Different switch varies.

For example, you can only configure VSL on S8600E series switches on 10G/40G optical ports.

VSL Detection:

VSL detection starts to detect peer chassis once VSU members boot and after VSL links come up, Topology Discovery begins.

Topology Discovery:

VSU members acquire global VSU network topology by flooding VSU hello packets through VSL. VSU Hello packets carry topology information including chassis ID, priority, MAC, VSL port etc.

VSU Role Election starts when Topology Discovery completes.

VSU Role Election:

The active chassis election mechanism operates as below:

Current host first

The higher priority first

The lower MAC address first

The slave chassis election mechanism is as follows:

The nearest to main first

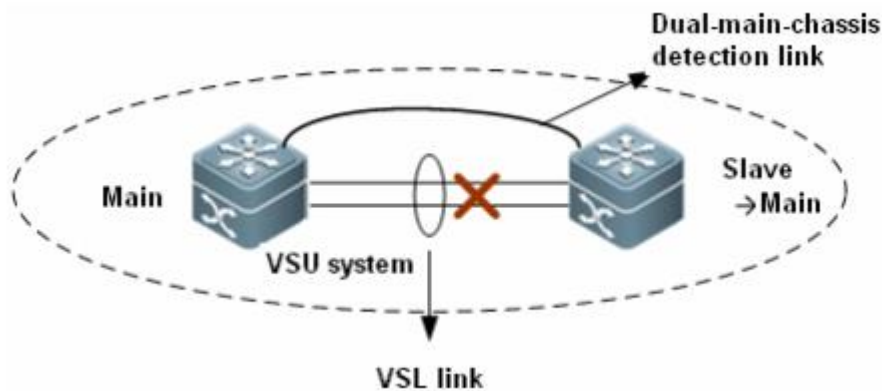
The higher priority first

The lower MAC address first

After finishing election, active chassis floods Convergence packets to the overall VSU, then VSU establishment completes.

Dual Active Detection:

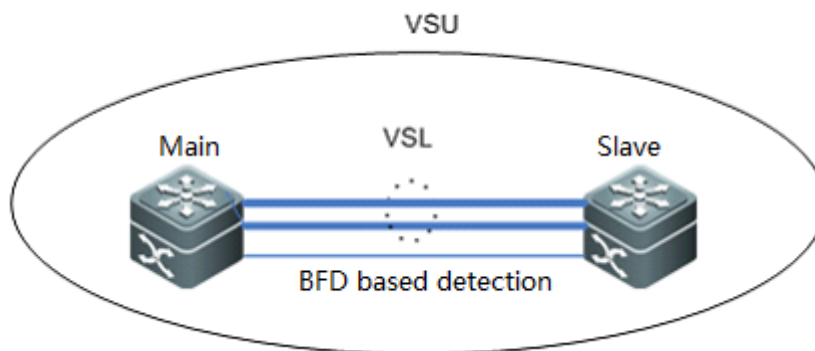
When VSL is disconnected, the slave chassis will be switched to main chassis. If the former main chassis is still running, then the existing two chassis will both become the main chassis. Since the configurations are completely same, a series of problems such IP address conflict will arise in the LAN. VSU must detect dual main chassis and take restoration measures.



As shown in the figure above, when deploying the VSU system, you need to configure an independent physical link between chassis in addition to the VSL. The physical link is used to transfer dual-main-chassis packets when the VSL is disconnected. It is called dual-main-chassis detection link. Ports connecting this link can be used to transfer only dual-main-chassis detection packets. You can run a CLI command to specify certain ports as the dual-main-chassis detection ports.

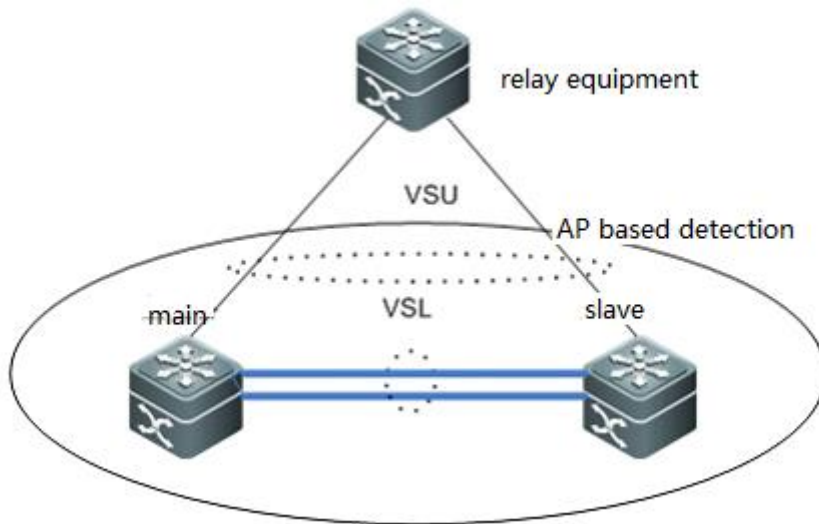
After dual main chassis are detected, generally, one chassis enters the recovery mode to avoid network abnormality. The VSU system supports the Bidirectional Forwarding Detection (BFD) and AP-based detection.

- 1) BFD based Detection: A port of BFD for dual main chassis must be a L3 physical port. Ports of other modes will not do. When you transform the port of BFD for dual main chassis from a L3 port into a port of other modes, the detection is automatically cleared and a prompt is displayed. Here, the extended BFD is used. That is, existing BFD configuration and display commands cannot be used to configure dual-main-chassis detection ports.



- 2) AP based Detection: The AP-based mechanism of detecting dual main chassis is similar as that based on BFD.

When the VSL is disconnected and two main chassis occur, the two main chassis send private protocol packets to each other for detecting dual main chassis. The difference from BFD based detection is AP-based Detection configures on the AP links between VSU and one relay equipment as figure shown below, and this relay equipment shall support forward private detection packets.



Recovery mode:

When the main chassis is in the recovery mode, all services ports except the following ports must be disabled:

VSL port: when the main chassis in the recovery mode detects that the VSL is UP again, the chassis resets itself, and joins the VSU system in the hot standby mode, becoming the new slave chassis.

MGMT port: You can use this port to perform remote management no matter the main chassis is in the recovery mode or not.

Exception port: You can specify certain ports as exception ports, which will not be disabled when the main chassis enters the recovery mode. Exception port: You can specify certain ports as exception ports, which will not be disabled when the main chassis enters the recovery mode. To configure exception ports, run the `dual-active exclude interface interface-name` command.

In the dual-main-chassis mode or when a main chassis enters the recovery mode, the simplest recovery solution is to reconnect the VSL. If VSL is not reconnected, but the main chassis in the recovery mode is manually restarted, the system enters dual-main-chassis state again when after the restart succeeds.

2.8.1.1 Configuring basic VSU

1. Configuring active and standby VSU members

Active switch:

```
Switch1# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch1(config)# switch virtual domain 1
```

```
Switch1(config-vs-domain)# switch 1
```

```
Switch1(config-vs-domain)# switch 1 priority 200
```

----->Priority is 100 by default , switch with the higher priority becomes the active chassis

```
Switch1(config-vs-domain)# exit
```

```
Switch1(config)# vsl-port
```

----->VSL is the heartbeat and traffic channel between 2 VSU members. You must configure at least 2 pair of VSL

```
Switch1(config-vsl-port)# port-member interface TenGigabitEthernet 2/1
Switch1(config-vsl-port)# port-member interface TenGigabitEthernet 2/2
Switch1(config-vsl-port)# exit
```

Standby switch:

```
Switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)# switch virtual domain 1 ----->domain ID must be the same to that of active chassis
Switch2(config-vs-domain)# switch 2 ----->switch ID must be different from that of active chassis
Switch2(config-vs-domain)# switch 2 priority 150
Switch2(config-vs-domain)# exit
Switch2(config)# vsl-port
Switch2(config-vsl-port)# port-member interface TenGigabitEthernet 2/1
Switch2(config-vsl-port)# port-member interface TenGigabitEthernet 2/2
Switch2(config-vsl-port)# exit
```

2. Connect VSL cable and confirm that links come up
3. Save configuration and convert both VSU members to virtual mode at the same time

Active switch

```
Switch1# wr
Switch1# switch convert mode virtual ----->convert switch working mode from standalone mode to virtual mode
Are you sure to convert switch to virtual mode[yes/no] : yes
Do you want to recovery "config.text" from "virtual_switch.text" [yes/no] : no
```

Standby switch

```
Switch2# switch convert mode virtual
Are you sure to convert switch to virtual mode[yes/no] : yes
Do you want to recovery "config.text" from "virtual_switch.text" [yes/no] : no
```

Both VSU members reloads automatically

Attention: Be patient and it costs about 10 minutes to finish building VSU.

System prints logs continuously during next 10 minutes as below if VSL links failed or peer switch doesn't reload yet:

*Aug 6 13:17:17: %VSU-5-RRP_TOPO_INIT: Topology initializing, please wait for a moment

*Aug 6 13:18:17: %VSU-5-RRP_TOPO_INIT: Topology initializing, please wait for a moment.

4. Verification

1. When VSU completes, you can manage VSU on active chassis.
2. You can identify the active switch by viewing the Primary LED on the front main board which is solid green
3. When VSU completes, you can no longer manage VSU on standby chassis through console port by default.

```
Ruijie# show switch virtual
```

| Switch_id | Domain_id | Priority | Position | Status | Role |
|-----------|-----------|----------|----------|--------|-----------------------|
| 1(1) | 1(1) | 200(200) | LOCAL | OK | ACTIVE ----->active |
| 2(2) | 1(1) | 150(150) | REMOTE | OK | STANDBY ----->standby |

```
Ruijie#sh version slot
```

| Dev Slot Port | Configured Module | Online Module | Software Status |
|---------------|-------------------|---------------|-----------------|
| ----- | ----- | ----- | ----- |

2.8.1.2 Configuring VSU optimization

Overview

1. When VSL is disconnected, the standby chassis will be switched to active chassis. If the former active chassis is still running, then the existing two chassis will both become the active chassis. Since the configurations are completely same, a series of problems such IP address conflict will arise in the LAN. VSU must detect dual-active chassis and take restoration measures.
2. After enable dual-active detection , system detects dual-active via control packets between BFD dedicated link and puts one chassis which has lower priority into recovery mode ,all port ,except for VSL port, MGMT port and exception port that administrator specifies (reserved for telnet), are mandatory shutdown

When dual-active occurs, dual-active detection ensures the stability and high availability of your network. (you must use redundant connection to connect other switches to VSU . In addition, you must connect one link to the active chassis, the other to standby chassis)

I. Configuration Steps

1. Configuring Dual-active Detections

```
Ruijie(config)# interface gi2/4/2
Ruijie(config-if)# no switchport ----->BFD detection must be applied on a Layer 3 port
Ruijie(config-if)# exit
Ruijie(config)# interface gi1/4/2
Ruijie(config-if)# no switchport
Ruijie (config-if)# exit

Ruijie (config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active detection bfd ----->enable BFD feature
```

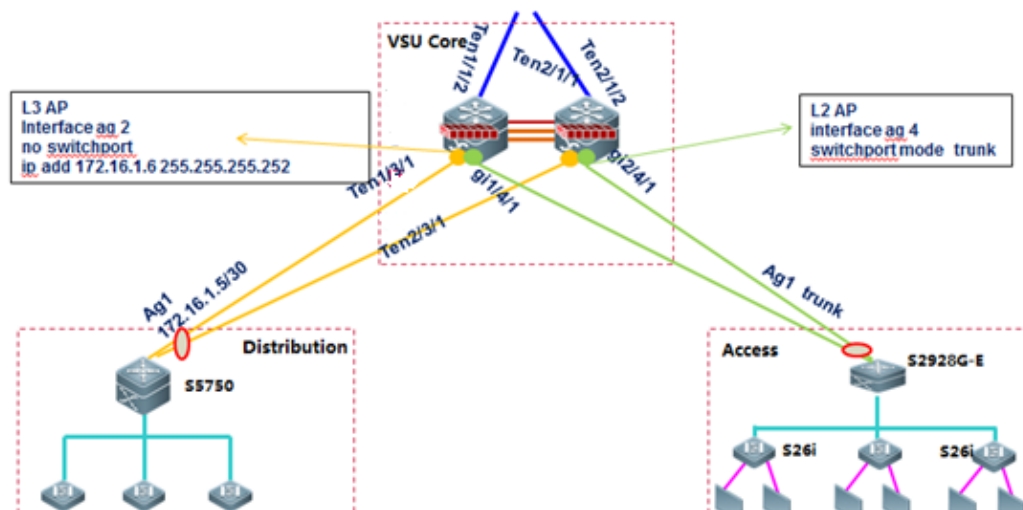
```
Ruijie(config-vs-domain)# dual-active pair interface gi1/4/2 interface gi2/4/2 ----->configure a pair of BFD
detection ports
Ruijie(config-vs-domain)# dual-active exclude interface ten1/1/2 ----->configure the exception port
Ruijie(config-vs-domain)# dual-active exclude interface ten2/1/2
```

2.8.1.3 Configuring AP in VSU

Overview

Inter-chassis aggregate port (AP) group includes member ports of two VSU chassis. Inter-chassis AP can connect to all devices (such as server, switch and router) supporting port aggregation function.

Inter-chassis AP allows load balancing of inter-chassis data streams. For example, when data streams enter from main chassis into VSU system, VSU will give preference to member ports located in the main chassis. This feature guarantees that some unnecessary data streams are not transmitted over VSL, thus reducing the load pressure of VSL. The following figure shows the typical application of AP in a VSU.



I. Configuration Steps

1. Configuring layer 3 AP on VSU:

```
Ruijie(config)#interface aggregateport 2
Ruijie(config-if-AggregatePort 2)#no switchport
Ruijie(config-if-AggregatePort 2)#description link-to-xxxx
Ruijie(config-if-AggregatePort 2)#ip add 172.16.1.6 255.255.255.252
Ruijie(config-if-AggregatePort 2)#exit
Ruijie(config)#interface ten 1/3/1
Ruijie(config-if-TengabitEthernet 1/3/1)#no switchport
Ruijie(config-if-TengabitEthernet 1/3/1)#description linktoyyyy
```

```

Ruijie(config-if-TengabitEthernet 1/3/1)#port-group 2
Ruijie(config-if-TengabitEthernet 1/3/1)#exit
Ruijie(config)#interface ten 2/3/1
Ruijie(config-if-TengabitEthernet 2/3/1)#no switchport
Ruijie(config-if-TengabitEthernet 2/3/1)#description link-to-yyyy
Ruijie(config-if-TengabitEthernet 2/3/1)#port-group 2
Ruijie(config-if-TengabitEthernet 2/3/1)#exit

```

2. Configuring layer 2 AP on VSU:

```

Ruijie(config)#interface aggregateport 4
Ruijie(config-if-AggregatePort 4)#switchport mode trunk
Ruijie(config-if-AggregatePort 4)#switchport trunk allowed vlan remove xxxx ----->prune trunk port based on
requirement
Ruijie(config-if-AggregatePort 4)#description linktoxxxx
Ruijie(config-if-AggregatePort 4)#exit
Ruijie(config)#interface gigabitEthernet 1/4/1
Ruijie(config-if-GigabitEthernet 1/4/1)#port-group 4
Ruijie(config-if-GigabitEthernet 1/4/1)#description link-to-yyyy
Ruijie(config-if-GigabitEthernet 1/4/1)#exit
Ruijie(config)#interface gigabitEthernet 2/4/1
Ruijie(config-if-GigabitEthernet 2/4/1)#port-group 4
Ruijie(config-if-GigabitEthernet 2/4/1)#description link-to-yyyy
Ruijie(config-if-GigabitEthernet 2/4/1)#exit

```

2.8.1.4 Verifying VSU

| | Verification Items | Description | Expected interrupt time | Result |
|------------------|--|-------------|-------------------------|--------|
| Links redundancy | Plug and unplug AP cable | Mandatory | in 2S | |
| | Plug and unplug ECMP/Routing cable | Mandatory | in 2S | |
| VSU switchover | Hot-plugging Dual-Management boards in one chassis of the VSU System | Optional | in 2S | |
| | Switch over main and slave chassis by executing "redundancy forceswitch" | Optional | in 2S | |
| | Power off VSU main/slave chassis | Mandatory | in 2S | |
| Dual-active | Unplug all VSL links | Mandatory | in 2S | |

2.8.2 1X-Web Authentication

2.8.2.1 Secure Channel, Authentication-Free, and Emergency Channel

Features

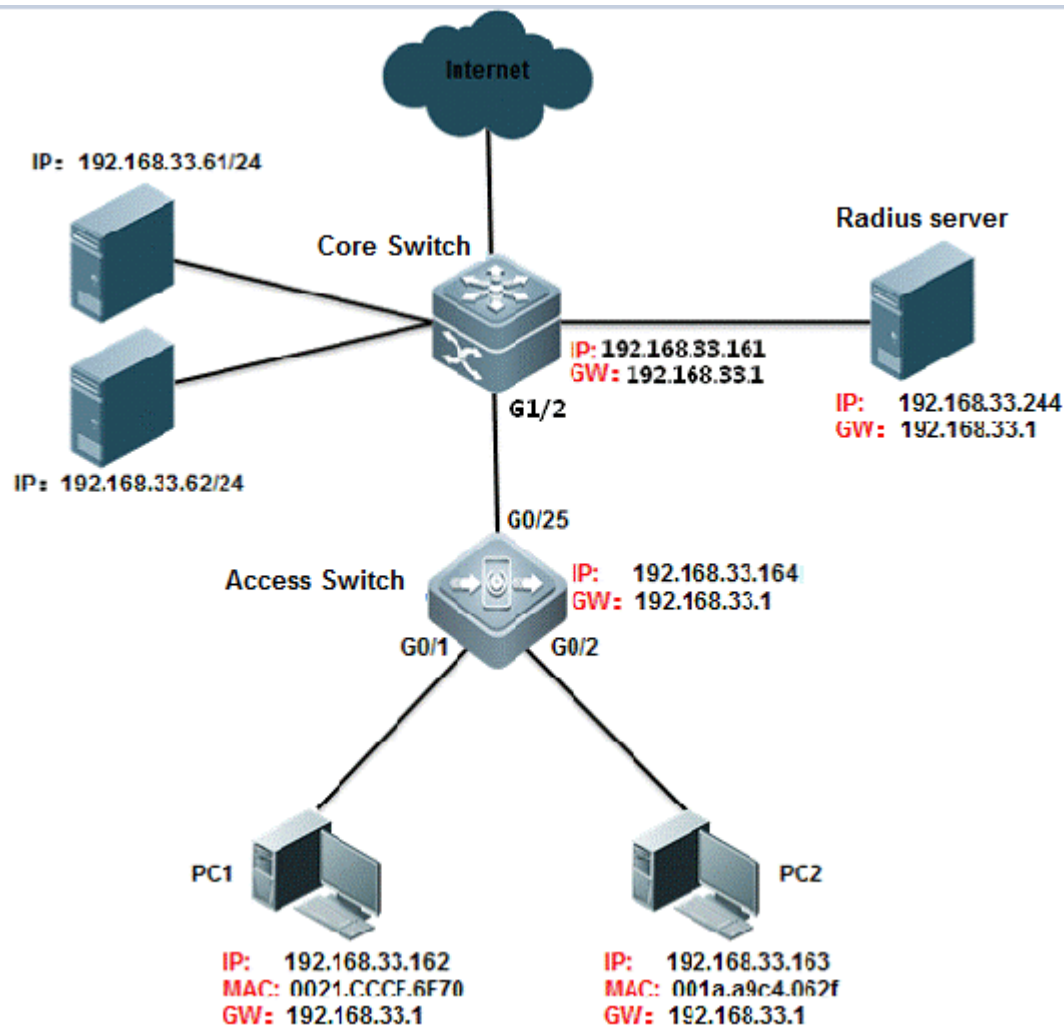
Secure channel: Generally, after 1X authentication is deployed, data packets from unauthenticated user ports are discarded. The secure channel allows user's access designated websites unauthenticated. It can be deployed to facilitate client distribution, backdoor reservation for leaders and terminals that do not support authentication (for example, printers and all-purpose terminals).

Emergency channel: In an 1X authentication scenario with only one Radius server, all users fail to access the Internet once the Radius server fails, services will be seriously affected. In that case, authentication configuration must be cancelled on all the ports one by one to recover services. If an emergency channel is deployed, the switch allows users access the Internet without authentication when authentication fails multiple times or the Radius server is considered dead.

I. Networking Requirements

1. The 1X function is enabled on the core server for resource access authentication on managed users.
2. Authenticated users can access all resources while unauthenticated users can access only certain Intranet resources.
3. Authentication-free access to intranet resources is enabled for some users (PC2).
4. When the active Radius server fails to function normally, user authentication is switched to the backup Radius server. When both active and standby Radius servers fail, managed users can access resources without authentication (through an emergency channel).

II. Network Topology



III. Configuration Tips

1. On the core server, enable AAA and configure the Radius server and key associated parameters.
2. On the Radius server, configure the related parameters. (In this example, the SAM is used as the Radius server.)
3. Configure a professional ACL to implement server access before user authentication.
4. The core switch, managed users, and the Radius server can be on different network segments, so long as the core switch can properly communicate with the Radius server and the clients can reach the controlled ports on the core switch via the access switch.
5. Configure the parameters for the communication between the switch and the Radius server to deploy an emergency channel.

IV. Configuration Steps

Configure the core server.

1. Basic dot1x configuration

```

Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#aaa new-model ----->trun on aaa switch
Ruijie(config)#radius-server host 192.168.33.244 ----->configure radius server
Ruijie(config)#radius-server host 192.168.33.245 ----->configure backup radius server
Ruijie(config)#radius-server key ruijie ----->configure radius key
Ruijie(config)#aaa authentication dot1x ruijie group radius none -----> Define an IEEE802.1x authentication
method list.
Ruijie(config)#aaa accounting network ruijie start-stop group radius -----> Define the AAA network accounting
method list.
Ruijie(config)#aaa accounting update periodic 15 -----> Set the account update function.
Ruijie(config)#dot1x authentication ruijie -----> 802.1X to select the authentication method list
Ruijie(config)#dot1x accounting ruijie -----> 802.1X to select the accounting method list
Ruijie(config)#interface gigabitEthernet 1/2
Ruijie(config-if-GigabitEthernet 1/2)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 1/2)#dot1x port-control auto -----> Enable 802.1X authentication on the
interface
Ruijie(config-if-GigabitEthernet 1/2)#ip add 192.168.33.161 255.255.255.0 -----> configure switch ip address
Ruijie(config-if-GigabitEthernet 1/2)#end
Ruijie#write -----> save configuration

```

2. Enable the secure channel function

```

Ruijie(config)#expert access-list extended ruijie
Ruijie(config-exp-nacl)#permit arp any any any any any ----->make the ip and arp packets free authentication
Ruijie(config-exp-nacl)#permit ip any any host 192.168.33.61 any -----> To allow access to the home page of the
site before authentication
Ruijie(config-exp-nacl)#permit ip any any host 192.168.33.62 any -----> To allow access to the home page of the
site before authentication
Ruijie(config-exp-nacl)#permit ip any any host 192.168.33.244 any -----> To allow access to the home page of the
site before authentication
Ruijie(config-exp-nacl)#permit host 192.168.33.163 host 001a.a9c4.062f any any-----> This host implements
authentication free
Ruijie(config-exp-nacl)#exit
Ruijie(config)#security global access-group ruijie

```

1x free authentication description

There are two ways to achieve user authentication: (1) configure the security channel to put the IP or MAC address; 2, configure the free VLAN authentication will be the corresponding VLAN users free of authentication

Plan 1 : Configure security channel , there are three methods :

Method 1 : permit host ip address

```

expert access-list extended no1x
10 permit arp any any any any any
20 permit ip host 192.168.1.23 any anyany ----->permit host ip address
security global access-group no1x

method 2 : permit host mac address
expert access-list extended no1x
10 permit arp any any any any any
30 permit ip any host 0010.123c.513d any any ----->permit hots mac address
security global access-group no1x

method 3 : permit ip+mac
expert access-list extended no1x
10 permit arp any any any any any
40 permit ip host 192.168.1.23 host 0010.123c.513d any any ----->permit ip and mac address
security global access-group no1x

Plan 2 : Configure direct-vlan
Configuration command : direct-vlan 1-20// direct-vlan can take effect on both 1x authentication and web
authentication

```

Notes:

If the secure channel (in priority over 1x authentication) is enabled, user ARP packets must be allowed to pass. In this way, users can communicate with the gateway. As the secure channel has higher priority, the anti ARP spoofing function will become invalid.

Solution: Do not permit all ARP packets. Permit only ARP packets destined for the gateway. In this way, ARP check is implemented and ARP spoofing among users are prevented. However, ARP spoofing is not completely prevented, because users can still spoof another user on the gateway.

```

Ruijie(config)#expert access-list extended permit1x
Ruijie(config-exp-nacl)#permit ip any any host 192.168.1.254 any -----> To allow access to the home
page of the site before authentication
Ruijie(config-exp-nacl)#permit arp any any any any any -----> Allow ARP message interaction between a user
and a gateway
Ruijie(config)#security global access-group permit1x
Ruijie(config-exp-nacl)#permit arp any any any any host 192.168.33.1

```

3. You can change the time parameter between the switch and the Radius server to switch the authentication method. For example, the configuration "aaa authentication dot1x ruijie group radius **none**" indicates that authentication by the active Radius server is implemented first, is switched to the backup Radius server if

the active Radius server does not respond in a specified period, and is switched to none authentication mode if both the active and backup Radius servers fail to respond.

```
Ruijie(config)#radius-server timeout 2 -----> Specify the waiting time before the router resend request (2 s by default)
Ruijie(config)#radius-server retransmit 2 -----> Specify the times of sending requests before the router confirms Radius invalid (3 by default)
Ruijie(config)#radius-server dead-criteria time 6 tries 3 ----->define the dead-criteria time and tries of the server
Ruijie(config)#radius-server deadtime 5 -----> Specify the waiting time before the server is considered dead in case of no response to the request sent by the device (5 minutes by default).
Ruijie(config)#dot1x timeout server-timeout 20
```

dot1x timeout indicates the timeout period of 1x authentication. The parameter is independent from the Radius timeout period (**radius timeout***). However, **radius timeout* (retransmit+1)** must be smaller than **dot1x timeout server-timeout**. Otherwise, the emergency channel does not take effect. In this example, $2*(2+1)=6s$, which is smaller than 20s, and therefore, the emergency channel is effective.

V. Verification

1. Before authentication, users can access the resources inside the secure channel, but can not access the resources inside the non secure channel

```
C:\Users\R03344>ping 192.168.33.61
```

The same can also be verified, the security channel is free to authenticate users of IP and MAC, the user can also communicate properly.

2、When the radius server hangs, the user can achieve escape function

```
Ruijie#show dot1x summary
```

| ID | MAC | Interface | VLAN | Auth-State | Backend-State | Port-Status | Us |
|----|----------------|-----------|------|---------------|---------------|-------------|----|
| 7 | 0021.cccf.6f70 | Gil/2 | 1 | Authenticated | Idle | Authed | st |

Check the user info.

```

Ruijie#show dot1x user id 7
User name: admin1234
User id: 7
Type: static
Mac address is 0021.cccf.6f70
Vlan id is 1
Access from port G11/2
Time online: 0days 0h 1m47s
User ip address is 192.168.33.162
Max user number on this port is 6000
Authorization session time is 20736000 seconds
Supplicant is private
Start accounting
Deny proxy user
Deny dial user
IP privilege is 0
user acl-name admin1234_1_0_0 :

```

4. open debug radius event, you can see the entire process of an escape function :

```

Ruijie#debug radius event
Ruijie#*Mar 16 18:07:20: %7: [radius] aaa req authentication to group radius
*Mar 16 18:07:20: %7: __rds_add_attr type = 24 len = 0
*Mar 16 18:07:20: %7: [radius] 16 send
*Mar 16 18:07:20: %7: pkt len 676 code 1 id 16
*Mar 16 18:07:20: %7: calcu msg auth ok
*Mar 16 18:07:20: %7: [radius] radius access requests(12). -----> sent access-request for the first time
*Mar 16 18:07:22: %7: [radius] user 16 retry
*Mar 16 18:07:22: %7: [radius] 16 send
*Mar 16 18:07:22: %7: pkt len 676 code 1 id 16
*Mar 16 18:07:22: %7: calcu msg auth ok
*Mar 16 18:07:22: %7: [radius] radius access requests retransmissions(18) timeout(18). -----> timeout for the first
time after 2 seconds
*Mar 16 18:07:24: %7: [radius] user 16 retry
*Mar 16 18:07:24: %7: [radius] 16 send
*Mar 16 18:07:24: %7: pkt len 676 code 1 id 16
*Mar 16 18:07:24: %7: calcu msg auth ok
*Mar 16 18:07:24: %7: [radius] radius access requests retransmissions(19) timeout(19). -----> timeout for the
second time after 4 seconds
*Mar 16 18:07:26: %7: [radius] user 16 retry
*Mar 16 18:07:26: %7: [rds_user] rds delete user, state 2, atype 0
*Mar 16 18:07:26: %7: [rds_user] rds free user id 7, pkid 16 -----> timeout for the third time after 6 seconds
*Mar 16 18:07:26: %AAA-7-FAILOVER: Failing over from 'dot1x' for client 0021.cccf.6f70 on Interface
GigabitEthernet 0/1.
*Mar 16 18:07:26: %7: [radius] aaa req accounting to group radius
*Mar 16 18:07:26: %7: [accounting] acct len 116

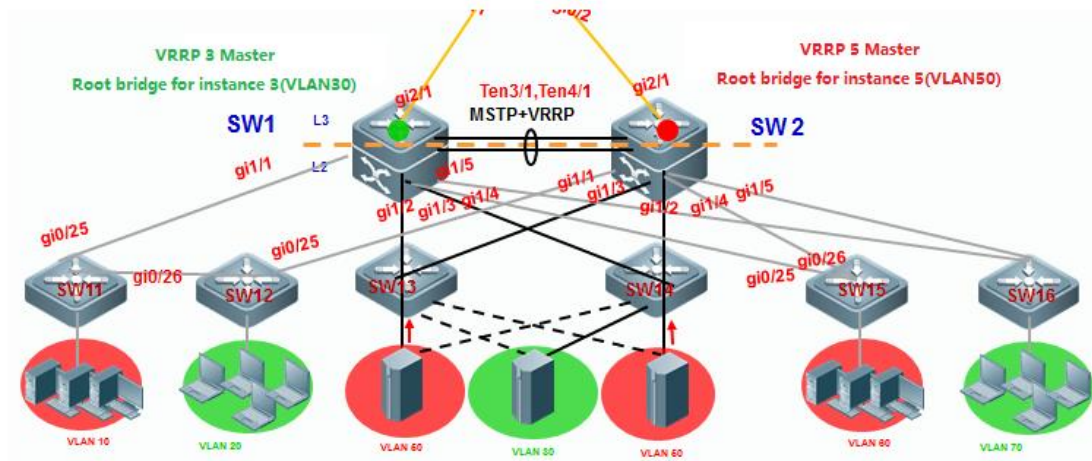
```


2. SW2 is Root Bridge for MSTP instance 2 and secondary root for instance 1. MSTP instance 1 includes VLAN 10, 60 and 80 and instance 2 includes VLAN 20, 30 and 70.

SW1 is the master VRRP gateway for VLAN 10, 60 and 80 and the backup VRRP gateway for VLAN 20, 30 and 70. SW2 is the master VRRP gateway for VLAN 20, 30 and 70 and the backup gateway for VLAN 10, 60 and 80.

Merit: Fully occupy network resource

Demerit: More complicated configuration and maintenance than MSTP with single instance



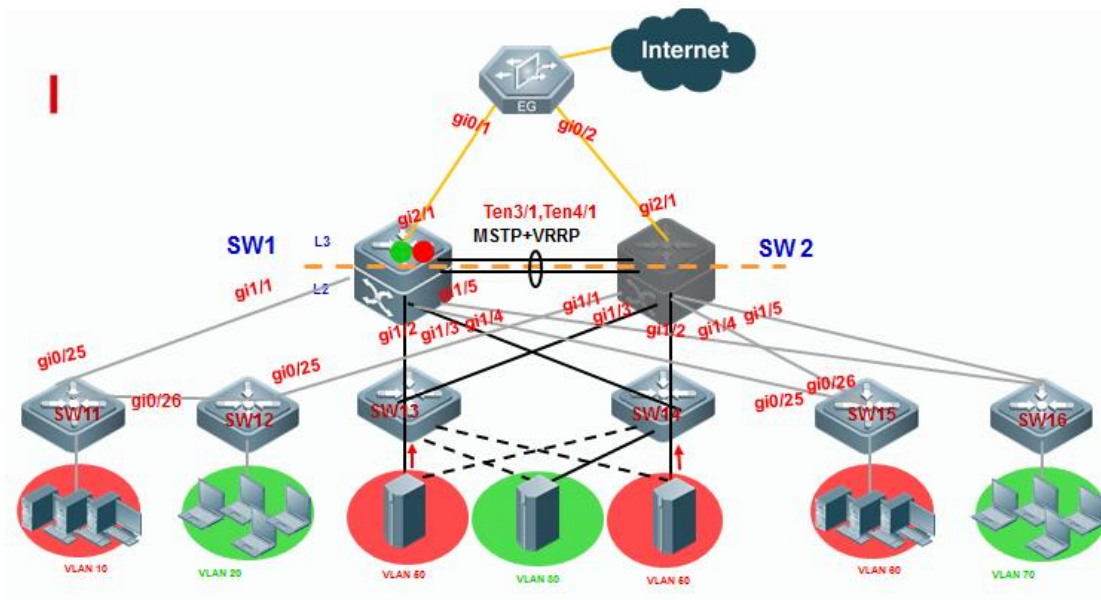
2.8.3.2 Configuring MSTP with single instance

Note:

The deployment pattern of "MSTP + VRRP" is replaced by deployment pattern of VSU day by day and we suggest you to apply VSU if possible. Even so, deployment pattern of "MSTP + VRRP" is still a fallback method to ensure a redundant and reliable network if core and distribution switches don't support VSU

We suggest you to remove some interconnection links first to avoid a Layer 2 loop

I. Network Topology



SW1 is the master VRRP gateway for users on all vlans, and SW2 is the backup VRRP gateway for users on all vlans.

Connect SW1 and SW2 through an Aggregate port to ensure reliability and configure this AP as Trunk port.

The IP address of SW1 on VLANs from 10 to 80 are 192.168.10.1 to 192.168.80.1 , and IP address of SW2 on VLANs from 10 to 80 are 192.168.10.2 to 192.168.80.2 , and VRRP IP address are 192.168.10.254 to 192.168.80.254.

II. Configuration Steps

Configuring SW1

```
Ruijie#config terminal
Ruijie(config)#spanning-tree mst 0 priority 0 ----->instance id=0 , priority=0(The lower the number, the more
likely the switch will be chosen as the root bridge) by default , all vlans are mapped to instance 0 .
Ruijie(config)#spanning-tree ----->enable STP feature and the default STP mode is MSTP
Ruijie(config)#exit
```

Configure MSTP

Configuring AP

```
Ruijie#config terminal
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#switchport mode trunk
Ruijie(config-if-AggregatePort 1)#exit
Ruijie(config)#interface tengigabitEthernet 3/1
Ruijie(config-if-TenGigabitEthernet 3/1)#port-group 1
Ruijie(config-if-TenGigabitEthernet 3/1)#exit
Ruijie(config)#interface tengigabitEthernet 3/2
```

```
Ruijie(config-if-TenGigabitEthernet 3/2)#port-group 1
Ruijie(config-if-TenGigabitEthernet 3/2)#exit

Ruijie(config)#interface range gigabitEthernet 1/1-5
Ruijie(config-if-range)#switchport mode trunk ----->don't forget to prune trunk port
```

Configuring VRRP

```
Ruijie(config)#vlan 10
Ruijie(config)#inter vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0
Ruijie(config-if-VLAN 10)#vrrp 10 ip 192.168.10.254
Ruijie(config-if-VLAN 10)#vrrp 10 priority 120 -----> vrrp group id=10 , priority value=120 (the bigger
the number , the more likely the switch will be chosen as the master ,and default value is 100)
Ruijie(config-if-VLAN 10)#exit

Ruijie(config)#vlan 20
Ruijie(config)#inter vlan 20
Ruijie(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0
Ruijie(config-if-VLAN 20)#vrrp 20 ip 192.168.20.254
Ruijie(config-if-VLAN 20)#vrrp 20 priority 120
Ruijie(config-if-VLAN 20)#exit

.....configuration of VLAN 30 ~ VLAN 70 are omitted.....

Ruijie(config)#vlan 80
Ruijie(config)#inter vlan 80
Ruijie(config-if-VLAN 80)#ip address 192.168.80.1 255.255.255.0
Ruijie(config-if-VLAN 80)#vrrp 80 ip 192.168.80.254
Ruijie(config-if-VLAN 80)#vrrp 80 priority 120
Ruijie(config-if-VLAN 80)#exit
```

Configuring SW2

```
Ruijie#config terminal
Ruijie(config)#spanning-tree mst 0 priority 4096 ----->instance id=0 , priority=4096(The lower the number, the
more likely the switch will be chosen as the root bridge) by default , all vlans are mapped to instance 0

Ruijie(config)#spanning-tree ----->enable STP feature and default mode is MSTP
Ruijie(config)#exit
```

Configuring AP

```
Ruijie#config terminal
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#switchport mode trunk
Ruijie(config-if-AggregatePort 1)#exit
Ruijie(config)#interface tengigabitEthernet 3/1
Ruijie(config-if-TenGigabitEthernet 3/1)#port-group 1
Ruijie(config-if-TenGigabitEthernet 3/1)#exit
Ruijie(config)#interface tengigabitEthernet 3/2
Ruijie(config-if-TenGigabitEthernet 3/2)#port-group 1
Ruijie(config-if-TenGigabitEthernet 3/2)#exit
Ruijie(config)#interface range gigabitEthernet 1/1-5
Ruijie(config-if-range)#switchport mode trunk ----->don't forget to prune trunk port
```

Configuring VRRP

```
Ruijie(config)#vlan 10
Ruijie(config)#inter vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.10.2 255.255.255.0
Ruijie(config-if-VLAN 10)#vrrp 10 ip 192.168.10.254 ----->vrrp group id=10 , priority value remains default
setting(the bigger the number , the more likely the switch will be chosen as the master ,and default value is 100)
Ruijie(config-if-VLAN 10)#exit

Ruijie(config)#vlan 20
Ruijie(config)#inter vlan 20
Ruijie(config-if-VLAN 20)#ip address 192.168.20.2 255.255.255.0
Ruijie(config-if-VLAN 20)#vrrp 20 ip 192.168.20.254
Ruijie(config-if-VLAN 20)#exit

.....configuration of VLAN 30 ~ VLAN 70 are omitted.....

Ruijie(config)#vlan 80
Ruijie(config)#inter vlan 80
Ruijie(config-if-VLAN 80)#ip address 192.168.80.2 255.255.255.0
Ruijie(config-if-VLAN 80)#vrrp 80 ip 192.168.80.254
Ruijie(config-if-VLAN 80)#exit
```

Configuring SW11, SW12, S13, S14, S15, S16

```
Ruijie#config terminal
Ruijie(config)#interface range gigabitEthernet 0/25-26
Ruijie(config-if-range)#switchport mode trunk
Ruijie(config-if-range)#exit
```

```
Ruijie(config)#spanning-tree ----->enable STP feature and default mode is MSTP
Ruijie(config)#exit
```

If we want to manually conduct MSTP to put G0/25 on SW11 and SW12 in forwarding state, we can assign a higher cost value to G0/26, then MSTP blocks G0/26. (If a loop occurs, MST uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission)

```
Ruijie(config)#interface gi0/26
Ruijie(config-if-GigabitEthernet 0/26)#spanning-tree cost 200000 ----->the default value is derived from the
media speed of the interface, and the cost value of a 1000M port is 20000
Ruijie(config-if-GigabitEthernet 0/26)#exit
```

Connecting cable and verifying status of STP and VRRP

1. This example displays that SW1 is the root bridge

SW1:

```
Ruijie#show spanning-tree
StpVersion : MSTP
SysStpStatus : ENABLED
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops: 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
LoopGuardDef : Disabled

##### mst 0 vlans map : ALL
BridgeAddr : 1414.4b19.ecc0 ----->local MAC address
Priority: 0
TimeSinceTopologyChange : 12d:0h:19m:46s
TopologyChanges : 0
DesignatedRoot : 0.1414.4b19.ecc0 ----->root MAC address
RootCost : 0
RootPort : 0
CistRegionRoot : 0.1414.4b19.ecc0
CistPathCost : 0
```

3. This example displays that SW1 is the VRRP master

```
Ruijie#show vrrp 10
VLAN 10 - Group 10
  State is Master
  Virtual IP address is 192.168.10.254 configured
  Virtual MAC address is 0000.5e00.010a
  Advertisement interval is 1 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.10.1 (local), priority is 120
  Master Advertisement interval is 1 sec
  Master Down interval is 3.53 sec
```

```
Ruijie#show vrrp brief
```

| Interface addr | Grp | Pri | timer | Own | Pre | State | Master addr | Group |
|---------------------------|-----|-----|-------|-----|-----|--------|--------------|-------|
| VLAN 10 192.168.10.254 | 10 | 120 | 3.53 | - | P | Master | 192.168.10.1 | |
| VLAN 20 192.168.20.254 | 20 | 120 | 3.53 | - | P | Master | 192.168.20.1 | |
| VLAN 30 192.168.30.254 | 30 | 120 | 3.53 | - | P | Master | 192.168.30.1 | |
| VLAN 40 192.168.40.254 | 40 | 120 | 3.53 | - | P | Master | 192.168.40.1 | |
| VLAN 50 192.168.50.254 | 50 | 120 | 3.53 | - | P | Master | 192.168.50.1 | |
| VLAN 60 192.168.60.254 | 60 | 120 | 3.53 | - | P | Master | 192.168.60.1 | |
| VLAN 70 192.168.70.254 | 70 | 120 | 3.53 | - | P | Master | 192.168.70.1 | |
| VLAN 80 192.168.80.254 | 80 | 120 | 3.53 | - | P | Master | 192.168.80.1 | |

3. This example displays that SW1 is the root bridge on SW2

SW2:

```
Ruijie#show spanning-tree
StpVersion : MSTP
SysStpStatus : ENABLED
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops: 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
LoopGuardDef  : Disabled

##### mst 0 vlans map : ALL
BridgeAddr : 00d0.f834.ea70  ----->SW2 MAC address
Priority: 4096
TimeSinceTopologyChange : 0d:0h:9m:2s
TopologyChanges : 6
DesignatedRoot : 0000.1414.4b19.ecc0  -----> root MAC address(SW1)
RootCost : 0
RootPort : 3
CistRegionRoot : 0000.1414.4b19.ecc0
CistPathCost : 20000
```

4. This example displays that SW2 is the VRRP Backup

```
CistPathCost : 20000 Ruijie#show vrrp 10
VLAN 10 - Group 10
  State is Backup
  Virtual IP address is 192.168.10.254 configured
  Virtual MAC address is 0000.5e00.010a
  Advertisement interval is 1 sec
  Preemption is enabled
  min delay is 0 sec
```

```

Priority is 100
Master Router is 192.168.10.1 , priority is 120
Master Advertisement interval is 1 sec
Master Down interval is 3 sec

```

5. This example displays how to verify Root Bridge on SW11 and SW12 and whether MSTP has blocked G0/26 as per design.

```

Ruijie#show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID    Priority    0
    Address   1414.4b19.ecc0  ----->root bridge MAC address
    this bridge is root
    Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

  Bridge ID  Priority    32768
    Address   00d0.f8b5.0a0b ----->local MAC address
    Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

Interface      Role Sts Cost      Prio   Type OperEdge
-----
Gi0/25         Root FWD 200000    128    P2p   False ----->root port
Gi0/26         Altn BLK 200000    128    P2p   ----->blocked port

```

When you connect Ruijie switch to other vendors, pay attention to spanning-tree compatibility:

1. When you connect Ruijie to Cisco, you must double confirm whether Cisco firmware supports standard MSTP. So far, Cisco switch with firmware 12.25(SE) and above supports standard MSTP, but any other older firmware doesn't, so the old firmware that runs nonstandard MSTP has compatibility issue. So you must upgrade switch to version 12.25(SE) and above. If Cisco switch is too old to upgrade to version 12.25(SE) and above, you can disable STP and enable BPDU bridge mode to bypass all bpdu packets. To enable BPDU bridge mode, perform this task:
Ruijie(config)#no spanning-tree
Ruijie(config)#bridge-frame forwarding protocol bpdu
2. We suggest you to configure completely the same MSTP name, revision, instance mapping when you enable MSTP on Ruijie and other vendors switch to prevent STP compatibility issue. You can also enable RSTP because RSTP has better compatibility.

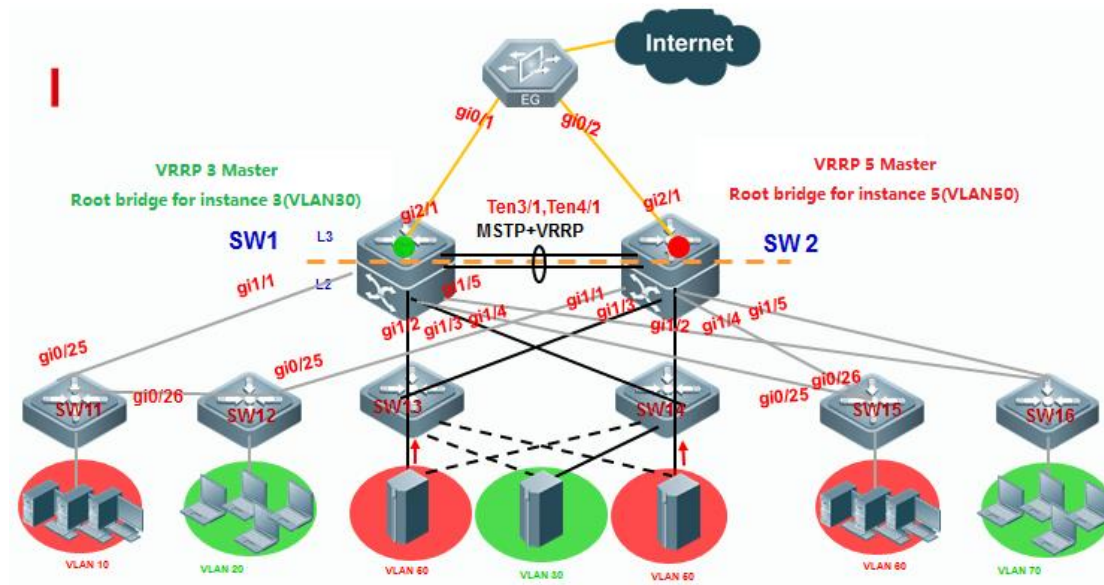
2.8.3.3 Configuring MSTP with multiple instances

Note:

The deployment pattern of "MSTP + VRRP" is replaced by deployment pattern of VSU day by day and we suggest you to apply VSU if possible. Even so, deployment pattern of "MSTP + VRRP" is still a fallback method to ensure a redundant and reliable network if core and distribution switches don't support VSU

We suggest you to remove some interconnection links first to avoid a Layer 2 loop

I. Network Topology



SW1 is the master VRRP gateway for users on vlan 10,20,30,40,60,and 70,and backup VRRP for servers on vlan 50 and 80.SW2 is the master VRRP gateway for servers on vlans 50 and 80 , and backup VRRP for users on vlan 10,20,30,40,60 and 70. Connect SW1 and SW2 through an Aggregate port to ensure reliability and configure this AP as Trunk port. The IP address of SW1 on VLANs from 10 to 80 are 192.168.10.1 to 192.168.80.1 , and IP address of SW2 on VLANs from 10 to 80 are 192.168.10.2 to 192.168.80.2 , and VRRP IP address are 192.168.10.254 to 192.168.80.254.

II. Configuration Steps

Configuring SW1

Configuring MSTP

```
Ruijie#config terminal
Ruijie(config)#vlan range 10,20,30,40,50,60,70,80
Ruijie(config-vlan-range)#exit
Ruijie(config)#spanning-tree mst configuration ----->enter mst configuration mode
Ruijie(config-mst)#name ruijie ----->switches in a same MSTP area must have the same instance name
Ruijie(config-mst)#instance 1 vlan 10,20,30,40,60,70 ----->map vlan 10,20,30,40,60,70 to instance 1 , and switches in
a same MSTP area must have the same mapping
Ruijie(config-mst)#instance 2 vlan 50,80 -----> map vlan 50,80 to instance 2 , and switches in a same MSTP area
must have the same mapping
```

```
Ruijie(config-mst)#exit
Ruijie(config)#spanning-tree mst 0 priority 0 ----->By default , instance 0 exists ,and any other vlans that haven't
mapped to an instance are mapped to instance 0. SW1 is the root bridge for instance 0
Ruijie(config)#spanning-tree mst 1 priority 0 ----->SW1 is the root bridge in instance 1
Ruijie(config)#spanning-tree mst 2 priority 4096 ----->SW1 is the secondary bridge in instance 2
Ruijie(config)#spanning-tree ----->enable STP feature
```

Configuring AP

```
Ruijie#config terminal
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#switchport mode trunk
Ruijie(config-if-AggregatePort 1)#exit
Ruijie(config)#interface tengigabitEthernet 3/1
Ruijie(config-if-TenGigabitEthernet 3/1)#port-group 1
Ruijie(config-if-TenGigabitEthernet 3/1)#exit
Ruijie(config)#interface tengigabitEthernet 3/2
Ruijie(config-if-TenGigabitEthernet 3/2)#port-group 1
Ruijie(config-if-TenGigabitEthernet 3/2)#exit
Ruijie(config)#interface range gigabitEthernet 1/1-5
Ruijie(config-if-range)#switchport mode trunk ----->don't forget to prune trunk port
```

Configuring VRRP

```
Ruijie(config)#vlan 10
Ruijie(config)#inter vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0
Ruijie(config-if-VLAN 10)#vrrp 10 ip 192.168.10.254
Ruijie(config-if-VLAN 10)#vrrp 10 priority 120 ----->vrrp group id=10 , priority value =120(the bigger the
number , the more likely the switch will be chosen as the master ,and default value is 100)
Ruijie(config-if-VLAN 10)#exit

Ruijie(config)#vlan 20
Ruijie(config)#inter vlan 20
Ruijie(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0
Ruijie(config-if-VLAN 20)#vrrp 20 ip 192.168.20.254
Ruijie(config-if-VLAN 20)#vrrp 20 priority 120
Ruijie(config-if-VLAN 20)#exit

.....Configuration of VLAN 30,40,60,70 are omitted.....

VRRP primary gateway of VLAN 50,80 is SW2 which is the root bridge of instance 2
Ruijie(config)#vlan 50
```

```

Ruijie(config)#inter vlan 50
Ruijie(config-if-VLAN 50)#ip address 192.168.50.1 255.255.255.0
Ruijie(config-if-VLAN 50)#vrrp 50 ip 192.168.50.254 ----->vrrp group id=50 , priority value remains default
setting(the bigger the number , the more likely the switch will be chosen as the master ,and default value is 100)
Ruijie(config-if-VLAN 50)#exit

Ruijie(config)#vlan 80
Ruijie(config)#inter vlan 80
Ruijie(config-if-VLAN 80)#ip address 192.168.80.1 255.255.255.0
Ruijie(config-if-VLAN 80)#vrrp 80 ip 192.168.80.254 ----->vrrp group id=80 , priority value remains default
setting(the bigger the number , the more likely the switch will be chosen as the master ,and default value is 100)
Ruijie(config-if-VLAN 80)#exit

```

Configuring SW2

Configuring MSTP

```

Ruijie#config terminal
Ruijie(config)#vlan range 10,20,30,40,50,60,70,80
Ruijie(config-vlan-range)#exit
Ruijie(config)#spanning-tree mst configuration ----->enter mst configuration mode
Ruijie(config-mst)#name ruijie ----->switches in a same MSTP area must have the same instance name
Ruijie(config-mst)#instance 1 vlan 10,20,30,40,60,70 ----->map vlan 10,20,30,40,60,70 to instance 1 , and switches in
a same MSTP area must have the same mapping
Ruijie(config-mst)#instance 2 vlan 50,80 ----->map vlan 50,80 to instance 2 , and switches in a same MSTP area must
have the same mapping
Ruijie(config-mst)#exit
Ruijie(config)#spanning-tree mst 0 priority 4096 ----->By default , instance 0 exists ,and any other vlans that haven't
mapped to an instance are mapped to instance 0. SW2 is the secondary root bridge in instance 0
Ruijie(config)#spanning-tree mst 1 priority 4096----->SW2 is the secondary root bridge in instance 1
Ruijie(config)#spanning-tree mst 2 priority 0 ----->SW2 is the root bridge in instance 2
Ruijie(config)#spanning-tree ----->enable STP feature

```

Configuring AP

```

Ruijie#config terminal
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#switchport mode trunk
Ruijie(config-if-AggregatePort 1)#exit

```

```

Ruijie(config)#interface tengigabitEthernet 3/1
Ruijie(config-if-TenGigabitEthernet 3/1)#port-group 1
Ruijie(config-if-TenGigabitEthernet 3/1)#exit
Ruijie(config)#interface tengigabitEthernet 3/2
Ruijie(config-if-TenGigabitEthernet 3/2)#port-group 1
Ruijie(config-if-TenGigabitEthernet 3/2)#exit

Ruijie(config)#interface range gigabitEthernet 1/1-5
Ruijie(config-if-range)#switchport mode trunk ----->don't forget to prune trunk port

```

Configuring VRRP

VRRP backup gateway of VLAN 10,20,30,40,60,70 is SW2 which is the backup bridge of instance 1

```

Ruijie(config)#vlan 10
Ruijie(config)#inter vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.10.2 255.255.255.0
Ruijie(config-if-VLAN 10)#vrrp 10 ip 192.168.10.254 ----->vrrp group id=10 , priority value remains
default setting(the bigger the number , the more likely the switch will be chosen as the master ,and default value is
100) .
Ruijie(config-if-VLAN 10)#exit

Ruijie(config)#vlan 20
Ruijie(config)#inter vlan 20
Ruijie(config-if-VLAN 20)#ip address 192.168.20.2 255.255.255.0
Ruijie(config-if-VLAN 20)#vrrp 20 ip 192.168.20.254 ----->vrrp group id=20 , priority value remains default
setting(the bigger the number , the more likely the switch will be chosen as the master ,and default value is 100) .
Ruijie(config-if-VLAN 20)#exit

.....Configuration of VLAN 30,40,60,70 are omitted.....

Ruijie(config)#vlan 50
Ruijie(config)#inter vlan 50
Ruijie(config-if-VLAN 50)#ip address 192.168.50.2 255.255.255.0
Ruijie(config-if-VLAN 50)#vrrp 50 ip 192.168.50.254

```

```

Ruijie(config-if-VLAN 50)#vrrp 50 priority 120      ----->vrrp group id=50 , priority value =120(the bigger
the number , the more likely the switch will be chosen as the master ,and default value is 100)
Ruijie(config-if-VLAN 50)#exit
Ruijie(config)#vlan 80
Ruijie(config)#int vlan 80
Ruijie(config-if-VLAN 80)#ip address 192.168.80.2 255.255.255.0
Ruijie(config-if-VLAN 80)#vrrp 80 ip 192.168.80.254
Ruijie(config-if-VLAN 80)#vrrp 80 priority 120      ----->vrrp group id=80 , priority value =120(the bigger
the number , the more likely the switch will be chosen as the master ,and default value is 100)
Ruijie(config-if-VLAN 80)#exit

```

Configuring SW11, SW12, S13, S14, S15, S16 :

```

Ruijie#config terminal
Ruijie(config)#interface range gigabitEthernet 0/25-26
Ruijie(config-if-range)#switchport mode trunk
Ruijie(config-if-range)#exit
Ruijie(config)#vlan range 10,20,30,40,50,60,70,80
Ruijie(config-vlan-range)#exit
Ruijie(config)#spanning-tree mst configuration
Ruijie(config-mst)#name ruijie
Ruijie(config-mst)#instance 1 vlan 10,20,30,40,60,70
Ruijie(config-mst)#instance 2 vlan 50,80
Ruijie(config-mst)#exit
Ruijie(config)#spanning-tree

```

Connectting cables and verifying status of MSTP and VRRP

1. This example displays that SW1 is the root bridge in instance 0 and 1, and SW2 is the root bridge in instance 2.

SW1:

```

RuijieSW1#show spanning-tree summary

Spanning tree enabled protocol mstp

MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-49, 51-59, 61-69, 71-79, 81-4094

  Root ID    Priority    0
    Address    1414.4b5a.198c      -----> MAC address of Root bridge in instance 0

```

```

    this bridge is root
    Hello Time    2 sec  Forward Delay 15 sec  Max Age 20 sec
  Bridge ID  Priority    0
    Address      1414.4b5a.198c      ----->local MAC address
    Hello Time    2 sec  Forward Delay 15 sec  Max Age 20 sec
Interface      Role Sts Cost      Prio    OperEdge Type
-----
Ag1             Desg FWD 19000      128     False    P2p
Gi0/1           Desg FWD 20000      128     False    P2p

MST 1 vlans map : 10, 20, 30, 40, 60, 70
  Region Root Priority    0
    Address      1414.4b5a.198c      ----->MAC address of Root bridge in instance 1
    this bridge is region root
  Bridge ID  Priority    0
    Address      1414.4b5a.198c      ----->local MAC address
    Interface      Role Sts Cost      Prio    OperEdge Type
    -----
Ag1             Desg FWD 19000      128     False    P2p
Gi0/1           Desg FWD 20000      128     False    P2p

MST 2 vlans map : 50, 80
  Region Root Priority    0
    Address      1414.4b5a.18d4      ----->MAC address of Root bridge in instance 2
    this bridge is region root

  Bridge ID  Priority    4096
    Address      1414.4b5a.198c
  Interface      Role Sts Cost      Prio    OperEdge Type
  -----
Ag1             Root FWD 19000      128     False    P2p
Gi0/1           Desg FWD 20000      128     False    P2p

```

SW2:

```

Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp

MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-49, 51-59, 61-69, 71-79, 81-4094

  Root ID    Priority    0
    Address   1414.4b5a.198c   ----->MAC address of Root bridge which is SW1 in instance 0
    this bridge is root
    Hello Time 2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    4096
    Address   1414.4b5a.18d4   ----->local MAC address
    Hello Time 2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Ag1             Root FWD 19000    128     False    P2p
Gi2/0/1        Desg FWD 20000    128     False    P2p

MST 1 vlans map : 10, 20, 30, 40, 60, 70

  Region Root Priority    0
    Address   1414.4b5a.198c   ----->MAC address of Root bridge in instance 1
    this bridge is region root

  Bridge ID  Priority    4096
    Address   1414.4b5a.18d4   ----->local MAC address

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Ag1             Root FWD 19000    128     False    P2p
Gi2/0/1        Desg FWD 20000    128     False    P2p

MST 2 vlans map : 50, 80

  Region Root Priority    0
    Address   1414.4b5a.18d4   ----->MAC address of Root bridge in instance 2

```

```

    this bridge is region root
  Bridge ID  Priority    0
            Address    1414.4b5a.18d4  ----->local MAC address
Interface   Role Sts Cost      Prio    OperEdge Type
-----
Ag1          Desg FWD 19000      128     False    P2p
Gi2/0/1      Desg FWD 20000      128     False    P2p

```

```

Ruijie#show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-49, 51-59, 61-69, 71-79, 81-4094
  Root ID  Priority    0
          Address    1414.4b5a.198c  ----->MAC address of Root bridge which is SW1 in instance
0
    this bridge is root
    Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec
  Bridge ID  Priority    4096
          Address    1414.4b5a.18d4  ----->local MAC address
    Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec
Interface   Role Sts Cost      Prio    OperEdge Type
-----
Ag1          Root FWD 19000      128     False    P2p
Gi2/0/1      Desg FWD 20000      128     False    P2p

MST 1 vlans map : 10, 20, 30, 40, 60, 70
  Region Root Priority    0
          Address    1414.4b5a.198c  ----->MAC address of Root bridge in instance 1
    this bridge is region root
  Bridge ID  Priority    4096
          Address    1414.4b5a.18d4  ----->local MAC address

Interface   Role Sts Cost      Prio    OperEdge Type

```

```

-----
Ag1          Root FWD 19000    128    False   P2p
Gi2/0/1      Desg FWD 20000    128    False   P2p

MST 2 vlans map : 50, 80
  Region Root Priority    0
        Address    1414.4b5a.18d4    ----->MAC address of Root bridge in instance 2
        this bridge is region root
  Bridge ID  Priority    0
        Address    1414.4b5a.18d4    ----->local MAC address
Interface    Role Sts Cost        Prio    OperEdge Type
-----
Ag1          Desg FWD 19000    128    False   P2p
Gi2/0/1      Desg FWD 20000    128    False   P2p

```

```

Ruijie#show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-49, 51-59, 61-69, 71-79, 81-4094
  Root ID    Priority    0
        Address    1414.4b5a.198c    ----->MAC address of Root bridge which is SW1 in instance 0
        this bridge is root
        Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec
  Bridge ID  Priority    4096
        Address    1414.4b5a.18d4    ----->local MAC address
        Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec
Interface    Role Sts Cost        Prio    OperEdge Type
-----
Ag1          Root FWD 19000    128    False   P2p
Gi2/0/1      Desg FWD 20000    128    False   P2p

MST 1 vlans map : 10, 20, 30, 40, 60, 70
  Region Root Priority    0

```

```

        Address      1414.4b5a.198c  ----->MAC address of Root bridge in instance 1
        this bridge is region root
    Bridge ID  Priority    4096
        Address      1414.4b5a.18d4  ----->local MAC address

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Ag1             Root FWD 19000    128     False    P2p
Gi2/0/1        Desg FWD 20000    128     False    P2p

MST 2 vlans map : 50, 80
    Region Root Priority    0
        Address      1414.4b5a.18d4  ----->MAC address of Root bridge in instance 2
        this bridge is region root
    Bridge ID  Priority    0
        Address      1414.4b5a.18d4  ----->local MAC address

Interface      Role Sts Cost      Prio    OperEdge Type
-----
Ag1             Desg FWD 19000    128     False    P2p
Gi2/0/1        Desg FWD 20000    128     False    P2p

```

2. This example displays that SW1 is the master on vlan 10, 20,30,40,60 and 70, and the backup on vlan 50 and 80. SW2 is the master on vlan 50 and 80, and the backup on vlan 10, 20,30,40,60 and 70.

SW1:

```

Ruijie#show vrrp brief

Interface      Grp  Pri   timer   Own  Pre   State   Master addr
Group addr

VLAN 10        10   120   3.53    -    P     Master  192.168.10.1
192.168.10.254

VLAN 20        20   120   3.53    -    P     Master  192.168.20.1
192.168.20.254

```

| | | | | | | | |
|---------------------------|----|-----|------|---|---|--------|--------------|
| VLAN 30 192.168.30.254 | 30 | 120 | 3.53 | - | P | Master | 192.168.30.1 |
| VLAN 40 192.168.40.254 | 40 | 120 | 3.53 | - | P | Master | 192.168.40.1 |
| VLAN 50 192.168.50.254 | 50 | 100 | 3.60 | - | P | Backup | 192.168.50.2 |
| VLAN 60 192.168.60.254 | 60 | 120 | 3.53 | - | P | Master | 192.168.60.1 |
| VLAN 70 192.168.70.254 | 70 | 120 | 3.53 | - | P | Master | 192.168.70.1 |
| VLAN 80 192.168.80.254 | 80 | 100 | 3.60 | - | P | Backup | 192.168.80.2 |

SW2:

```
RuijieSW2#show vrrp brief
```

| Interface Group addr | Grp | Pri | timer | Own | Pre | State | Master addr |
|---------------------------|-----|-----|-------|-----|-----|--------|--------------|
| VLAN 10 192.168.10.254 | 10 | 100 | 3.60 | - | P | Backup | 192.168.10.1 |
| VLAN 20 192.168.20.254 | 20 | 100 | 3.60 | - | P | Backup | 192.168.20.1 |
| VLAN 30 192.168.30.254 | 30 | 100 | 3.60 | - | P | Backup | 192.168.30.1 |

| | | | | | | | |
|---------------------------|----|-----|------|---|---|--------|--------------|
| VLAN 40 192.168.40.254 | 40 | 100 | 3.60 | - | P | Backup | 192.168.40.1 |
| VLAN 50 192.168.50.254 | 50 | 120 | 3.53 | - | P | Master | 192.168.50.2 |
| VLAN 60 192.168.60.254 | 60 | 100 | 3.60 | - | P | Backup | 192.168.60.1 |
| VLAN 70 192.168.70.254 | 70 | 100 | 3.60 | - | P | Backup | 192.168.70.1 |
| VLAN 80 192.168.80.254 | 80 | 120 | 3.53 | - | P | Master | 192.168.80.2 |

3. This example displays how to verify Root Bridge on access switches and whether MSTP has blocked some ports to prevent a loop.

```
Ruijie#show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-49, 51-59, 61-69, 71-79, 81-4094

Root ID    Priority    0
    Address      1414.4b5a.198c
    this bridge is root
    Hello Time    2 sec  Forward Delay 15 sec  Max Age 20 sec

Bridge ID   Priority    32768
    Address      001a.a9c4.05f2
    Hello Time    2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface    Role Sts Cost      Prio    Type OperEdge
-----
Gi0/24       Altn BLK 20000    128     P2p    False  ----->one Blocked port
Gi0/23       Root FWD 20000    128     P2p    False  ----->one Root port
```

MST 1 vlans map : 10, 20, 30, 40, 60, 70

Region Root Priority 0

Address 1414.4b5a.198c ----->MAC address of Root bridge which is SW1 in instance 1
this bridge is region root

Bridge ID Priority 32768

Address 001a.a9c4.05f2

| Interface | Role | Sts Cost | Prio | Type | OperEdge | |
|-----------|----------|----------|------|------|----------|------------------------|
| ----- | | | | | | |
| Gi0/24 | Altn BLK | 20000 | 128 | P2p | False | ----->one Blocked port |
| Gi0/23 | Root FWD | 20000 | 128 | P2p | False | ----->one Root port |

MST 2 vlans map : 50, 80

Region Root Priority 0

Address 1414.4b5a.18d4 ----->MAC address of Root bridge which is SW2 in instance 2
this bridge is region root

Bridge ID Priority 32768

Address 001a.a9c4.05f2

| Interface | Role | Sts Cost | Prio | Type | OperEdge | |
|-----------|----------|----------|------|------|----------|------------------------|
| ----- | | | | | | |
| Gi0/24 | Root FWD | 20000 | 128 | P2p | False | ----->one Blocked port |
| Gi0/23 | Altn BLK | 20000 | 128 | P2p | False | ----->one Root port |

When you connect Ruijie switch to other vendors, pay attention to spanning-tree compatibility:

1. When you connect Ruijie to Cisco, you must double confirm whether Cisco firmware supports standard MSTP. So far, Cisco switch with firmware 12.25(SE) and above supports standard MSTP, but any other older firmware doesn't, so the old firmware that runs nonstandard MSTP has compatibility issue. So you must upgrade switch to version 12.25(SE) and above. If Cisco switch is too old to upgrade to version 12.25(SE) and above, you can disable STP and enable BPDU bridge mode to bypass all bpdu packets. To enable BPDU bridge mode, perform this task:

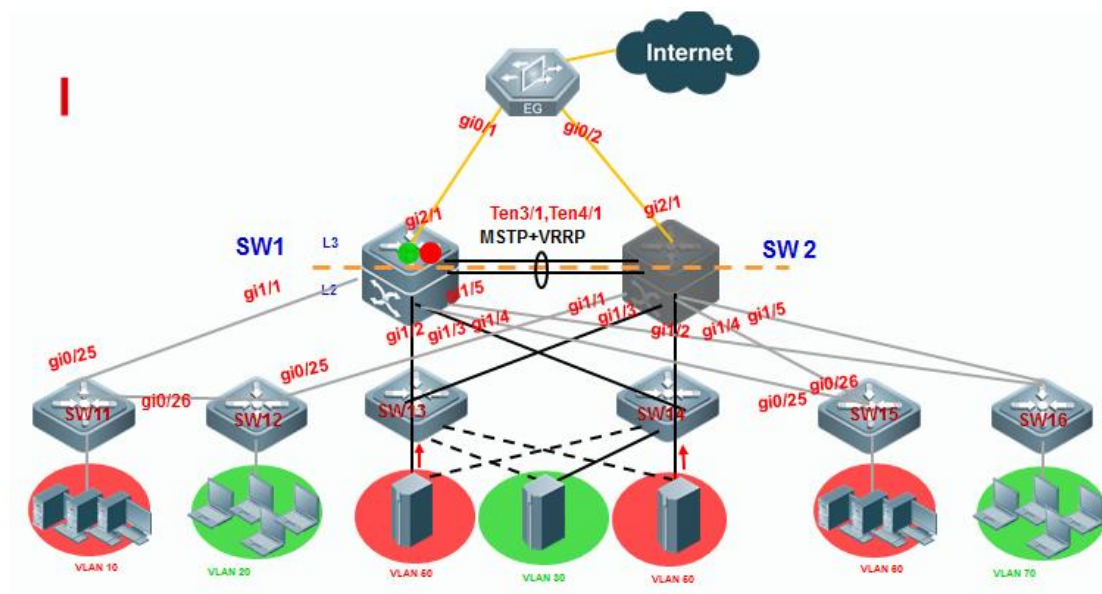
```
Ruijie(config)#no spanning-tree
```

```
Ruijie(config)#bridge-frame forwarding protocol bpdu
```

- We suggest you to configure completely the same MSTP name, revision, instance mapping when you enable MSTP on Ruijie and other vendors switch to prevent STP compatibility issue. You can also enable RSTP because RSTP has better compatibility.

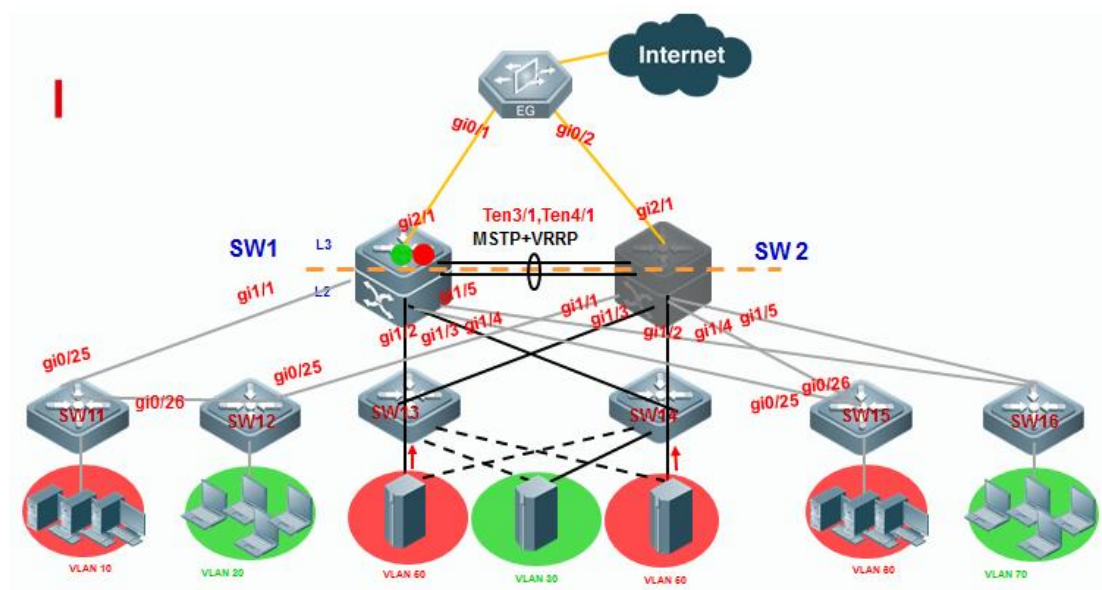
2.8.3.4 Configuring Spanning tree optimization

I. Network Topology



2.8.3.5 Verifying MSTP+VRRP

I. Network Topology

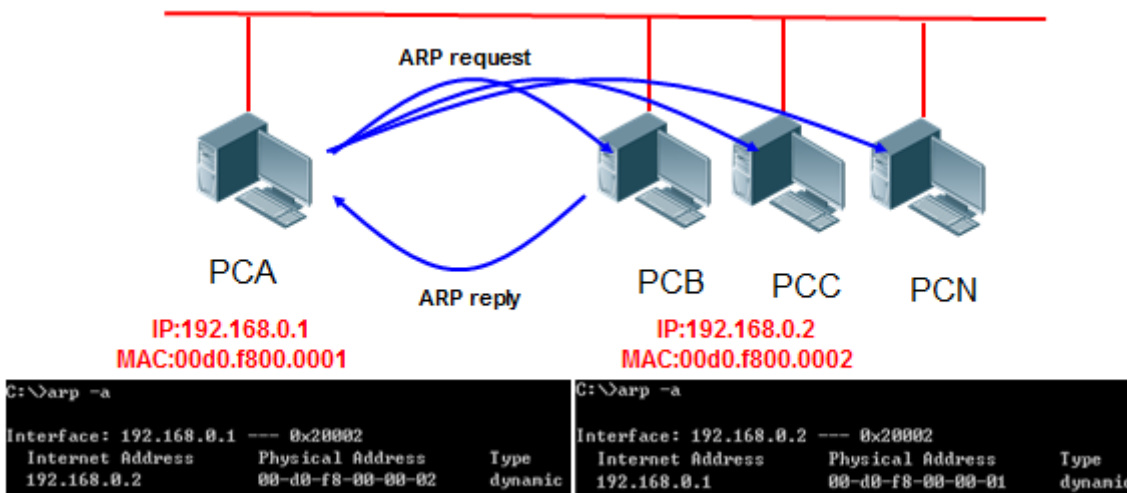


2.8.4 ARP Spoofing Protection

Overview

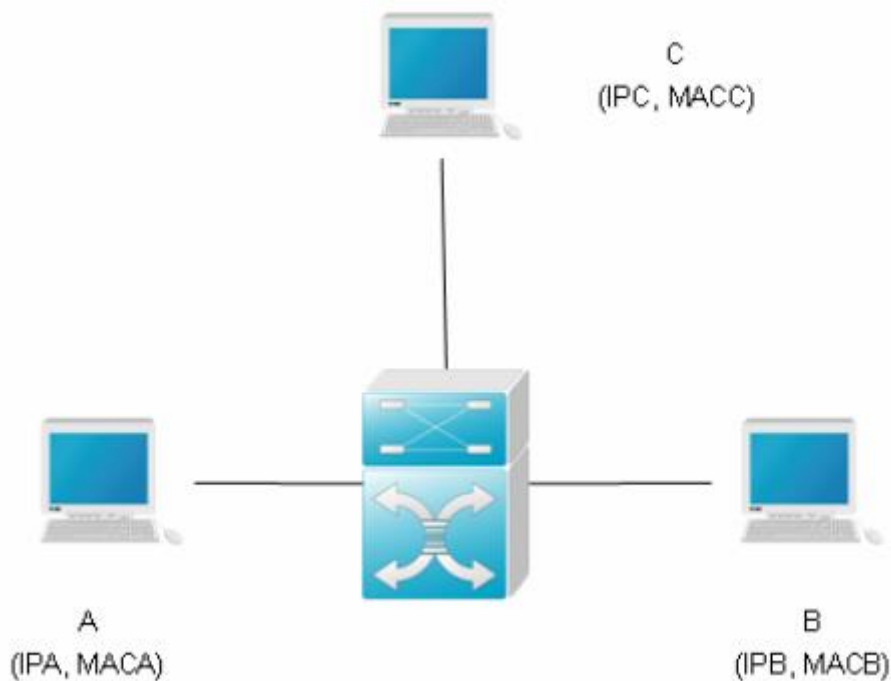
ARP (Address Resolution Protocol) provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, host B wants to send information to host A, but does not have the MAC address of host A in its ARP cache. In ARP terms, host B is the sender and host A is the target.

To get the MAC address of host A, host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of host A. All hosts within the broadcast domain receive the ARP request, and host A responds with its MAC address.



Feature

ARP itself does not check the validity of incoming ARP packets, a drawback of ARP. In this way, attackers can launch ARP spoofing attacks easily by exploiting the drawback of the protocol. The most typical one is the man in the middle attack, which is described as follows:



As shown in the diagram, devices A, B and C are connected to Ruijie device and located in the same subnet. Their IP and MAC addresses are respectively represented by (IPA, MACA), (IPB, MACB) and (IPC, MACC). When device A needs to communicate with device B in the network layer, device A broadcasts an ARP request in the subnet to query the MAC value of device B. Upon receiving this ARP request packet, device B updates its ARP buffer using IPA and MACA, and sends an ARP response. Upon receiving this response, device A updates its ARP buffer using IPB and MACB.

With this model, device C will cause the corresponding relationship of ARP entries in device A and device B incorrect. The policy is to broadcast ARP response to the network continuously. The IP address in this response is IPA/IPB, and the MAC address is MACC. Then, ARP entries (IPB and MACC) will exist in device A, and ARP entries (IPA and MACC) exist in device B. Communication between device A and device B is changed to communication with device C, which is unknown to devices A and B. Device C acts as an intermediary and it just modifies the received packets appropriately and forwards to another device. This is the well-known man in the middle attack.

2.8.4.1 Scenario of static IP address assignment

Scenario

Port IP&MAC binding + ARP-check: In a network without 802.1x authentication, you can manually bind IP&MAC address of users to a security entry on each port on a switch and enable ARP-check feature globally to prevent ARP spoofing. Users connected to a switch port can pass through the port verification and have access to network only when IP&MAC address of the users are totally the same to the security entry on the port.

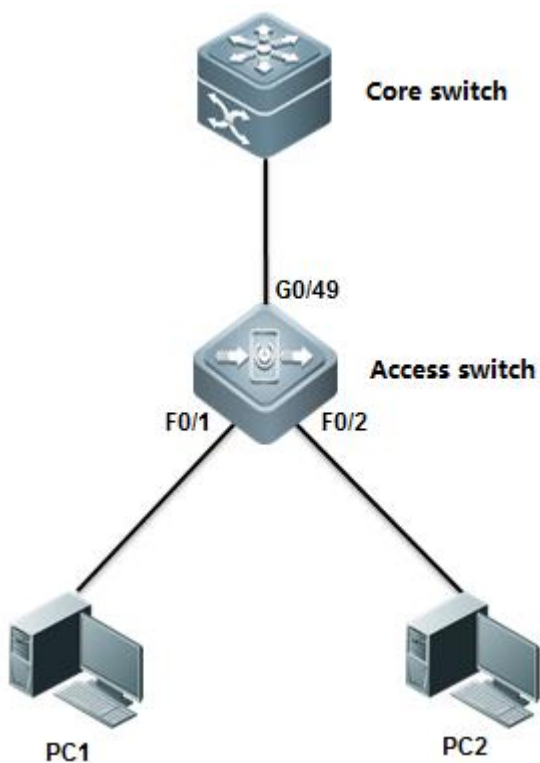
Merit: This is a very strict method to control all users in your network and switches verify each ARP packet in hardware without consuming CPU resource

Demerit: You must collect IP&MAC address of each users and the port numbers to which every users connect on each switch, so this method cost you plenty of time to collect information and configure switches and it is also not flexible if users move their physical location very often.

I. Requirements

Administrator assign IP address to users manually ,and configure "port-security + ARP-check" method on switches to defend against ARP spoofing.

II. Network Topology



III. Configuration Tips

1. You must enable port-security on port connected to users, not uplink port
2. You must enable ARP-check on port connected to users, not uplink port

IV. Configuration Steps

Configuring core switch:

Assign IP address to vlan 10 which is user gateway

```
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.1.254 255.255.255.0
```

```
Ruijie(config-if-VLAN 10)#end
Ruijie#wr
```

Configuring access switch:

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)#switchport port-security binding 0021.CCCF.6F70 vlan 10 192.168.1.1
-----> bind static IP address 192.168.1.1 and MAC address 0021.CCCF.6F70 on VLAN 10 to security entry on F0/1
Ruijie(config-if-FastEthernet 0/1)#switchport port-security ----->enable port-security
Ruijie(config-if-FastEthernet 0/1)#arp-check ----->enable arp-check
Ruijie(config-if-FastEthernet 0/1)#exit

Ruijie(config)#interfac fastEthernet 0/2
Ruijie(config-if-FastEthernet 0/2)# switchport port-security binding 0023.5abd.1975 vlan 10 192.168.1.2
----->bind static IP address 192.168.1.2 and MAC address 0023.5abd.1975 on VLAN 10 to security entry on
F0/2
Ruijie(config-if-FastEthernet 0/2)#switchport port-security ----->enable port-security
Ruijie(config-if-FastEthernet 0/2)#arp-check ----->enable arp-check
Ruijie#write

Ruijie(config)#interfac fastEthernet 0/3
Ruijie(config-if-FastEthernet 0/3)# switchport port-security binding 192.168.1.3
----->you can also bind only static IP address 192.168.1.3 to security entry on F0/3 in order to be more flexible but
lower security
Ruijie(config-if-FastEthernet 0/3)#switchport port-security
Ruijie(config-if-FastEthernet 0/3)#arp-check
Ruijie#write
```

V. Verification

- 1) How to display security entry on each port

```
Ruijie#show port-security address
Vlan Mac Address      IP Address      Type      Port      Rem
-----
1 0021.cccf.6f70 192.168.1.1    Configured Fa0/1
1 0023.5abd.1975 192.168.1.2    Configured Fa0/2
```

→ IP&MAC binding entries

- 2) How to display status of ARP-check

```
Ruijie#show interfaces arp-check list
```

| Interface | Sender MAC | Sender IP | Policy Source |
|-----------|----------------|-------------|---------------|
| Fa0/1 | 0021.cccf.6f70 | 192.168.1.1 | port-security |
| Fa0/2 | 0023.5abd.1975 | 192.168.1.2 | port-security |

ARP-check utilizes security entry of port-security to validate each ARP packet

Scenario

Global IP&MAC binding+ ARP-check: In a network without 802.1x authentication, you can manually bind IP&MAC address of users to global security table on a switch and enable ARP-check feature globally to prevent ARP spoofing. Users connected to a switch port can pass through the global verification and have access to network only when IP&MAC address of the users are totally the same to the global security table on the switch

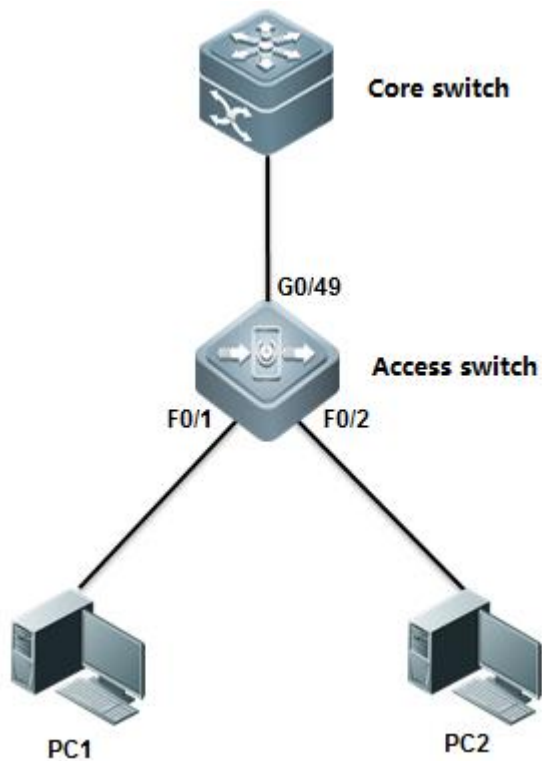
Merit: This is a less strict method to control all users in your network than solution 1, and switches verify each ARP packet in hardware without consuming CPU resource

Demerit: You must collect IP&MAC address of each users on each switch, so this method cost you plenty of time to collect information and configure switches.

I. Requirements

Administrator assign static IP address to users, and configures "port-security + ARP-check" method on switches to prevent ARP spoofing

II. Network Topology



III. Configuration Tips

1. Bind IP&MAC address of users to global security table
2. Configure uplink port as trusted port on which all packets can pass through without validation
3. Enable address-bind feature globally
4. Enable arp-check feature globally

IV. Configuration Steps

Configuring core switch:

Manually assign IP address to Vlan 10 which is user gateway

```
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-VLAN 10)#end
Ruijie#wr
```

Configuring access switch:

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#address-bind 192.168.1.1 0021.cccf.6f70 ----->bind IP 192.168.1.1 and MAC address
0021.cccf.6f70 to global security table
```

```

Ruijie(config)#address-bind 192.168.1.2 0023.5abd.1975 ----->bind IP 192.168.1.2 and MAC address
0023.5abd.1975 to global security table
Ruijie(config)#address-bind uplink gigabitEthernet 0/25 ----->configure uplink port G0/25 as trusted port on
which all packets can pass through without validation
Ruijie(config)#address-bind install ----->enable address-bind
Ruijie(config)#interface range fastEthernet 0/1-2
Ruijie(config-if-range)#arp-check ----->enable arp-check
Ruijie(config-if-range)#end
Ruijie#write

```

Note:

If users want to use IPv6 address to visit network, you must enable IPv6 compatible mode on switch that have address-bind enabled. Perform this task:

```

Ruijie(config)#address-bind ipv6-mode ?
compatible  IPV6 compatible mode ----->compatible mode ,allow binding users to visit network via IPv6
address
loose       IPV6 loose mode ----->loose mode , allow all IPv6 users to visit network unlimitedly
strict     IPV6 strict mode (default: strict)----->strict mode , even binding users can't visit network via
IPv6 address, this is the default mode
Ruijie(config)#address-bind ipv6-mode compatible

```

V. Verification

1. How to display global security table

```

Ruijie#show address-bind
Total Bind Addresses in System : 2
IP Address      Binding MAC Addr
-----
192.168.1.1     0021.cccf.6f70
192.168.1.2     0023.5abd.1975

```

2. How to display trusted port

```

Ruijie#show address-bind uplink
Ports      State
-----
Fa0/1      Disabled

```

3. How to verify ARP-check table

```

Ruijie#show interfaces arp-check list
Interface  Sender MAC      Sender IP      Policy Source
-----
Fa0/1      0023.5abd.1975  192.168.1.2   address-bind
Fa0/1      0021.cccf.6f70  192.168.1.1   address-bind
Fa0/2      0023.5abd.1975  192.168.1.2   address-bind
Fa0/2      0021.cccf.6f70  192.168.1.1   address-bind

```

policy source is address-bind

Scenario

802.1X authentication+ ARP-check: In a network that have 802.1x authentication enabled, users must be running 802.1X-compliant client software ,such as Ruijie supplicant SU and SA . Switch collects IP&MAC address when communicates with 802.1X-compliant client software and write these information into global security table.ARP-check validate each users based on thie global security table to prevent ARP spoofing.

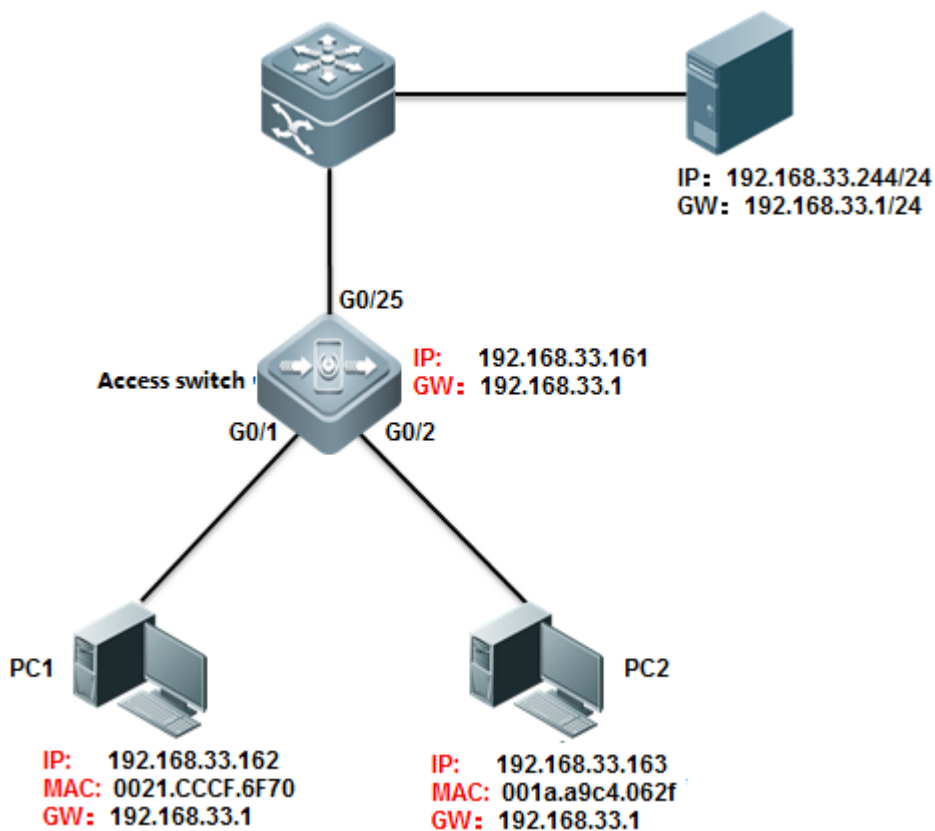
Merit: This is the simplest method for you to configure switch and maintenance

Demerit : You must build your network with Ruijie 802.1X-compliant client software SU/SA and a Radius Server (for example ,Ruijie SAM), and it consumes more hardware resource because it costs switch one more security entry in hardware when a user pass the authentication .

I. Requirements

Administrator assigns static IP address to user and enable 802.1x authentication through the overall network with Ruijie SU/SA and SAM to prevent ARP spoofing.

II. Network Topology



III. Configuration Tips

1. Enable basic dot1x authentication function on access switch
2. Modify authorization mode to "supplicant mode"
3. Enable arp-check on port connected to users

IV. Configuration Steps

Configuring access switch

1) Configure dot1x authentication on switch

For complete information about 802.1x configuration ,see switch configuration guide , such as 《RG-S8600E Series Switches RGOS Configuration Guide》

2) Configure authorization mode in "supplicant mode"

```
Ruijie(config)#aaa authorization ip-auth-mode supplicant
```

Note: If users want to use IPv6 address to visit network, you must enable IPv6 compatible mode on switch that have address-bind enabled. Perform this task:

```
Ruijie(config)#address-bind ipv6-mode ?
```

compatible IPv6 compatible mode ----->compatible mode ,allow binding users to visit network via IPv6 address

loose IPv6 loose mode ----->loose mode , allow all IPv6 users to visit network unlimitedly

strict IPv6 strict mode (default: strict)----->strict mode , even binding users can't visit network via IPv6

address, this is the default mode

```
Ruijie(config)#address-bind ipv6-mode compatible
```

3) Enable arp-check

```
Ruijie(config)#interface range g0/1-2
```

```
Ruijie(config-if-range)#arp-check
```

```
Ruijie(config-if-range)#end
```

```
Ruijie#write
```

V. Verification

```
Ruijie(config)#show interfaces gigabitEthernet 0/1 arp-check list
```

2.8.4.2 Scenario of dynamic IP address assignment (DHCP)

Scenario

DHCP Snooping with ARP-check: This solution can prevent ARP spoofing in the network in which the DHCP server assigns IP addresses to users. You can also enable 802.1x authentication or web authentication or you can disable any authentications in your network.

Merit: Very simple configuration and easy maintenance.

Demerit: DHCP snooping and ARP-check are enforced in hardware, so this method is not applied if there are insufficient hardware resources available on the switch. How many users the switch can carry depends on its specification.

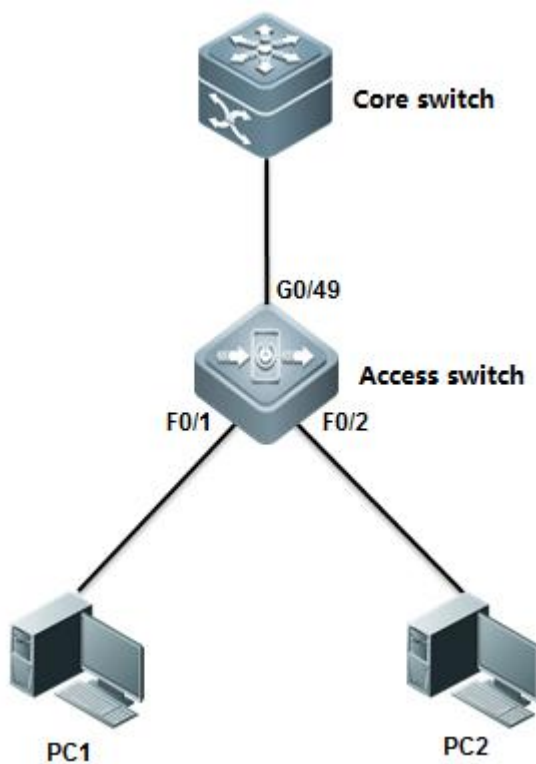
When switch hardware resources are insufficient, the system returns the following syslog:

%SECURITY-3-TCAM_RESOURCE_LIMIT: TCAM resource is temporarily not available.

I. Requirements

DHCP server assigns IP addresses to users, and the administrator uses "DHCP Snooping with ARP-check" to prevent ARP spoofing.

II. Network Topology



III. Configuration Tips

1. Core switch acts as DHCP server
2. Enable DHCP Snooping on access switch and configure uplink port as DHCP Snooping trusted port.

3. Enable ARP-check on ports connected to user

IV. Configuration Steps

Configuring core switch:

1. Enable DHCP service

```
Ruijie(config)#service dhcp
```

2. Manually Assign IP address to vlan 1 which is user gateway

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-VLAN 1)#exit
```

3. Create DHCP IP address pool

```
Ruijie(config)#ip dhcp pool vlan1
Ruijie(dhcp-config)#network 192.168.1.0 255.255.255.0      ----->network subnet
Ruijie(dhcp-config)#dns-server 218.85.157.99                ----->DNS Server
Ruijie(dhcp-config)#default-router 192.168.1.254            ----->specify user gateway
Ruijie(dhcp-config)#end
Ruijie#wr
```

Configuring access switch:

1. Enable DHCP Snooping

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#ip dhcp snooping
```

2. Configure the port connected to DHCP server as DHCP Snooping trusted port.

```
Ruijie(config)#interface gigabitEthernet 0/49
Ruijie(config-GigabitEthernet 0/49)#ip dhcp snooping trust ----->By default , all ports are DHCP Snooping
untrusted port. Only trusted port can forward DHCP Offer and Ack packets
```

Note:

If users want to use IPv6 address to visit network, you must enable IPv6 compatible mode on switch that have address-bind enabled. Perform this task

```
Ruijie(config)#address-bind ipv6-mode ?
compatible  IPV6 compatible mode ----->compatible mode ,allow binding users to visit network via IPv6
address
loose       IPV6 loose mode ----->loose mode , allow all IPv6 users to visit network unlimitedly
strict      IPV6 strict mode (default: strict)----->strict mode , even binding users can't visit network via
IPv6 address, this is the default mode
```

```
Ruijie(config)#address-bind ipv6-mode compatible
```

3. Enable arp-check

```
Ruijie(config)#interface range fastEthernet 0/1-2
```

```
Ruijie(config-if-range)#arp-check
```

V. Verification

```
Ruijie#show ip dhcp binding
```

| IP address | Client-Identifier/ Hardware address | Lease expiration | Type |
|-------------|--|---------------------------|-----------|
| 192.168.1.1 | 0100.21cc.cf6f.70 | 000 days 23 hours 42 mins | Automatic |
| 192.168.1.2 | 0100.1aa9.c405.f347. 6967.6162.6974.4574. 6865.726e.6574.302f. 31 | 000 days 23 hours 44 mins | Automatic |

allocated IP address

01 indicates ethernet and following 12 bits indicate client MAC address

2. How to display NIC information on a station, click " Start -> Run -> cmd -> ipconfig/all "

```
Ethernet adapter
```

```
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : 00-21-CC-CF-6F-70 → MAC address
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::248b:c4f7:acc4:8ec1%13<Preferred>
IPv4 Address. . . . . : 192.168.1.1<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 2013 . 3 . 8 9:38:56
Lease Expires . . . . . : 2013 . 3 . 9 9:39:40
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 352330188
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-5B-95-3B-60-67-20-AE-75-E4
DNS Servers . . . . . : 218.85.157.99
NetBIOS over Tcpip. . . . . : Enabled
```

3. How to display DHCP snooping table on a access switch

```
Ruijie#show ip dhcp snooping binding
```

Total number of bindings: 2

| MacAddress | IpAddress | Lease(sec) | Type | VLAN | Interface |
|----------------|-------------|------------|---------------|------|------------------|
| 0021.cccf.6f70 | 192.168.1.1 | 86234 | dhcp-snooping | 1 | FastEthernet 0/1 |
| 001a.a9c4.05f3 | 192.168.1.2 | 86367 | dhcp-snooping | 1 | FastEthernet 0/2 |

4. How to display ARP-Check table

```
Ruijie#show interfaces arp-check list
```

| Interface | Sender MAC | Sender IP | Policy Source |
|-----------|----------------|-------------|---------------|
| Fa0/1 | 001a.a9c4.05f3 | 192.168.1.2 | DHCP snooping |
| Fa0/2 | 0021.cccf.6f70 | 192.168.1.1 | DHCP snooping |

policy source is
DHCP snooping

Scenario

DHCP Snooping with DAI(Dynamic ARP inspection): This solution can prevent ARP spoofing in the network in which DHCP server assigns IP address to users. You can also enable 802.1x authentication or web authentication or you can disable any authentications in your network.

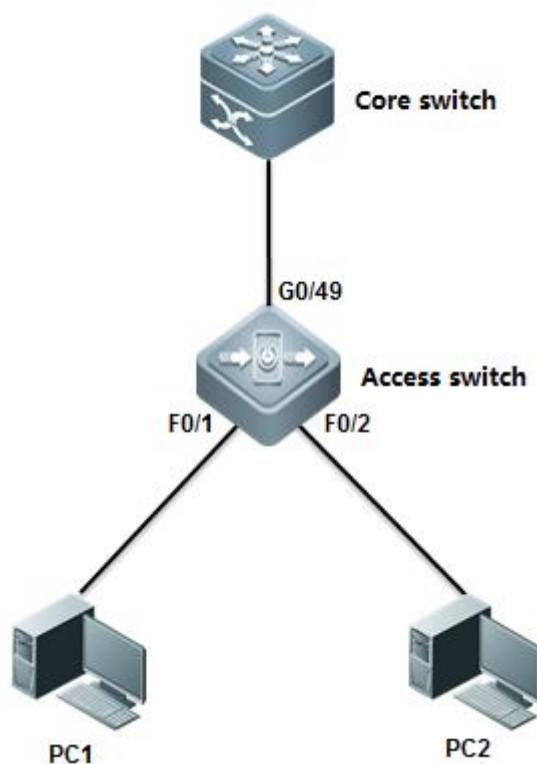
Merit: Very simple configuration and easy maintenance. DAI is enforced in CPU, but ARP-check is enforced in hardware.

Demerit: When an access switch carries more than 50 users, we recommend you to use solution 1 in case CPU resources are insufficient.

I. Requirements

DHCP server assigns IP address to users, and administrator uses "DHCP Snooping with DAI" to prevent ARP spoofing.

II. Network Topology



III. Configuration Tips

1. Core switch acts as DHCP server
2. Enable DHCP Snooping on access switch and configure uplink port as DHCP Snooping trusted port.
3. Enable DAI on access switch and configure uplink port as DAI trusted port.
4. Fine tune CPP and NFPP parameters and prune trunk port

IV. Configuration Steps

Configuring core switch:

1. Enable DHCP service

```
Ruijie(config)#service dhcp
```

2. Manually Assign IP address to vlan 1 which is user gateway

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-VLAN 1)#exit
```

3. Create DHCP IP address pool

```
Ruijie(config)#ip dhcp pool vlan1
Ruijie(dhcp-config)#network 192.168.1.0 255.255.255.0      ----->network segment
Ruijie(dhcp-config)#dns-server 218.85.157.99                ----->DNS server
Ruijie(dhcp-config)#default-router 192.168.1.254            ----->specify user gateway
Ruijie(dhcp-config)#end
Ruijie#wr
```

Configuring access switch:

1. Enable DHCP Snooping

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#ip dhcp snooping
```

2. Configure the port connected to DHCP server as DHCP Snooping trusted port

```
Ruijie(config)#interface gigabitEthernet 0/49
Ruijie(config-GigabitEthernet 0/49)#ip dhcp snooping trust ----->By default , all ports are DHCP snooping
untrust ports. Only trusted port can forward DHCP Offer and Ack packets
```

3. Enable DAI in VLAN 1

```
Ruijie(config)#ip arp inspection vlan 1 ----->DAI inspects VLAN 1
```

4 . Configure the uplink port as DAI trusted port

```
Ruijie(config)#int gigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#ip arp inspection trust
```

Configuring DAI optimization (Mandatory)

When DAI is enabled, switch forwards all ARP packets to CPU to validate, and you must configure the following optimization.

1. Prune trunk port on uplink port on access switch

This example shows how to prune trunk port G0/25 and this port can carry traffic for VLAN 1 and VLAN 9 only:

```
Ruijie(config-if-GigabitEthernet 0/25)#switchport trunk allowed vlan remove 2-8,10-4094
```

For complete information, see [Initialization --->Configuring a Layer 2 Port ---> Access or Trunk port](#)

3. Disable NFPP on the uplink port on access switch, otherwise if the number of ARP packets sent from Core switch to access switch exceeds the default NFPP rate-limit threshold, NFPP will drop the exceeding arp packets which would be users'

```
Ruijie(config)#int g0/25
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp arp-guard enable
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp dhcp-guard enable
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp dhcpv6-guard enable
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp icmp-guard enable
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp ip-guard enable
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp nd-guard enable
Ruijie(config-if-GigabitEthernet 0/25)#exit
Ruijie(config)#
```

4. Increase CPP arp rate-limit threshold to 500PPS (180PPS by default) in case that CPP drops the exceeding packets.

```
Ruijie(config)#cpu-protect type arp pps 500
```

V. Verification

1. How to display DAI status

```
Ruijie#sho ip arp inspection vlan 1
Vlan      Configuration
-----
1         Enable
Ruijie#
```

2. How to display DHCP Snooping binding table

```
Ruijie#show ip dhcp snooping binding.  
  
Total number of bindings: 2  
  
-----  
MacAddress      IpAddress      Lease(sec)    Type           VLAN  Inter  
-----  
0021.cccf.6f70   192.168.1.1    86234         dhcp-snooping  1     Fast  
001a.a9c4.05f3   192.168.1.2    86367         dhcp-snooping  1     Fast
```

Scenario

802.1X authentication with ARP-check: In a network that have 802.1x authentication enabled, users must be running 802.1X-compliant client software ,such as Ruijie supplicant SU and SA and DHCP server assigns IP address to users before authentication.

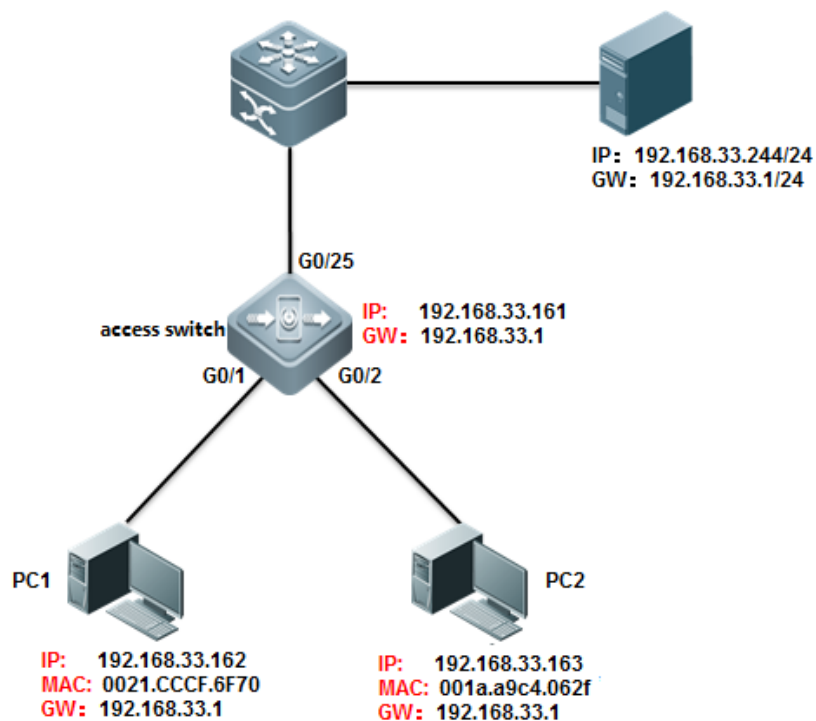
Merit: This is the simplest method for you to configure switch and maintenance

Demerit : You must build your network with Ruijie 802.1X-compliant client software SU/SA and a Radius Server (for example ,Ruijie SAM), and it consumes more hardware resource because it costs switch one more security entry in hardware when a user pass the authentication .In addition , you must configure a global security tunnel to bypass DHCP packets because users must acquire IP address before 802.1X authentication

I. Requirements

DHCP Server assigns IP address to users ,then administrator uses "802.1X authentication+ ARP-check" to prevent ARP spoofing.

II. Network Topology



III. Configuration Tips

1. Enable basic dot1x authentication on access switch
2. Configure a global security tunnel to bypass DHCP packets
3. Modify authorization mode to "supplicant mode"
4. Enable arp-check on port connected to users

IV. Configuration Steps

Configuring access switch

1. Configure dot1x authentication on switch

For complete information about 802.1x configuration, see switch configuration guide, such as 《RG-S8600E Series Switches RGOS Configuration Guide》

3. Configure a global security tunnel to bypass DHCP packets

```
Ruijie(config)#expert access-list extended dhcp
Ruijie(config-exp-nacl)#permit udp any any any any eq bootps ----->bypass DHCP packets
Ruijie(config-exp-nacl)#
Ruijie(config)#security global access-group dhcp
```

4. Modify authorization mode to "supplicant mode"

```
Ruijie(config)#aaa authorization ip-auth-mode supplicant
```

Note:

If users want to use IPv6 address to visit network, you must enable IPv6 compatible mode on switch that have address-bind enabled. Perform this task:

```
Ruijie(config)#address-bind ipv6-mode ?
compatible  IPV6 compatible mode  ----->compatible mode ,allow binding users to visit network via IPv6
address
loose       IPV6 loose mode        ----->loose mode , allow all IPv6 users to visit network unlimitedly
strict      IPV6 strict mode      (default: strict)----->strict mode , even binding users can't visit network via
IPv6 address, this is the default mode
Ruijie(config)#address-bind ipv6-mode compatible
```

5. Enable arp-check

```
Ruijie(config)#interface range g0/1-2
Ruijie(config-if-range)#arp-check
Ruijie(config-if-range)#end
Ruijie#write
```

V. Verification

```
Ruijie(config)#show interfaces gigabitEthernet 0/1 arp-check list
```

2.8.5 L2 GRE**2.8.5.1 L2 GRE Principle and Scenario****Scenario**

In recent years, server high-availability cluster technologies and virtual server dynamic migration technologies (such as VMotion of VMware) have been widely used in disaster recovery and computing resource allocation of a data center. Both technologies not only require extensive layer-2 network access in a data center but also wide layer-2 network extension between data centers. The L2 GRE function can exactly satisfy the requirement of connection between offsite data centers at layer 2.

Overview

Generic Routing Encapsulation (GRE) is a protocol that encapsulates data packets of certain network layer protocols (for example, IP and IPX) so that encapsulated data packets can be transmitted in another network layer protocol (IP). L2 GRE provides L2VPN services via the GRE tunnel in the IP core network.

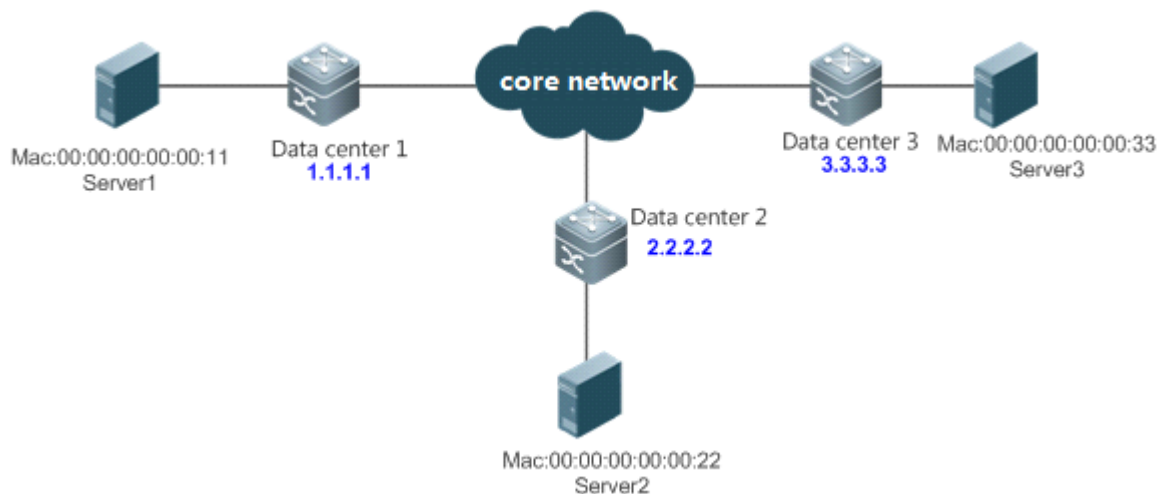
It provides two kinds of L2VPN services: L2 GRE LINE and L2 GRE LAN.

L2 GRE LINE is an end-to-end L2 service carrying technology and implements point-to-point L2VPN. It provides IP-based L2VPN services.



IP Core Network

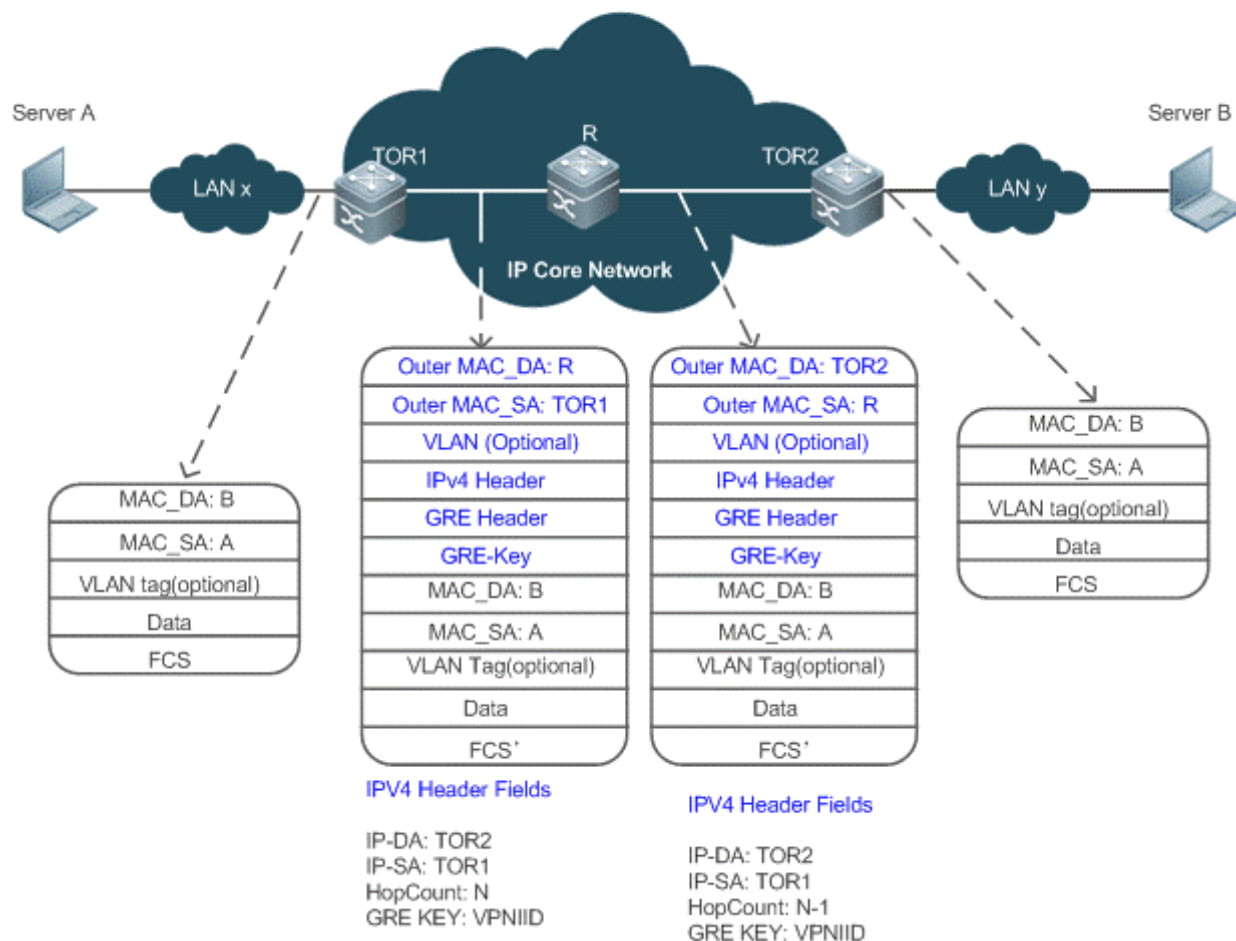
L2 GRE LAN is a technology that provides virtual private Ethernet in the IP network.



L2 GRE encapsulates the Ethernet packets into GRE packets and transmits them in the IP network, and the receiver decapsulates the GRE packets into the Ethernet packets and forward them.

L2 GRE Forwarding Principle

As shown in the following figure, L2 GRE encapsulates the Ethernet packets into GRE packets and transmits them in the IP network, and the receiver decapsulates the GRE packets into the Ethernet packets and forward them.



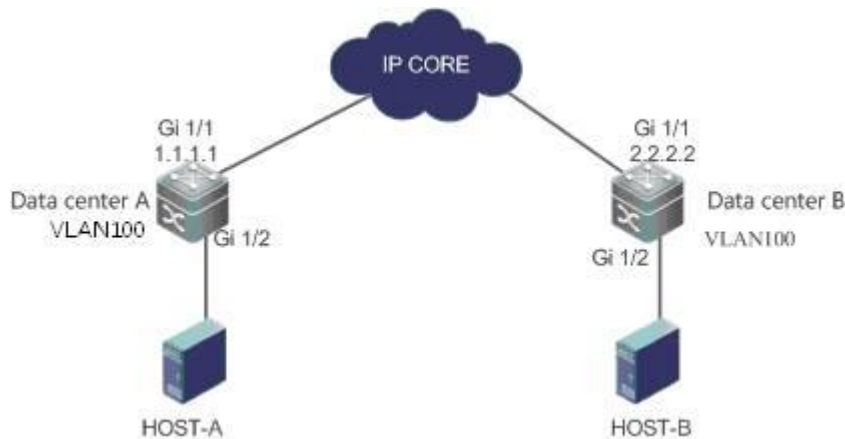
- 1) Switch TOR1 receives the Ethernet packets from LANX and encapsulates them into L2 GRE packets.
- 2) L2 GRE packets are forwarded in the IP core network. As shown in the above figure, GRE packets are forwarded by R.
- 3) TOR2 receives GRE packets, decapsulates them, and forwards them at layer 2 LAN.

2.8.5.2 L2 GRE LINE

I. Requirements

Two data centers are connected at layer 2 via the IP core network.

II. Network Topology



III. Configuration Tips

Configure VLANs on the switch. (Omitted)

Configure an IPv4 unicast routing protocol (such as OSPF) to ensure connectivity. (Omitted)

Create an L2 GRE instance.

Configure the local address and destination address of the L2 GRE instance.

Configure VLANs that the L2 GRE instance is allowed to forward data from.

Enable the keep-alive function. (Optional)

Note: The keep-alive function detects the destination address of the instance (which is also called neighbor detection). After the function is enabled, a prompt of the neighbor status is printed to the console via syslog. For example:

```
%L2GRE-6-KEEPALIVE: L2GRE instance VPNID[4000] Source[3.1.1.1] to Destination[4.1.1.1] keepalive is down.
```

```
%L2GRE-6-KEEPALIVE: L2GRE instance VPNID[4000] Source[3.1.1.1] to Destination[4.1.1.1] keepalive is up.
```

It is recommended to enable the keep-alive function.

IV. Configuration Steps

Configure Data Center Switch A.

```
A#conf t
A(config)# l2 gre vpn-l2gre id 100 type line
A(config-l2gre-line-100)# source interface gi1/1
A(config-l2gre-line-100)# destination 2.2.2.2
A(config-l2gre-line-100)# extend-vlan add 100
A(config-l2gre-line-100)# keepalive 60 3
A(config-l2gre-line-100)# end
A(config)#
```

Configure Data Center Switch B.---->See the steps for configuring Data Center Switch A.

```
B#conf t
B(config)# l2 gre vpn-l2gre id 100 type line
```

```

B(config-l2gre-line-100)# source interface gi1/1
B(config-l2gre-line-100)# destination 1.1.1.1
B(config-l2gre-line-100)# extend-vlan add 100
B(config-l2gre-line-100)# keepalive 60 3
B(config-l2gre-line-100)# end
B(config)#

```

V. Verification

1. View details of the L2 GRE instance of data center switch A.

```

A#show l2 gre vpn-l2gre
name: vpn-l2gre id: 100  type: l2gre-line
source: 1.1.1.1
destination: 2.2.2.2
extend-vlan: 100
tunnel ttl: 64
Keepalive set (60 sec), retries 3

```

3. View details of the L2 GRE instance of data center switch B.

```

B#show l2 gre vpn-l2gre
name: vpn-l2gre  id: 100  type: l2gre-line
source: 2.2.2.2
destination: 1.1.1.1
extend-vlan: 100
tunnel ttl: 64
Keepalive set (60 sec), retries 3

```

3. HOST A and HOST B can access each other.

4. The data center switches can learn the MAC addresses in the layer-2 network.

```

A# show l2 gre vpn-l2gre mac

```

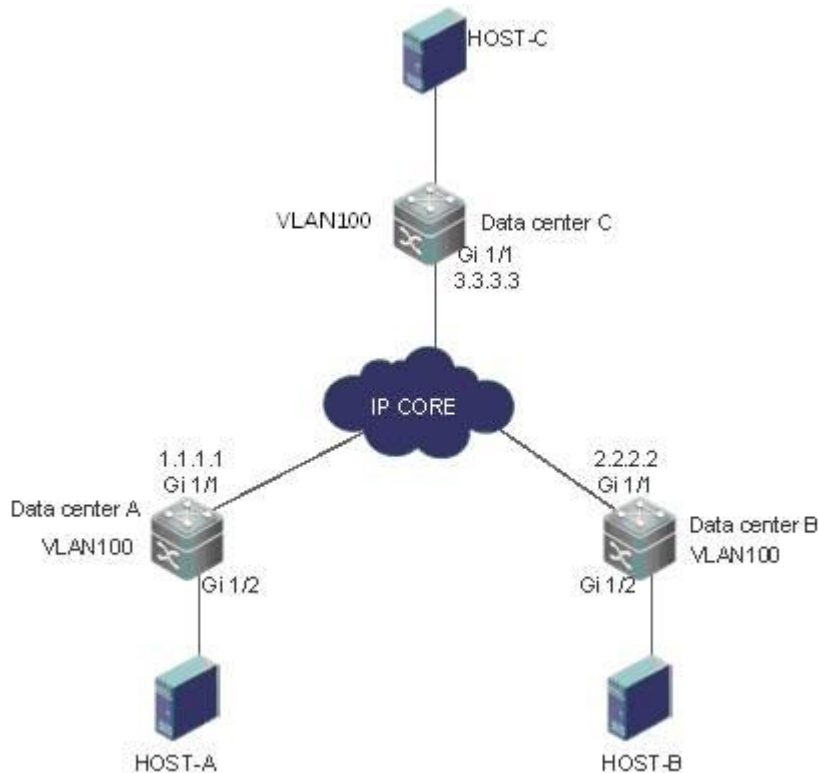
| MAC Address | Destination Address | Type | Interface |
|----------------|---------------------|------|-----------|
| 14fe.b5e1.0890 | 2.2.2.2 | D | |
| 14fe.b5e1.0970 | | D | Gi1/2 |

2.8.5.3 L2 GRE LAN

I. Requirements

Three data centers in two sites are connected at layer 3 via the IP core network.

II. Network Topology



III. Configuration Tips

Configure VLANs on the switch. (Omitted)

Configure an IPv4 unicast routing protocol (such as OSPF) to ensure connectivity. (Omitted)

Enable the multicast IGMP function to ensure that the switch can receive packets from a specific multicast group. (Optional and omitted)

Create an L2 GRE instance.

Configure the local address and destination address of the L2 GRE instance.

Configure VLANs that the L2 GRE instance is allowed to forward data from.

Enable the keep-alive function. (Optional)

Enable multicast and GRE packets flooding function (**Optional: Enable it when the multicast function is needed**).

Note: The keep-alive function detects the destination address of the instance (which is also called neighbor detection). After the function is enabled, a prompt of the neighbor status is printed to the console via syslog. For example:

```
%L2GRE-6-KEEPALIVE: L2GRE instance VPNID[4000] Source[3.1.1.1] to Destination[4.1.1.1] keepalive is down.
```

```
%L2GRE-6-KEEPALIVE: L2GRE instance VPNID[4000] Source[3.1.1.1] to Destination[4.1.1.1] keepalive is up.
```

It is recommended to enable the keep-alive function.

IV. Configuration Steps

Configure Data Center Switch A.

```
A#conf t
A(config)# l2 gre vpn-l2gre id 100 type lan
```

```
A(config-l2gre-lan-100)# source interface gi1/1
A(config-l2gre-lan-100)# destination 3.3.3.3
A(config-l2gre-lan-100)# destination 2.2.2.2
A(config-l2gre-lan-100)# extend-vlan add 100
A(config-l2gre-lan-100)# keepalive 60 3
A(config-l2gre-lan-100)# multicast 224.1.1.1
A(config-l2gre-lan-100)# end
A(config)#
```

Configure Data Center Switch B---->[the same configuration with switch A](#)

```
B#conf t
B(config)# l2 gre vpn-l2gre id 100 type lan
B(config-l2gre-lan-100)# source interface gi1/1
B(config-l2gre-lan-100)# destination 3.3.3.3
B(config-l2gre-lan-100)# destination 1.1.1.1
B(config-l2gre-lan-100)# extend-vlan add 100
B(config-l2gre-lan-100)# keepalive 60 3
B(config-l2gre-lan-100)# multicast 224.1.1.1
B(config-l2gre-lan-100)# end
```

Configure Data Center Switch C---->[the same configuration with switch A](#)

```
C#conf t
C(config)# l2 gre vpn-l2gre id 100 type lan
C(config-l2gre-lan-100)# source interface gi1/1
C(config-l2gre-lan-100)# destination 2.2.2.2
C(config-l2gre-lan-100)# destination 1.1.1.1
C(config-l2gre-lan-100)# extend-vlan add 100
C(config-l2gre-lan-100)# keepalive 60 3
C(config-l2gre-lan-100)# multicast 224.1.1.1
C(config-l2gre-lan-100)# end
```

V. Verification

1. View details of the L2 GRE instance of data center switch A.

```
A#show l2 gre vpn-l2gre
name: vpn-l2gre id: 100 type: l2gre-lan
source: 1.1.1.1
destination: 2.2.2.2
destination: 3.3.3.3
extend-vlan: 100
tunnel ttl: 64
```

```
Keepalive set (60 sec), retries 3
multicast: enable. Ip 224.1.1.1
```

3. View details of the L2 GRE instance of data center switch B.

```
B#show l2 gre vpn-l2gre
name: vpn-l2gre   id: 100   type: l2gre-lan
source: 2.2.2.2
destination: 1.1.1.1
destination: 3.3.3.3
extend-vlan: 100
tunnel ttl: 64
Keepalive set (60 sec), retries 3
multicast: enable. Ip 224.1.1.1
```

4. View details of the L2 GRE instance of data center switch C.

```
C#show l2 gre vpn-l2gre
name: vpn-l2gre   id: 100   type: l2gre-lan
source: 3.3.3.3
destination: 1.1.1.1
destination: 2.2.2.2
extend-vlan: 100
tunnel ttl: 64
Keepalive set (60 sec), retries 3
multicast: enable. Ip 224.1.1.1
```

4. HOST A and HOST B can access each other.
5. The data center switches can learn the MAC addresses in the layer-2 network.

```
A# show l2 gre vpn-l2gre mac
```

| MAC Address | Destination Address | Type | Interface |
|----------------|---------------------|------|-----------|
| 14fe.0811.7300 | 3.3.3.3 | D | |
| 14fe.b5e1.0890 | 2.2.2.2 | D | |
| 14fe.b5e1.0970 | | D | Gi1/2 |

2.8.6 VSD

Scenario

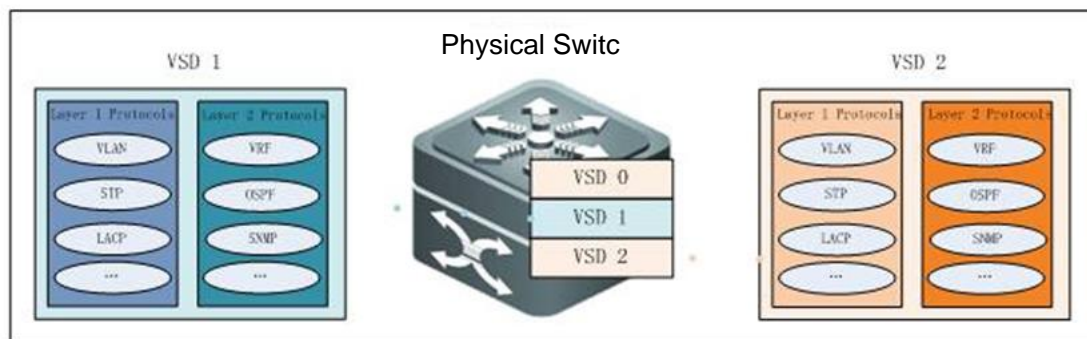
As the data center network expands, the service type is varied, and network management becomes more complicated, higher requirements are raised on service isolation, safety, and reliability of the network. With the rapid development of hardware and maturity of the multi-frame, clustered, and distributed routing and switching system, the service processing capability of a single physical network device has reached a new level. It is urgent to make full use of the powerful service

processing capability of a single physical device, adapt to the current service requirements, and realize smooth evolution of future expansion. Network device virtualization is a perfect method. It provides an easier virtualization means for network users. It is not limited to specific services or channels but serves to provide virtualization of the entire device.

Function Overview

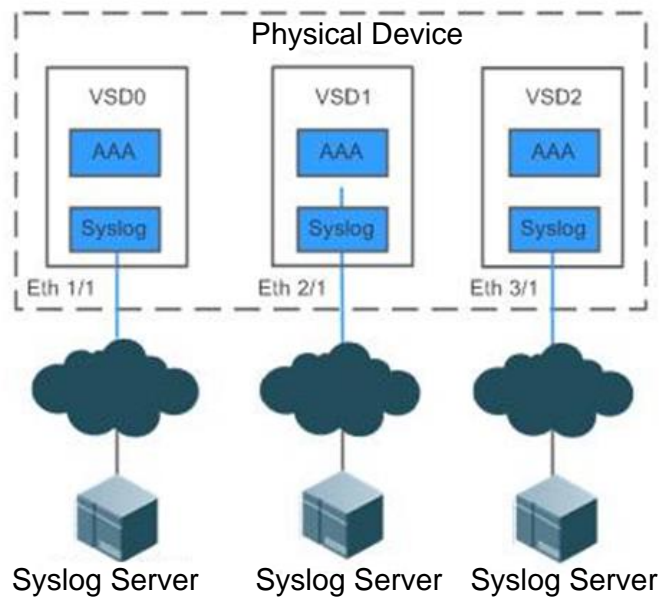
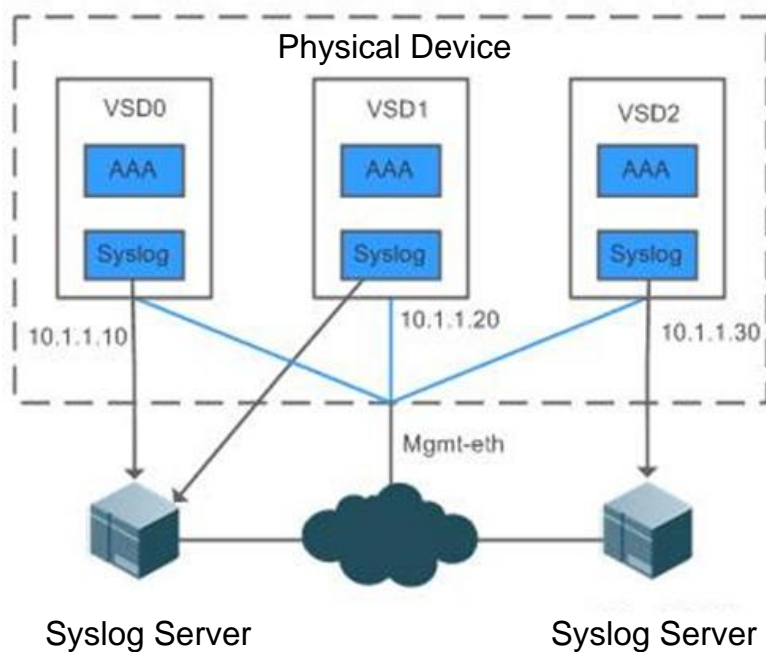
The Virtual Switch Device (VSD) is a network system virtualization technology which divides a physical device into multiple logical devices. Each logical device is called a VSD. Each VSD has independent hardware and software resources, including independent interface resources, CPU resources, independently-maintained routing table and forwarding table, and its own administrator and configuration file. For users, each VSD is an independent device.

By VSDx technology, a physical device can be virtualized to multiple logical devices, as shown in the following figure. A physical device can carry multiple network nodes in the logical topology to maximize utilization of available resources and reduce network operation costs. Different VSs can be deployed with different services to isolate services from failures, improving safety and reliability of the network.



VSD Management

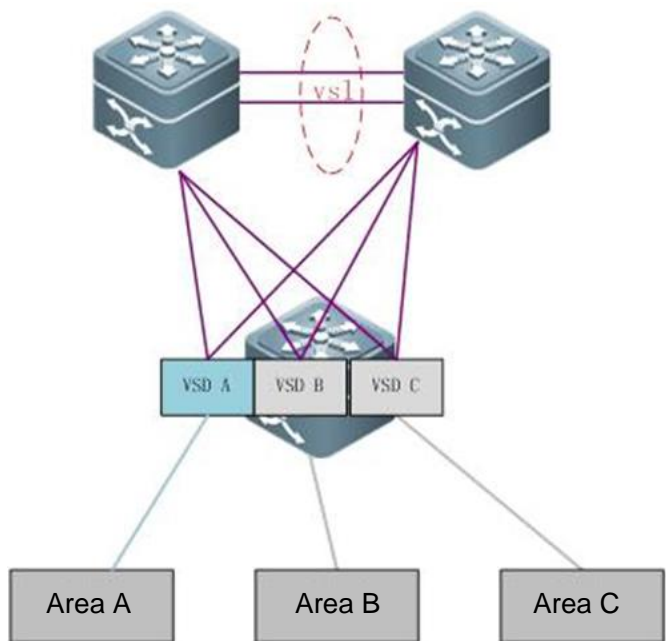
Out-of-band management is management through the mgmt interface. Inband management is management through an Ethernet physical interface.



I. Requirements

To carry multiple users on a network device, isolate management, simplify operation and maintenance, and isolate services, a network device with good performance is virtualized to multiple logical devices, making full use of device resources and ensuring strong scalability of the network. Services of virtual devices are managed independently of each other.

II. Network Topology



III. Configuration Tips

Install a VSD license.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# license install usb0:/LIC-VSD00000002328406.lic----> VSD function need license
Success to install license file, service name: LIC-N18000-VSD.
```

Create VSD A.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vsd VSDA
Ruijie(config-vsd)# allocate int gi 1/1
Moving ports will cause all config associated to them in source vsd to be removed. Are you sure
to move the ports? [yes] yes
Entire port-group is not present in the command. Missing ports will be included automatically
Ruijie(config-vsd)#
```

Create VSD B.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vsd VSDB
Ruijie(config-vsd)# allocate int gi 2/1
Moving ports will cause all config associated to them in source vsd to be removed. Are you sure
to move the ports? [yes] yes
```

Entire port-group is not present in the command. Missing ports will be included automatically
 Ruijie(config-vsd)#

Create VSD C.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vsd VSDC
Ruijie(config-vsd)# allocate int gi 3/1
Moving ports will cause all config associated to them in source vsd to be removed. Are you sure
to move the ports? [yes] yes
Entire port-group is not present in the command. Missing ports will be included automatically
Ruijie(config-vsd)#
Manage VSDs.
Configure VSD functions based on actual service planning requirements. (Omitted)
```

IV. Configuration Steps

Install a VSD license.

Create VSD A.

V. Verification

View division details of line cards on the VSD interface.

```
Ruijie-N18K#show vsd all
vsd_id: 0
vsd_name: Ruijie
vsd mac address: 00d0.f876.9888
interface:
interface:
GigabitEthernet 4/1          GigabitEthernet 4/2
GigabitEthernet 4/3          GigabitEthernet 4/4
GigabitEthernet 4/5          GigabitEthernet 4/6
GigabitEthernet 4/7          GigabitEthernet 4/8
GigabitEthernet 4/9          GigabitEthernet 4/10
GigabitEthernet 4/11         GigabitEthernet 4/12
GigabitEthernet 4/13         GigabitEthernet 4/14
GigabitEthernet 4/15         GigabitEthernet 4/16
GigabitEthernet 4/17         GigabitEthernet 4/18
GigabitEthernet 4/19         GigabitEthernet 4/20
GigabitEthernet 4/21         GigabitEthernet 4/22
GigabitEthernet 4/23         GigabitEthernet 4/24
GigabitEthernet 4/25         GigabitEthernet 4/26
```

| | |
|---------------------------------|----------------------|
| GigabitEthernet 4/27 | GigabitEthernet 4/28 |
| GigabitEthernet 4/29 | GigabitEthernet 4/30 |
| GigabitEthernet 4/31 | GigabitEthernet 4/32 |
| GigabitEthernet 4/33 | GigabitEthernet 4/34 |
| GigabitEthernet 4/35 | GigabitEthernet 4/36 |
| GigabitEthernet 4/37 | GigabitEthernet 4/38 |
| GigabitEthernet 4/39 | GigabitEthernet 4/40 |
| GigabitEthernet 4/41 | GigabitEthernet 4/42 |
| GigabitEthernet 4/43 | GigabitEthernet 4/44 |
| GigabitEthernet 4/45 | GigabitEthernet 4/46 |
| GigabitEthernet 4/47 | GigabitEthernet 4/48 |
| slot: | |
| slot 4 | |
| vsd_id: 1 | |
| vsd_name: VSDA | |
| vsd mac address: 00d0.f876.988a | |
| interface: | |
| GigabitEthernet 1/1 | GigabitEthernet 1/2 |
| GigabitEthernet 1/3 | GigabitEthernet 1/4 |
| GigabitEthernet 1/5 | GigabitEthernet 1/6 |
| GigabitEthernet 1/7 | GigabitEthernet 1/8 |
| GigabitEthernet 1/9 | GigabitEthernet 1/10 |
| GigabitEthernet 1/11 | GigabitEthernet 1/12 |
| GigabitEthernet 1/13 | GigabitEthernet 1/14 |
| GigabitEthernet 1/15 | GigabitEthernet 1/16 |
| GigabitEthernet 1/17 | GigabitEthernet 1/18 |
| GigabitEthernet 1/19 | GigabitEthernet 1/20 |
| GigabitEthernet 1/21 | GigabitEthernet 1/22 |
| GigabitEthernet 1/23 | GigabitEthernet 1/24 |
| GigabitEthernet 1/25 | GigabitEthernet 1/26 |
| GigabitEthernet 1/27 | GigabitEthernet 1/28 |
| GigabitEthernet 1/29 | GigabitEthernet 1/30 |
| GigabitEthernet 1/31 | GigabitEthernet 1/32 |
| GigabitEthernet 1/33 | GigabitEthernet 1/34 |
| GigabitEthernet 1/35 | GigabitEthernet 1/36 |
| GigabitEthernet 1/37 | GigabitEthernet 1/38 |
| GigabitEthernet 1/39 | GigabitEthernet 1/40 |
| GigabitEthernet 1/41 | GigabitEthernet 1/42 |
| GigabitEthernet 1/43 | GigabitEthernet 1/44 |
| GigabitEthernet 1/45 | GigabitEthernet 1/46 |
| GigabitEthernet 1/47 | GigabitEthernet 1/48 |

slot:

slot 1

vsd_id: 2

vsd_name: VSDB

vsd mac address: 00d0.f876.988c

interface:

| | |
|----------------------|----------------------|
| GigabitEthernet 2/1 | GigabitEthernet 2/2 |
| GigabitEthernet 2/3 | GigabitEthernet 2/4 |
| GigabitEthernet 2/5 | GigabitEthernet 2/6 |
| GigabitEthernet 2/7 | GigabitEthernet 2/8 |
| GigabitEthernet 2/9 | GigabitEthernet 2/10 |
| GigabitEthernet 2/11 | GigabitEthernet 2/12 |
| GigabitEthernet 2/13 | GigabitEthernet 2/14 |
| GigabitEthernet 2/15 | GigabitEthernet 2/16 |
| GigabitEthernet 2/17 | GigabitEthernet 2/18 |
| GigabitEthernet 2/19 | GigabitEthernet 2/20 |
| GigabitEthernet 2/21 | GigabitEthernet 2/22 |
| GigabitEthernet 2/23 | GigabitEthernet 2/24 |
| GigabitEthernet 2/25 | GigabitEthernet 2/26 |
| GigabitEthernet 2/27 | GigabitEthernet 2/28 |
| GigabitEthernet 2/29 | GigabitEthernet 2/30 |
| GigabitEthernet 2/31 | GigabitEthernet 2/32 |
| GigabitEthernet 2/33 | GigabitEthernet 2/34 |
| GigabitEthernet 2/35 | GigabitEthernet 2/36 |
| GigabitEthernet 2/37 | GigabitEthernet 2/38 |
| GigabitEthernet 2/39 | GigabitEthernet 2/40 |
| GigabitEthernet 2/41 | GigabitEthernet 2/42 |
| GigabitEthernet 2/43 | GigabitEthernet 2/44 |
| GigabitEthernet 2/45 | GigabitEthernet 2/46 |
| GigabitEthernet 2/47 | GigabitEthernet 2/48 |

slot:

slot 2

vsd_id: 3

vsd_name: VSDC

vsd mac address: 00d0.f876.988d

interface:

| | |
|---------------------|----------------------|
| GigabitEthernet 3/1 | GigabitEthernet 3/2 |
| GigabitEthernet 3/3 | GigabitEthernet 3/4 |
| GigabitEthernet 3/5 | GigabitEthernet 3/6 |
| GigabitEthernet 3/7 | GigabitEthernet 3/8 |
| GigabitEthernet 3/9 | GigabitEthernet 3/10 |

| | |
|----------------------|----------------------|
| GigabitEthernet 3/11 | GigabitEthernet 3/12 |
| GigabitEthernet 3/13 | GigabitEthernet 3/14 |
| GigabitEthernet 3/15 | GigabitEthernet 3/16 |
| GigabitEthernet 3/17 | GigabitEthernet 3/18 |
| GigabitEthernet 3/19 | GigabitEthernet 3/20 |
| GigabitEthernet 3/21 | GigabitEthernet 3/22 |
| GigabitEthernet 3/23 | GigabitEthernet 3/24 |
| GigabitEthernet 3/25 | GigabitEthernet 3/26 |
| GigabitEthernet 3/27 | GigabitEthernet 3/28 |
| GigabitEthernet 3/29 | GigabitEthernet 3/30 |
| GigabitEthernet 3/31 | GigabitEthernet 3/32 |
| GigabitEthernet 3/33 | GigabitEthernet 3/34 |
| GigabitEthernet 3/35 | GigabitEthernet 3/36 |
| GigabitEthernet 3/37 | GigabitEthernet 3/38 |
| GigabitEthernet 3/39 | GigabitEthernet 3/40 |
| GigabitEthernet 3/41 | GigabitEthernet 3/42 |
| GigabitEthernet 3/43 | GigabitEthernet 3/44 |
| GigabitEthernet 3/45 | GigabitEthernet 3/46 |
| GigabitEthernet 3/47 | GigabitEthernet 3/48 |
| slot: | |
| slot 3 | |

Verify VSD login and management modes.

```

Ruijie# switchto vsd VSDA
*****

Ruijie General Operating System Software
Copyright (c) 1998-2013s by Ruijie Networks.
All Rights Reserved.
Neither Decompiling Nor Reverse Engineering Shall Be Allowed.
*****

Ruijie-VSDA> enable
Ruijie-VSDA#conf
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie-VSDA(config)#int mgmt 0
Ruijie-VSDA(config-if-Mgmt 0)#ip address 10.1.1.10 255.255.255.0
Ruijie-VSDA(config-if-Mgmt 0)#end
Ruijie-VSDA#switchback

Ruijie# switchto vsd VSDB
*****

```

```
Ruijie General Operating System Software
Copyright (c) 1998-2013s by Ruijie Networks.
All Rights Reserved.
Neither Decompiling Nor Reverse Engineering Shall Be Allowed.
*****

Ruijie-VSDB> enable
Ruijie-VSDB#conf
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie-VSDB(config)#int mgm
Ruijie-VSDB(config)#int mgmt 0
Ruijie-VSDB(config-if-Mgmt 0)#ip address 10.1.1.20 255.255.255.0
Ruijie-VSDB(config-if-Mgmt 0)#end
Ruijie-VSDB#switchback

Ruijie# switchto vsd VSDC
*****

Ruijie General Operating System Software
Copyright (c) 1998-2013s by Ruijie Networks.
All Rights Reserved.
Neither Decompiling Nor Reverse Engineering Shall Be Allowed.
*****

Ruijie-VSDC> enable
Ruijie-VSDC#conf
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie-VSDC(config)#int mgm
Ruijie-VSDC(config)#int mgmt 0
Ruijie-VSDC(config-if-Mgmt 0)#ip address 10.1.1.30 255.255.255.0
Ruijie-VSDC(config-if-Mgmt 0)#end
Ruijie-VSDC#switchback
```

2.9 Common Feature

2.9.1 Ethernet Switching

2.9.1.1 Voice VLAN

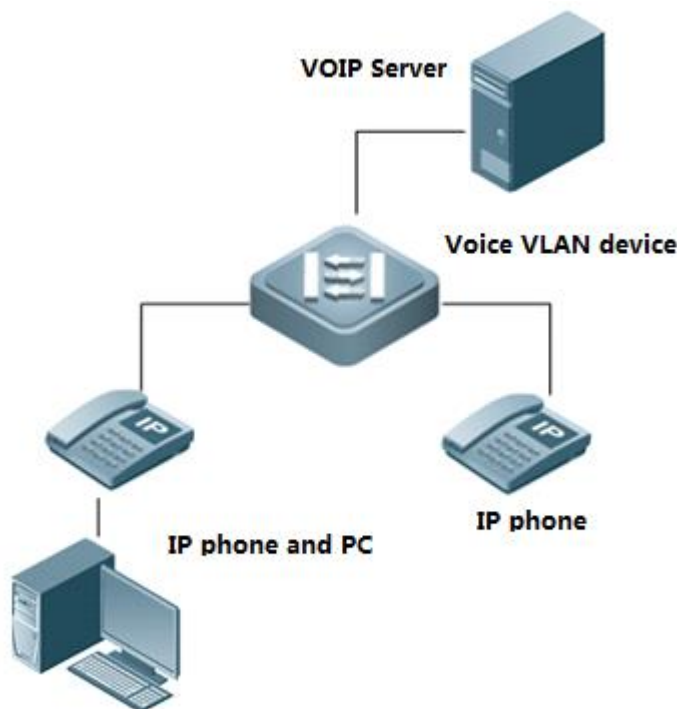
2.9.1.1.1 Introduction

Scenario

With the continual development of technology, IP phone is being used more and more widely. It converts analog signals into digital signals which are transmitted over the IP network to the receiver. Then, upon the receipt of data packets, the receiver converts digital signals back to the analog signals. Combined other voice devices, IP phone offers high capacity and low cost voice communications solution for users.

Voice VLAN is specially designed for voice streams. By creating a voice VLAN and adding the ports connecting voice devices to the voice VLAN, users can centrally transmit voice streams in the voice VLAN, and configure QoS specific for voice streams to improve the priority of voice stream transmission and ensure voice quality.

Following figure displays the basic networking of Voice VLAN:



There are usually two types of connection (see Figure above) between IP phones and Voice VLAN:

1. IP phones separately access to Voice VLAN with only voice streams transmitted. This type of connection is usually applied to IP phones arrangement in meeting rooms or occasions where PC is not necessary for data processing.
2. PC and IP phones form a daisy chain to access the network with voice and data streams transmitted. In this case, voice streams and data streams are transmitted in voice VLAN and data VLAN respectively. Generally, this type of connection is applied when office clerks need to conduct both data communication with PC and voice communication with IP phones.

Voice VLAN-enabled device determines whether the packet is the voice stream to the specific voice device by matching the source MAC address of incoming packet with the OUI (Organizationally Unique Identifier) of the voice device. If so, the packet is partitioned into the voice VLAN for transmission.

Auto mode and manual mode of Voice VLAN

A port can work in the auto mode or manual mode of voice VLAN with different join methods.

- 1) Auto mode: When a subscriber runs an IP phone and sends protocol packet through a voice VLAN-enabled equipment, the equipment identifies the source MAC address of protocol packet and matches the MAC address with the OUI address set on the switch. If succeed, the equipment will automatically add the input port of the voice message to Voice VLAN and issue the policy to modify the priority of voice message as the one voice stream of voice VLAN configured on the equipment. Meanwhile, the subscriber may set Voice VLAN aging time on the equipment. When no voice message is received from the input port within the aging time, the system will delete the port from Voice VLAN. Adding or deleting a port to or from voice VLAN is automatically executed by the system. Port aging mechanism may prevent the speech equipment port out of use for a long time from remaining in Voice VLAN.
- 2) Manual mode: Users manually add the IP phone connected port to the voice VLAN on voice VLAN supported Equipment. In the course IP phone communication, the equipment identifies the source MAC Address of data packet and matches the MAC address with the OUI address of the configured voice VLAN. If succeed, the equipment will automatically add the input port of the voice message to Voice VLAN and issue the policy to modify the priority of voice message as the one voice stream of voice VLAN configured on the equipment. In manual mode, adding or deleting a port to or from voice VLAN is done by administrators manually.

Auto mode is better for PC--IP phone framework that transmit voice data and pc data at the same time.

Manual mode is better for only IP phone framework that transmit voice data only.

The way Voice VLAN and IP phone works

Generally speaking, there are two kinds of IP phones by the way to obtain IP address and voice VLAN message.

- 1) Automatically acquire IP address and Voice VLAN numbers. This kind of IP phones sends tagged or untagged voice streams.
- 2) Manually configure IP addresses and Voice VLAN numbers. This kind of IP phones can only send tagged voice streams.

IP phone working principle

The same to other network device, IP phone need an IP address to work in network. There're 2 ways to acquire IP address:

- 1) DHCP automatically
- 2) Configuration manually

When request IP address from DHCP Server automatically, IP phone request for Voice VLAN info at the same time. IP phone begin to send voice stream with Voice VLAN tag once DHCP Server return Voice VLAN info and send voice stream without Voice VLAN tag if DHCP doesn't return Voice VLAN info.

If user set IP phone IP address and Voice VLAN info manually, IP phone may send voice stream with tagged or untagged based on the manual configuration.

Matching relationship between port mode and voice stream type

| Voice VLAN working mode | Voice stream type | Port type | Support |
|-------------------------|-----------------------|------------------------------------|--|
| Auto mode | Tagged voice stream | Access Port | No |
| | | Private VLAN host-port interface | No |
| | | Private VLAN hybrid-port interface | No |
| | | Trunk Port | Yes, native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the port allows native VLAN passing. |
| | | Hybrid Port | Yes, native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the port allows native VLAN passing. |
| | | Uplink Interface | Yes, native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the port allows native VLAN passing. |
| | Untagged voice stream | Access Port | No |
| | | Private VLAN host-port interface | No |
| | | Private VLAN hybrid-port interface | No |
| | | Trunk Port | No |
| | | Hybrid Port | No |
| | | Uplink interface | No |
| Manual mode | Tagged voice stream | Access Port | No |

| | | | |
|--|-----------------------|------------------------------------|--|
| | | Private VLAN host-port interface | No |
| | | Private VLAN hybrid-port interface | No |
| | | Trunk Port | Yes, Native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the access port allows native VLAN and Voice VLAN passing |
| | | Hybrid Port | Yes, Native VLAN of the access port must not be Voice VLAN. Meanwhile, the port allows native VLAN passing, and the Voice VLAN should be in the list of tagged VLANs whose passing is allowed by the port. |
| | | Uplink interface | Yes, Native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the access port allows native VLAN and Voice VLAN passing. |
| | Untagged voice stream | Access Port | Yes, Voice VLAN must be consistent with the VLAN which the access port belongs to. |
| | | Private VLAN host-port interface | Yes, Voice VLAN must be configured to be Isolated VLAN or Community VLAN corresponding to the port. |
| | | Private VLAN hybrid-port interface | Yes, Voice VLAN must be configured to be Primary VLAN. |
| | | Trunk Port | Yes, Native VLAN of the access port must be Voice VLAN and the access port allows the VLAN passing. |
| | | Hybrid Port | Yes, Native VLAN of the access port must be Voice VLAN and be in the list of untagged VLANs whose passing is allowed by the access port. |
| | | Uplink interface | No |

Voice VLAN safe mode

Safe mode is available for separate transmission of voice streams and data streams. When safe mode is enabled, Voice VLAN only permits voice stream transmission. Only the streams whose source MAC address matches the OUI address of voice VLAN are allowed to transmit in voice VLAN, others are dropped. When safe mode is disabled, the source MAC address of streams will not be checked, and all streams will be permitted to transmit within Voice VLAN.

Voice VLAN Working Principles

By transmitting data streams and voice streams in the data VLAN and the voice VLAN respectively, the voice VLAN-supported equipment avoids mutual influence between them. Meanwhile, the equipment issues priority policy to improve the priority of voice streams and guarantee session quality. The basic working principle is described as below:

Step 1: The user creates on the equipment one VLAN dedicated to transmitting voice packets, i.e., Voice VLAN, and enables Voice VLAN function on the port that connects with IP phone.

Step 2: As a key step, the port that connects with IP phone joins Voice VLAN in different ways by the working mode of Voice VLAN:

Under auto mode, after receiving untagged message from the port, the equipment will match its source MAC address with legal OUI address. If the source MAC is OUI address, the message will be considered to be voice message. And the equipment will automatically join the port in Voice VLAN, and learn this MAC address on the port at the same time.

Under manual mode, subscribers should manually configure the port which connects with IP phones to join Voice VLAN.

Step 3: Whether under auto mode or manual mode, the equipment will issue a policy and improve the priority of packets whose source MAC address matches the OUI address of voice VLAN. The CoS is set to 6 and DSCP is set to 46 for matched voice packets. Following these steps, the port that connects with IP phone joins Voice VLAN, and voice packets will be centrally transmitted in Voice VLAN and forwarded out with high priority.

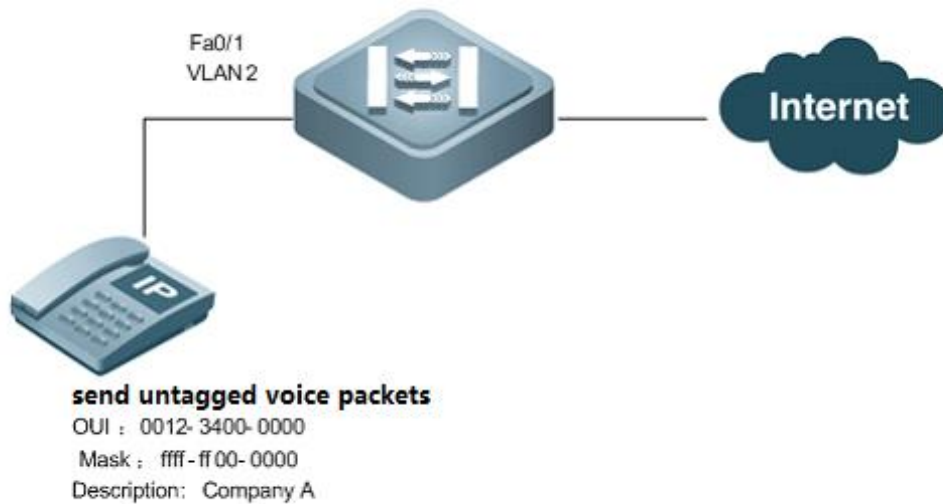
If IP phone supports LLDP, user doesn't need to configure OUI manually. Switch could recognize and identify IP phone by the LLDP packets sending from IP phone.

2.9.1.1.2 Single IP phone with untagged traffic

I. Requirements

1. Vlan 2 is Voice Vlan which only carries voice traffic. Vlan 3 is Data Vlan which carries other traffic
2. The MAC address of IP phone is 0012.3456.7890 and OUI address is 0012.3400.0000. The IP phone acquires IP address from DHCP Server and sends **untagged** voice traffic to the network.

II. Network Topology



III. Configuration Tips

When port F0/1 works in Voice Vlan auto mode , it doesn't forward untagged voice traffic,so you must convert it to manual mode and configure F0/1 as Hybrid port.Native Vlan must be the same to Voice Vlan, and switch shall forward untagged traffic of Voice Vlan on F0/1.

IV. Configuration Steps

1. Create Vlan 2 and configure Vlan 2 as Voice VLAN

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

2. Allow switch to forward Voice traffic, which OUI address is "0012.3400.0000", mask is "ffff.ff00.0000" and description is Company , on Voice Vlan

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
```

3. Configure port Fa0/1 as a Hybrid port and specify Vlan 2 to be the native Vlan

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode hybrid ---->configure Fa0/1 as a Hybrid Port
Ruijie(config-if)# switchport hybrid native vlan 2 ---->specify Voice VLAN 2 to be the native VLAN
```

```
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 2 ---->allow this port to forward untagged traffic of Vlan 2
```

4. Enable Voice VLAN on Fa0/1 and convert working mode of Voice Vlan to Manul mode.By default , the working mode is auto

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# no voice vlan mode auto
Ruijie(config-if)# voice vlan enable
```

5. Configure uplink port as Trunk port

```
Ruijie(config)# interface fastEthernet 0/24
Ruijie(config-if)# switchport mode trunk
```

V. Verification

How to display status of Voice VLAN

```
Ruijie(config)# show voice vlan
Voice Vlan status: ENABLE
Voice Vlan ID      : 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440minutes
Voice Vlan cos      : 6
Voice Vlan dscp      : 46
Current voice vlan enabled port mode:
PORT                MODE
-----
Fa0/1                MANUAL
```

How to display Voice VLAN OUI address

```
Ruijie(config)# show voice vlan oui
```

| Oui Address | Mask | Description | Status |
|----------------|----------------|-------------|--------|
| 0012.3400.0000 | ffff.ff00.0000 | Company A | static |

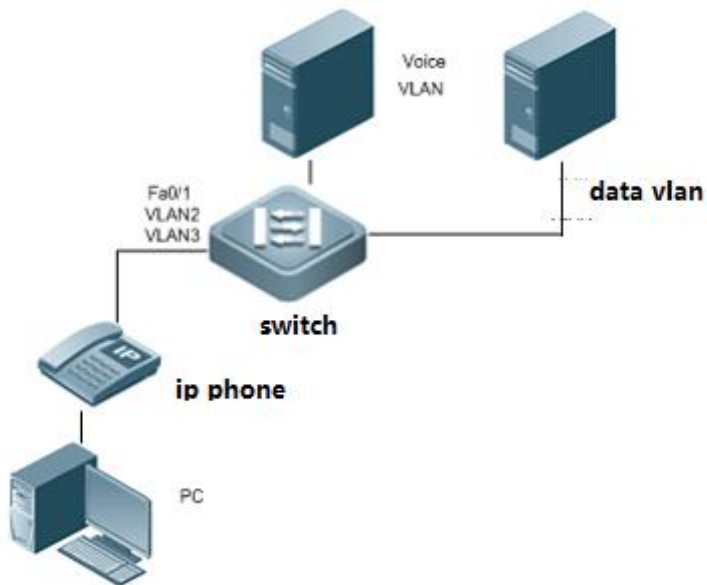
2.9.1.1.3 IP phone sends untagged traffic and connects to PC on downlink

I. Requirements

1. Vlan 2 is Voice Vlan. Vlan 3 is Data Vlan.Switch forwards Voicd traffic on Vlan 2 only and forwards other traffic on VLAN 3.

2. The MAC address of IP phone is 0012.3456.7890 and OUI address is 0012.3400.0000 . Both IP phone and station acquire IP address from DHCP Server and sends untagged traffic to the network.

II. Network Topology



III. Configuration Tips

1. Set Fa0/1 to Hybrid port. **Native VLAN 3 is for pc data and Voice VLAN 2 is for voice data.**
2. Set Voice VLAN in manual mode because both PC and IP phone send untagged packets .Meanwhile, activate MAC VLAN to guide voice flow into Voice VLAN. Then add VLAN 2 and 3 to untagged list to make sure both direction flows are untagged.

IV. Configuration Steps

1. Create Voice VLAN and Data VLAN

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan 3
Ruijie(config-vlan)# exit
#Create Voice VLAN
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

2. Allow switch to forward Voice traffic , which OUI address is "0012.3400.0000" , mask is "ffff.ff00.0000" and description is Company , on Voice Vlan

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
```

3. Configure port Fa0/1 as a Hybrid port and specify Vlan 3 to be the native Vlan

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode hybrid ----->configure Fa0/1 as Hybrid port
Ruijie(config-if)# switchport hybrid native vlan 3 ----->specify Vlan 3 to be native vlan
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 2-3 ----->allow this port to forward untagged traffic of
Vlan 2 and 3
```

4. Configure MAC-VLAN to guide voice data into Voice VLAN 2 and disable voice security

```
Ruijie(config)# mac-vlan mac-address 0012.3456.7890 mask ffff.ffff.ffff vlan 2
Ruijie(config)# no voice vlan security enable
```

5. Enable Voice Vlan and Mac Vlan on Fa0/1 and convert working mode of Voice Vlan to Manul mode. And enable mac-vlan for this interface.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# no voice vlan mode auto
Ruijie(config-if)# voice vlan enable
Ruijie(config-if)# mac-vlan enable
```

V. Verification

How to display status of Voice VLAN

```
Ruijie(config)# show voice vlan
Voice Vlan status: ENABLE
Voice Vlan ID      : 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440minutes
Voice Vlan cos      : 6
Voice Vlan dscp      : 46
Current voice vlan enabled port mode:
PORT              MODE
-----
Fa0/1              MANUAL
```

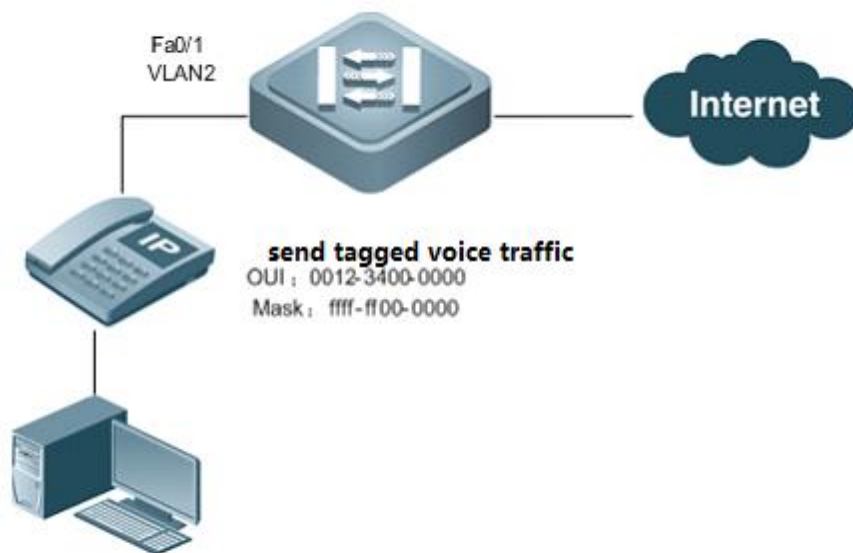
2.9.1.1.4 IP phone sends tagged traffic and connects to PC on downlink

I. Requirements

1. Vlan 2 is Voice Vlan which aging time is 1000 minutes and only carries Voice traffic
2. The MAC address of IP phone is 0012.3456.7890 and OUI address is 0012.3400.0000 . Both IP phone and PC acquire IP address from DHCP Server and IP phone sends tagged voice traffic and PC sends untagged traffic to the network.
3. 802.1X authentication is enabled on F0/1 (optional)

Notes: IP Phone sends untagged traffic by default. For tagged vlan, it's configured on IP Phone manually or obtain specific DHCP option from DHCP server. (For more details, please refer IP Phone user guide or connect IP Phone technical engineer)

II. Network Topology



III. Configuration Tips

1. Configure F0/1 as hybrid port and Voice Vlan forwards voice traffic and Native Vlan forwards other traffic.
2. Configure global security tunnel to allow voice traffic pass through F0/1 without 802.1X authentication
3. Convert Voice Vlan working mode of F0/1 to manual mode.

IV. Configuration Steps

1. Create VLAN 2 as voice VLAN and VLAN 5 as data VLAN

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

```
Ruijie(config)# vlan 5
```

2. Set Voice VLAN aging time to 1000 minutes and disable voice vlan security

```
Ruijie(config)# voice vlan aging 1000  
Ruijie(config)# no voice vlan security enable
```

3. Allow switch to forward Voice traffic , which OUI address is "0012.3400.0000" , mask is "ffff.ff00.0000"

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
```

4. Configure MAC-VLAN to guide voice data into Voice VLAN 2

```
Ruijie(config-if)# mac-vlan mac-address 0012.3456.7890 mask ffff.ffff.ffff vlan 2
```

5. Configure port Fa0/1 as a hybrid port and specify Vlan 5 to be the native Vlan

```
Ruijie(config)# interface fastEthernet 0/1  
Ruijie(config-if)# switchport mode hybrid ---->configure Fa0/1 as hybrid Port  
Ruijie(config-if)# switchport hybrid native vlan 5---->specify Vlan 5 to be native VLAN  
Ruijie(config-if)# switchport hybrid allowed vlan add tagged 2 ----> allow VLAN 2 voice traffic with tag passthrough
```

6. Switch the voice working mode to manual and enable Voice VLAN and mac-vlan on fastEthernet 0/1.

```
Ruijie(config)# interface fastEthernet 0/1  
Ruijie(config-if)# no voice vlan mode auto  
Ruijie(config-if)# voice vlan enable  
Ruijie(config-if)# mac-vlan enable
```

7. Enable 802.1X authentication on F0/1 (optional)

```
Ruijie(config)# interface fastEthernet 0/1  
Ruijie(config-if)# dot1x port-control auto
```

For complete information about 802.1x configuration ,see switch configuration guide , such as 《RG-S8600E Series Switches RGOS Configuration Guide》

If you enable Guest Vlan feature , you must assign different Vlan ID to Voice Vlan , Guest Vlan and native Vlan independently

8. Configure global security tunnel to allow voice traffic pass through F0/1 without 802.1X authentication

```
Ruijie(config)# expert access-list extended safe_channel ---->define Expert ACL named "safe_channel"
```

```
Ruijie(config-exp-nacl)# permit etype-any 0012.3400.0000 0000.00ff.ffff any ---->permit source host
0012.3400.0000 (OUI address of IP phone)to any destination host
Ruijie(config)# security global access-group safe_channel ---->enable security tunnel feature globally
```

V. Verification

How to display status of Voice VLAN

```
Ruijie(config)# show voice vlan
Voice Vlan status: ENABLE
Voice Vlan ID      : 2
Voice Vlan security mode: Normal
Voice Vlan aging time: 1000minutes
Voice Vlan cos      : 6
Voice Vlan dscp      : 46
Current voice vlan enabled port mode:
PORT              MODE
-----
Fa0/1              MANUAL
```

How to display OUI address on Voice Vlan

```
Ruijie(config)# show voice vlan oui
```

| Oui Address | Mask | Description | Status |
|----------------|----------------|-------------|--------|
| 0012.3400.0000 | ffff.ff00.0000 | Company A | static |

2.9.1.2 Aggregate Port

Scenario

Multiple physical links can be bound into a logical link, called an aggregate port (herein after referred to as AP). Ruijie devices provide the AP function that complies with the IEEE802.3ad standard. This function can be used to expand link bandwidth and improve reliability. AP function supports traffic balancing that evenly allocating the traffic to every member link. AP function also supports link backup. When a link member in an AP is disconnected, the system will automatically allocate the traffic of the member link to other active member links in the AP, except for the broadcast or multicast packets it received.

Dynamic mode and Static mode

- 1) If you configure aggregate port mode to static on a port, the port is converted to aggregate port without negotiating.
- 2) If you configure aggregate port mode to dynamic with LACP (Link Aggregation Control Protocol), the port negotiates with the other end of the link whether to be an aggregate port.

Aggregate ports consist of three modes: Active, Passive and Static.

The port in active mode sends the LACP packets actively to the peer

The port in passive mode only responds when it receives LACP packets from the peer.

The port in static mode is converted to aggregate port without sending any LACP packets.

The following table describes the matching of different modes

| Port mode | Neighbor port mode |
|--------------|-------------------------|
| Active mode | Active or passive mode. |
| Passive mode | Active mode |
| Static mode | Static mode. |

Aggregate Port Load Balancing

Traffic can be evenly distributed on the member links of an AP according to the features such as source MAC address, destination MAC address, combination of source MAC address and destination MAC address, source IP address, destination IP address, and combination of source IP address and destination IP address.

Note: By default , the load balancing method is src-dst-mac.

This example shows how to configure load balance:

```
Ruijie(config)#aggregateport load-balance ?
dst-ip          Destination IP address
dst-mac         Destination MAC address
help           Help information
mpls-label      Mpls label
src-dst-ip      Source and destination IP address
src-dst-ip-l4port Source and destination IP address, source and
                destination L4port
src-dst-mac     Source and destination MAC address
src-ip         Source IP address
src-mac        Source MAC address
src-port       Source port
Ruijie(config)#aggregateport load-balance  src-dst-ip ----->recommended
```

Attention:

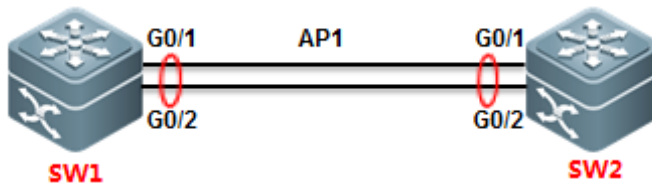
1. You must configure the same speed,duplex and media-type on both ends of AP.You cannot put a copper port and a optical port in the same AP.
2. You can only put L2 port in a L2 AP and L3 port in a L3 AP. You cannot change the port from L2 to L3 , or from L3 to L2 after you put the ports in a AP.
3. Ruijie switch supports to put 8 ports in a AP at most
5. When you finish configuring AP , you can enter "interface aggregateport x/x" command to manage the AP.You can no longer manage the AP member independently.

Layer 2 Aggregate Port (Static and Dynamic)

I. Requirements

Enable Layer 2 AP on the ports between two Core switches to expand inter-connection bandwidth and ensure a high available network. Use src-mac load balance method.

II. Network Topology



III. Configuration Tips

1. Put AP members ports in a specified AP
2. Configure AP as Trunk
3. Modify load balance method

IV. Configuration Steps

Static mode:

SW1:

```
SW1>enable
SW1#configure terminal
SW1(config)#interface range gigabitEthernet 0/1-2      ----->configure a range of interfaces with the same
command
SW1(config-if-range)#port-group 1                      ----->put G0/1 and G0/2 in AP 1 in static mode
SW1(config-if-range)#exit
SW1(config)#interface aggregateport 1
SW1(config-if-AggregatePort 1)#switchport mode trunk  ----->configure AP 1 as Trunk
SW1(config-if-AggregatePort 1)#exit
SW1(config)#aggregateport load-balance src-mac          ----->modify load balance method to Src-MAC. By
default, it is Src-Dst-MAC.
SW1(config)#exit
SW1#wr
```

SW2:

```
SW2>enable
```

```
SW2#configure terminal
SW2(config)#interface range gigabitEthernet 0/1-2
SW2(config-if-range)#port-group 1
SW2(config-if-range)#exit
SW2(config)#interface aggregateport 1
SW2(config-if-AggregatePort 1)#switchport mode trunk
SW2(config-if-AggregatePort 1)#exit
SW2(config)#aggregateport load-balance src-mac
SW2(config)#exit
SW2#wr
```

Dynamic mode:

```
SW1(config)#interface range gigabitEthernet 0/1-2
SW1(config-if-range)#port-group 1 mode active           ----->put G0/1 and G0/2 in AP 1 in
dynamic mode
SW1(config-if-range)#exit
SW1(config)#interface aggregateport 1
SW1(config-if-AggregatePort 1)#switchport mode trunk   ----->configure AP 1 as Trunk
SW1(config-if-AggregatePort 1)#exit
SW2 is the same.
```

3. This example shows how to configure L2 AP in **static mode** when connect Ruijie a switch to a Cisco switch

Cisco:

```
interface Port-channel1
switchport mode access
interface FastEthernet0/1
switchport mode access
channel-group 1 mode on
interface FastEthernet0/2
switchport mode access
channel-group 1 mode on
```

Ruijie :

```
interface AggregatePort 1
interface FastEthernet 0/1
port-group 1
interface FastEthernet 0/2
port-group 1
```

4. This example shows how to configure L2 AP in **dynamic mode** when connect Ruijie a switch to a Cisco switch

Cisco:

```

interface Port-channel1
switchport mode access
interface FastEthernet0/1
switchport mode access
channel-group 1 mode active
interface FastEthernet0/2
switchport mode access
channel-group 1 mode active

```

Ruijie :

```

interface FastEthernet 0/1
port-group 1 mode active
interface FastEthernet 0/2
port-group 1 mode active
interface AggregatePort 1

```

V. Verification

1. How to display status of aggregate port

```

SW1#show aggregatePort summary
AggregatePort MaxPorts SwitchPort Mode Ports
-----
Ag1           8      Enabled   TRUNK  Gi0/1 ,Gi0/2

```

2. How to display information of AP 1

```

SW1#show interfaces aggregateport 1
Index(dec):25 (hex):19
AggregatePort 1 is UP , line protocol is UP
Hardware is Aggregate Link AggregatePort
Interface address is: no ip address
MTU 1500 bytes, BW 2000000 Kbit
Encapsulation protocol is Bridge, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec

```

3. How to display the load balance method

```

SW1#show aggregatePort load-balance
Load-balance : Source MAC
SW1#

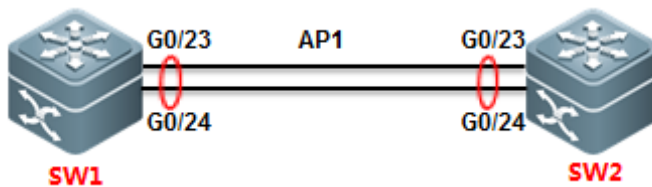
```

Layer 3 Aggregate Port (Static and Dynamic)

I. Requirements

Enable Layer 3 AP on the ports between two Core switches to expand inter-connection bandwidth and ensure a high available network. Use src-dst-IP load balance method.

II. Network Topology



III. Configuration Tips

1. First, you must create a AP and convert it to a L3 AP, then assign a IP address to it.
2. Convert AP members to L3 ports.
3. Put the AP members in the AP
4. Modify load balance method

Note: You must follow the tips above step by step ,otherwise you could fail to configure L3 AP.

IV. Configuration Steps

SW1:

```
SW1>enable
SW1#configure terminal
SW1(config)#interface aggregateport 1
SW1(config-if-AggregatePort 1)#no switchport          ----->convert AP 1 from L2
to L3
SW1(config-if-AggregatePort 1)#ip address 1.1.1.1 255.255.255.0
SW1(config-if-AggregatePort 1)#exit
SW1(config)#interface range gigabitEthernet 0/23-24    ----->configure a range of
interfaces with the same commands
SW1(config-if-range)#no switchport                    ----->convert AP
members to layer 3
SW1(config-if-range)#medium-type fiber
SW1(config-if-range)#port-group 1 mode active          ----->put G0/23 and G0/24 in
AP 1 in active mode
SW1(config-if-range)#exit
SW1(config)#aggregateport load-balance src-dst-ip      ----->put G0/23 and G0/24 in AP 1 in
active mode
```

```

-----
or
SW1(config-if-range)#port-group 1
G0/24 in AP 1 in static mode
SW1(config-if-range)#end
----->put G0/23 and

```

SW2:

```

SW2>enable
SW2#configure terminal
SW2(config)#interface aggregateport 1
SW2(config-if-AggregatePort 1)#no switchport
SW2(config-if-AggregatePort 1)#ip address 1.1.1.2 255.255.255.0
SW2(config-if-AggregatePort 1)#exit
SW2(config)#interface range gigabitEthernet 0/23-24
SW2(config-if-range)#no switchport
SW2(config-if-range)#medium-type fiber
SW2(config-if-range)#port-group 1 mode active
SW2(config-if-range)#end
SW2(config)#aggregateport load-balance src-dst-ip

-----
or
SW2(config-if-range)#port-group 1
SW2(config-if-range)#end

```

V. Verification

1. When both ends negotiate to join a AP successfully, system returns the following message:

```

*Dec 17 13:23:52: %LLDP-4-ERRDETECT: Link aggregation for the port GigabitEthernet 0/23 may not match with
one for the neighbor port.
*Dec 17 13:23:52: %LLDP-4-ERRDETECT: Link aggregation for the port GigabitEthernet 0/24 may not match with
one for the neighbor port.
*Dec 17 13:23:59: %LACP-5-ATTACH: Interface GigabitEthernet 0/23 attached to AggregatePort 1.
*Dec 17 13:23:59: %LACP-5-ATTACH: Interface GigabitEthernet 0/24 attached to AggregatePort 1.
*Dec 17 13:24:00: %LACP-5-BUNDLE: Interface GigabitEthernet 0/23 joined AggregatePort 1.
*Dec 17 13:24:00: %LACP-5-BUNDLE: Interface GigabitEthernet 0/24 joined AggregatePort 1.
*Dec 17 13:24:02: %LINK-3-UPDOWN: Interface AggregatePort 1, changed state to up.
*Dec 17 13:24:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface AggregatePort 1, changed state to up.

```

2. How to display status of all AP

```
SW1#show aggregatePort summary
AggregatePort MaxPorts SwitchPort Mode Ports
-----
Ag1            8          Disable  "Disable" indicates it is a L3 port  Gi0/23 ,Gi0/24 AP members
```

3. How to display information of AP 1

```
SW1#show int aggregateport 1
Index(dec):25 (hex):19
AggregatePort 1 is UP , line protocol is UP
Hardware is Aggregate Link AggregatePort, address is 1414.4b1b.546d (bia
Interface address is: 1.1.1.1/24
ARP type: ARPA, ARP Timeout: 3600 seconds
MTU 1500 bytes, BW 2000000 Kbit
```

2.9.1.3 Super VLAN

Scenario

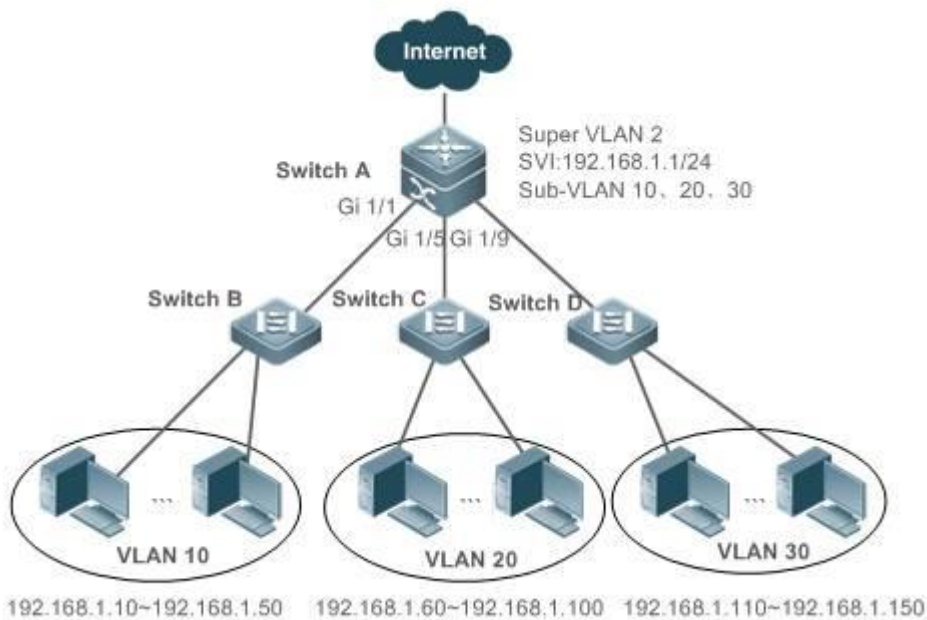
The Super VLAN function economizes IP address resources, segregates broadcast storms, reduces virus attacks, and controls L2 access on the ports. The function is suitable for extensive L2 structure environments with large numbers of users and VLANs and all IP addresses on a same network segment, where L2 segmentation and mutual access between certain VLANs (ARP aging for corresponding sub VLANs) are required. Common application scenarios include broadband access in hotels and residential areas and campus networks run cooperatively by telecom carriers and colleges. In these scenarios, each room or household uses one VLAN, which is segregated from each other. However, due to limited IP address resources, it is impossible to allocate each VLAN with a network segment. A group of VLANs needs to share one network segment. For example, if VLAN 10 is allocated with the network segment 10.10.10.0/24, the household may only use one or two IP addresses, and in this case, over 200 IP addresses are wasted. In addition, unified IP addresses facilitate network management for network maintenance personnel.

The Super VLAN solution is suitable for small- and medium-sized networks that require L2/L3 segmentation. Super VLAN is a function provided by an L3 switch and is implemented on the L3 network. Private VLAN is a function provided by an L2 switch. Compared with Private VLAN, super VLAN features simpler configuration and yet lower access control flexibility. To query temporarily offline users within a Super VLAN, the gateway needs to initiate a broadcast within each sub-VLAN, and the process may consume large CPU resources on the device.

I. Networking Requirements

Core switch A serves as the user gateway and is connected to the access devices Switch B, Switch C, and Switch D through the Trunk ports. L2 network segmentation is implemented through VLAN setup for access users. All VLAN users share one IP gateway for L3 communication and Internet access.

II. Network Topology



III. Configuration Tips

1. On the access devices (Switch B, Switch C, and Switch D), configure only common VLANs (VLAN 10, VLAN 20, and VLAN 30 in this example).
2. On the user gateway device, create a Super VLAN and set the VLAN 10, VLAN 20, and VLAN 30 of the access devices as sub VLANs.
3. Set the SVI port for the Super VLAN and specify IP address ranges for each sub VLAN.

IV. Configuration Steps

On the core server, perform the following steps:

1. Create VLAN 2, VLAN 10, VLAN 20, and VLAN 30.

```
Ruijie#configure terminal
Ruijie(config)#vlan 2
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 20
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 30
Ruijie(config-vlan)#exit
```

2. Set VLAN 2 as the Super VLAN and VLAN 10, VLAN 20, and VLAN 30 as its sub VLANs.

```
Ruijie(config)#vlan 2
Ruijie(config-vlan)#supervlan ----->configure Vlan2 as Super vlan
```

```
Ruijie(config-vlan)#subvlan 10,20,30 -----> SVI port could not be added to subvlan, need to execute command "no
interface vlan vlan-id" to remove SVI port before adding to subvlan )
Ruijie(config-vlan)#exit
```

On a non-simplified network (gateway mode), Super VLAN broadcast packets are replicated to all its sub VLANs. Therefore, if a Super VLAN is configured with too many sub VLANs, the performance is undermined. Considering the packet forwarding performance, it is recommended that a Super VLAN is configured with no more than 200 sub VLANs.

3. **Set the L3 virtual interface for the Super VLAN 2. The users of the sub VLANs of the Super VLAN 2 communicate through the configured interface.**

```
Ruijie(config)#interface vlan 2 ----->configure svi interface
Ruijie(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0
```

4. **Set the IP address range of the sub VLAN 10 to 192.168.1.10 to 192.168.1.50, that of sub VLAN 20 to 192.168.1.60 to 192.168.1.100, and that of sub VLAN 30 to 192.168.1.110 to 192.168.1.150.**

```
Ruijie(config)#vlan 10
Ruijie(config-vlan)#subvlan-address-range 192.168.1.10 192.168.1.50
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 20
Ruijie(config-vlan)#subvlan-address-range 192.168.1.60 192.168.1.100
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 30
Ruijie(config-vlan)#subvlan-address-range 192.168.1.110 192.168.1.150
```

5. **Set the ports Gi 1/1, Gi 1/5, and Gi 1/9 as the Trunk ports for connecting Switch B, Switch C, and Switch D.**

```
Ruijie(config)#interface range gigabitEthernet 1/1,1/5,1/9
Ruijie(config-if-range)#switchport mode trunk
```

6. **Save the configurations.**

```
Ruijie(config-if-range)#end
Ruijie#write
```

Note:

1. **By default, the Super VLAN agent APR function is enabled on the switch.** In this case, users can access each other between sub VLANs. To prevent access between sub VLANs, disable the agent function of the Super VLAN.

```
Ruijie(config)#vlan 2
Ruijie(config-vlan)#no proxy-arp
```

```
Ruijie(config-vlan)#end
```

2. In a DHCP environment, you do not have to specify the IP address range for a sub VLAN.

In this case, the IP addresses are randomly allocated within one sub VLAN. The VLAN of the port connecting the access switch determines the home sub VLAN of a PC.

```
Ruijie(config)#vlan 10
Ruijie(config-vlan)#subvlan-address-range 192.168.1.10 192.168.1.50
Ruijie(config-vlan)#vlan 20
Ruijie(config-vlan)#subvlan-address-range 192.168.1.60 192.168.1.100
Ruijie(config-vlan)#vlan 30
Ruijie(config-vlan)#subvlan-address-range 192.168.1.110 192.168.1.150
```

3. Disable broadcast storm prevention on the connecting port of the access switch.

When a user on another network segment accesses a user in the Super VLAN, if the user device does not exist, the switch sends ARP requests to all sub VLANs of the Super VLAN, as the Super VLAN does not obtain the ARP information during query when resolving the user device ARP before forwarding the IP packet to the designated user device. In this case, If the Super VLAN is configured with many sub VLANs, the Super VLAN has to send a large number of ARP packets.

In a DHCP environment, if there are too many sub VLANs in the Super VLAN, the number of broadcast packets sent on each sub VLAN is great as well, because the broadcast packet is replicated on each sub VLAN.

In this case, if the broadcast storm prevention function is enabled on corresponding port on the access switch, some broadcast packets, including DHCP packets or ARP packets, are discarded. To prevent this, you are recommended to disable the broadcast storm prevention function for the port on the access switch. For details, see [Storm Control](#).

4. A Super VLAN is subject to the following restrictions:

- a. A Super VLAN does not have physical interfaces as its direct member. A Super VLAN is configured with only sub VLANs and a sub VLAN contains physical interfaces.
- b. A Super VLAN cannot be configured as a sub VLAN of another Super VLAN.
- c. VLAN 1 cannot be configured as a Super VLAN.
- d. A sub VLAN cannot be configured as a network interface and cannot be allocated with an IP address.

V. Verification

Check the Super VLAN.

```
Ruijie#show supervlan
supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip range
-----
2              ON10ON192.168.1.10 - 192.168.1.50
20ON192.168.1.60 - 192.168.1.100
              30ON192.168.1.110 - 192.168.1.150
```

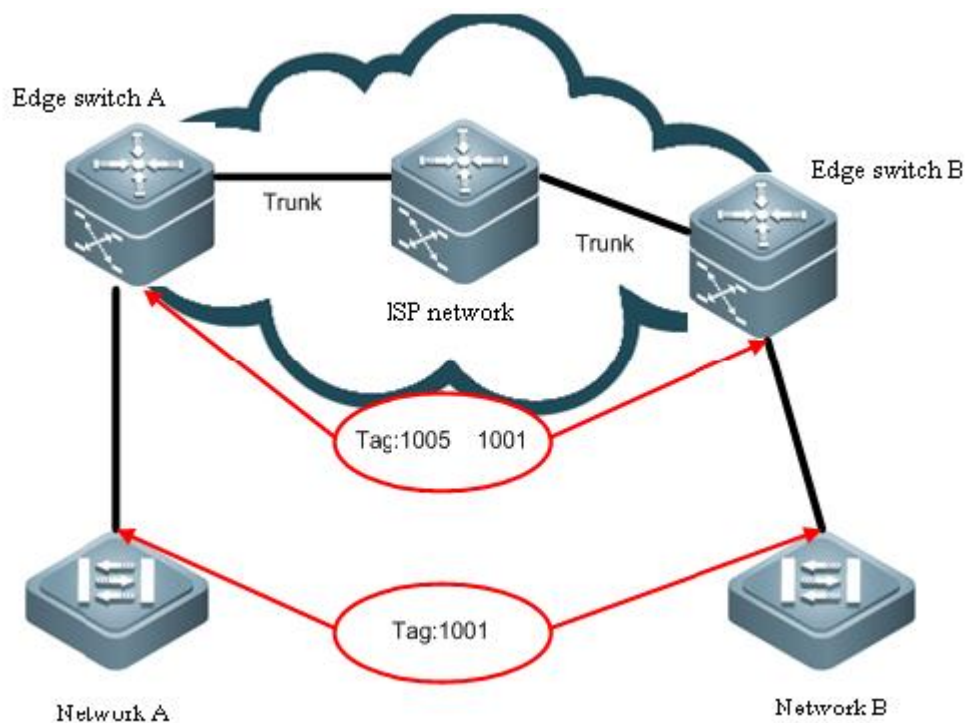
2.9.1.4 QinQ

Scenario

Business users of a network service provider usually have special requirements on the number of supported VLANs and the VLAN ID. The VLAN scope required by one user of a service provider may overlap with the VLAN scope required another user. In addition, the switching channels of VLANs of different users may mix up on the core network of the service provider. However, if each user is specified with a VLAN scope, the user configuration will be restricted and the number of VLANs will easily exceed the limit 4096 defined in the 802.1Q. Utilizing the IEEE 802.1Q Tunneling function, the service provider can use one VLAN (service provider VLAN) to support multiple VLAN users. The user VLANs is reserved. In this case, even if the users of a network service provider are of the same VLAN, they are segregated on the internal network of the service provider. The tunneling function extends the VLAN scope by using double tags. The maximum number of VLANs provided a tunnel port (a port that supports IEEE 802.1Q Tunneling) reaches 4K*4K. When configuring a tunnel, you can assign a VLAN to the tunnel port as its dedicated VLAN. In this case, the cascaded user networks require only one service provider VLAN. The user traffic is packed into double-tag frames by the service provider VLAN during transmission on the service provider network. The two layers of tags of QinQ packets are transmitted on the carrier network. The internal tags are transmitted transparently, featuring simplicity and practicability. It can serve an extension of core MPLS VPN in Metro Ethernet VPN and become an end-to-end VPN technology.

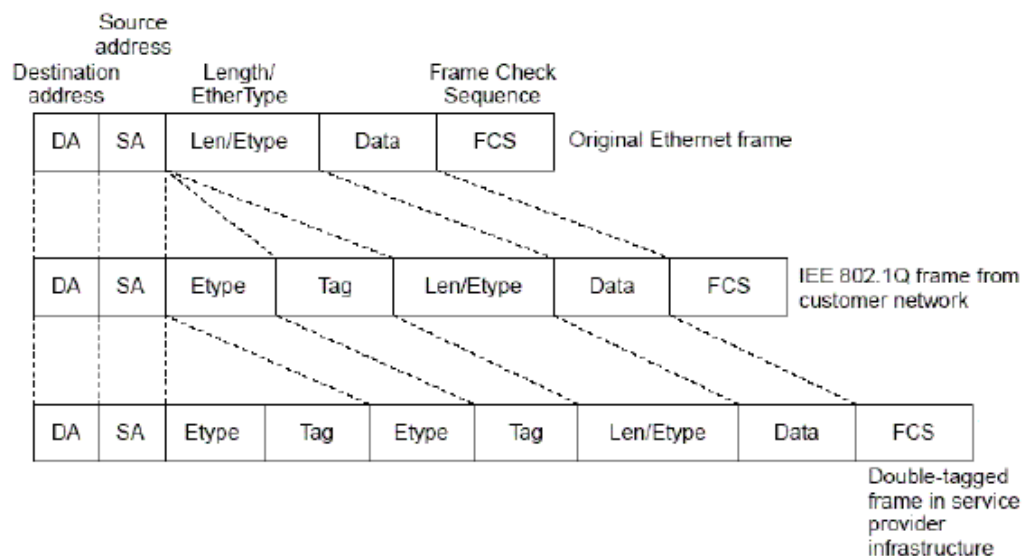
As shown in Figure 1, the packets from Network A's VLAN 1001 are added with the outer VLAN tag 1005 before entering the ISP's network. Hence, the packets carry with two tags and be propagated in the ISP's network by the outer VLAN tag 1005. The outer VLAN tag 1005 will be stripped when the packets leave the ISP's network. In Network B, the packets are propagated by VLAN tag 1001.

Figure 1-1 QinQ sketch map



The following figure illustrates the course of adding two tags. The ingress of edge device is dot1q-tunnel port (or abbreviated as tunnel port). All frames entering the edge device are considered to be untagged, no matter whether are really untagged or tagged with 802.1Q tag, and then are encapsulated with the tag of ISP. VLAN ID is the default VLAN of tunnel port.

Figure 1-2 Double-Tag packet structure



Capture the message format as follows :

```

+ Frame 176: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
+ Ethernet II, Src: Fujianst_00:00:01 (00:d0:f8:00:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 200
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = CFI: Canonical (0)
  .... 0000 1100 1000 = ID: 200
  Type: 802.1Q Virtual LAN (0x8100)
- 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 20
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = CFI: Canonical (0)
  .... 0000 0001 0100 = ID: 20
  Type: ARP (0x0806)
  Padding: 000000000000000000000000
- Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: d0:00:00:00:01:00 (d0:00:00:00:01:00)
  Sender IP address: 172.18.10.1 (172.18.10.1)
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.18.10.254 (172.18.10.254)

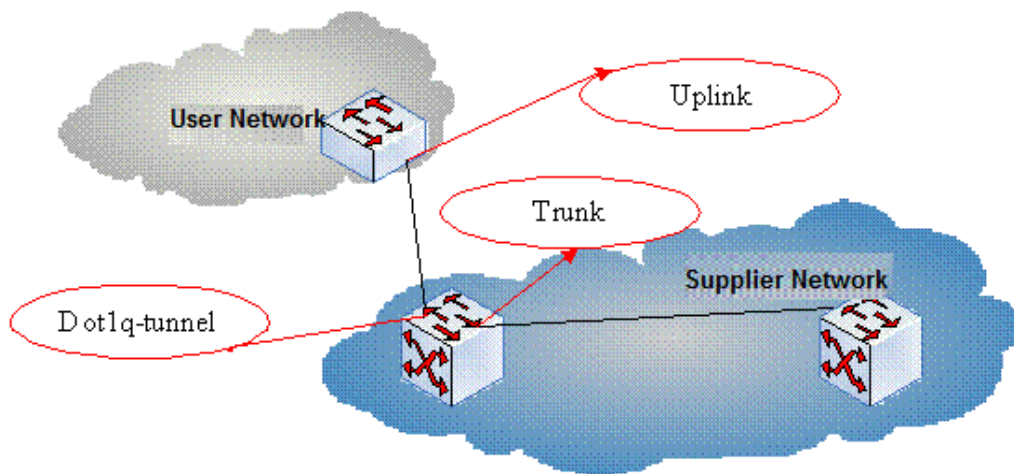
```

Note :

1. N18000-CB products do not support the flexible QinQ function or the VLAN MAPPING function. N18000-CB products support 3 TPIDs in the global configuration mode, namely, 0x8100, 0x8100, and 0x8100.
2. N18000-ED/DB products support 4 TPID values in the global configuration mode, namely, 0x8100 and 3 any values.

QinQ Port

Ruijie has brought in two new bridge interfaces, Dot1q-Tunnel and Uplink, in QinQ implement. The following figure shows the application model:



In the preceding figure, the customer bridged LAN connects to the provider bridged network through the Customer Bridge (CB) and the Provider Bridge (PB). The service provider provides different services and links to different customers. Data are forwarded on the customer bridged LAN with C-TAGs and are added with (or stripped of) S-TAGs on the customer network port for transmission on the service provider network. Data forwarding on the provider bridged network is transparent compared with data transmission on the customer bridged LAN.

Tunnel Port

Utilizing the IEEE 802.1Q Tunneling function, the service provider can use one VLAN (service provider VLAN) to support multiple VLAN users. The user VLANs is reserved. In this case, even if the users of a network service provider are of the same VLAN, they are segregated on the internal network of the service provider. The tunneling function extends the VLAN scope by using double tags. The port that supports IEEE 802.1Q Tunneling is called a tunnel port. When configuring a tunnel, you can assign a VLAN to the tunnel port as its dedicated VLAN. In this case, the cascaded user networks require only one service provider VLAN. The user traffic is packed into double-tag frames by the service provider VLAN during transmission on the service provider network.

Uplink port

Uplink port essentially is a special trunk port. The difference is that the packets outputted from the uplink port are tagged, but the packets outputted from the trunk port (when they are forwarded from native VLAN) are untagged. A typical example is the port of a user network connecting to an ISP network.

QinQ Classification

Basic QinQ

Basic QinQ is enabled based on port. When tunnel port is configured, the device will add the VLAN tag of the default VLAN of the tunnel port to the packet arriving the tunnel port. If the packet is already of a VLAN tag, this means it has two tags. Basic QinQ is simple, but the encapsulation of outer VLAN tag is not flexible enough.

Flexible QinQ

Flexible QinQ can flexibly encapsulate different outer VLAN tags for different flows by flow classification method like user VLAN tag, MAC address, IP protocol, source address, destination address, priority or port number of application program.

You can:

- Add outer VLAN tag by inner VLAN tag
- Modify inner VLAN tag by outer VLAN tag
- Modify outer VLAN tag by inner VLAN tag
- Add outer VLAN tag by ACL
- Modify outer VLAN tag by ACL
- Modify inner VLAN tag by ACL

Restriction of QinQ Configuration

The following restrictions apply to QinQ configuration:

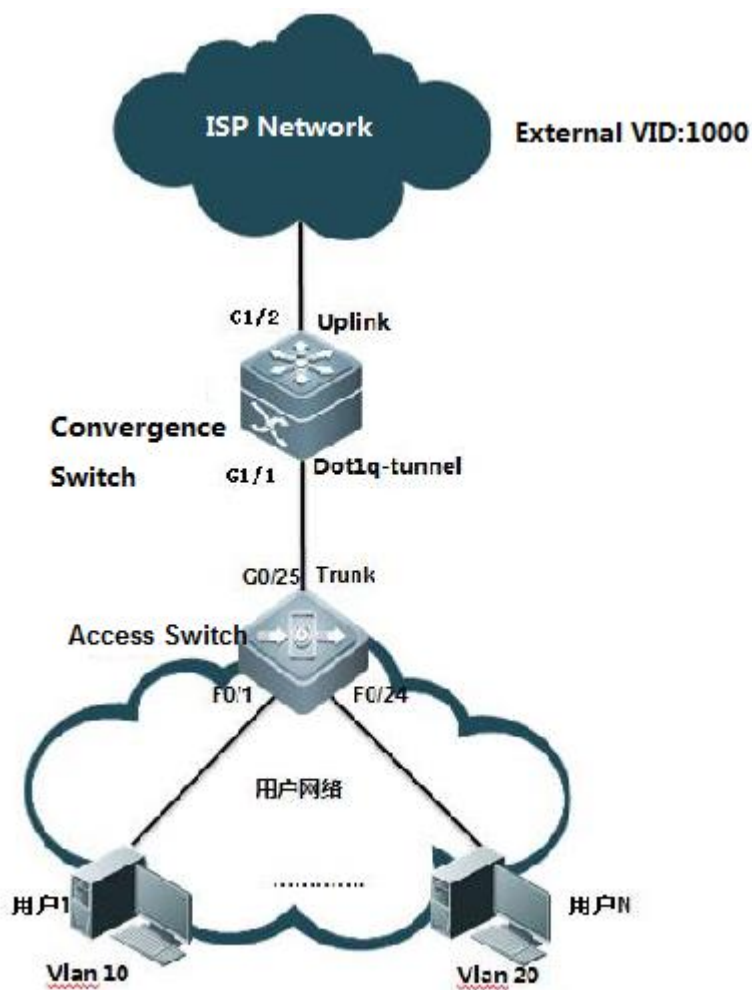
- The routed ports cannot be configured as tunnel ports.
- The 802.1x function cannot be enabled on the port configured as a tunnel port.
- Port security cannot be enabled on the port configured as a tunnel port.
- For the ACL applied on the tunnel port, the inner keyword is necessary to match the VID of user tag.
- It is recommended to configure the egress of user network connecting the ISP network as uplink port as well. If the TPID of ISP tag is set on the QinQ-enabled port of the user network, the TPID of ISP tag of uplink port should be set with the same value.
- QinQ does not support hot backup.
- The MTU of a port is 1500 bytes by default. A packet will be increased by 4 bytes when it is added with outer VLAN tag. It is recommended to increase the MTU value of ports in ISP network at an appropriate extent, or at least 1504 bytes.
- Once QinQ is enabled on a port, to enable IGMP Snooping, you need set SVGL sharing mode or otherwise IGMP Snooping does not function on the port with QinQ enabled.

2.9.1.4.1 Basic QinQ

I. Networking Requirements

Customer PCs on VLAN 10 and VLAN 20 are connected to the access switch. The Trunk port of the access switch is connected to the convergence switch. The convergence switch requires basic QinQ functions and adds external tag VLAN 1000 to tagged data stream forwarded by access users.

II. Network Topology



III. Configuration Tips

1. On the convergence switch, set the port that connects the carrier network as an uplink port and configure the QinQ function on the port that connects the access switch.
2. On the access switch, create the related VLANs, set the port that connects users as an access port and the port that connects the convergence switch as a trunk port.

IV. Configuration Steps

On the convergence switch, perform the following steps:

1. Create the external VLAN 1000.

```
Ruijie#configure terminal
Ruijie(config)#vlan 1000
Ruijie(config-vlan)#exit
Ruijie(config)#
```

2. Enable the basic QinQ functions on the port that connects the access switch.

```
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)#switchport mode dot1q-tunnel ----->configure interface G1/1 as dot1q-tunnel
Ruijie(config-if-GigabitEthernet 1/1)#switchport dot1q-tunnel native vlan 1000 ----->configure vid of dot1q-tunnel as 1000
Ruijie(config-if-GigabitEthernet 1/1)#switchport dot1q-tunnel allowed vlan add untagged 1000
```

3. Set the port that connects the carrier network as an uplink port.

```
Ruijie(config)# interface gigabitEthernet 1/2
Ruijie(config-if-GigabitEthernet 1/2)#switchport mode uplink
```

4. On the uplink port, modify the TPID value of output packets to a value identifiable by a third-party devices, which is **0x9100**. (**This step is optional.** The default TPID for Ruijie devices is **0x8100**.) The TPIDs for devices vary with manufactures. For example, the default TPID for Huawei devices is **0x9100**. To interconnect with Huawei devices, you need to change the TPID to **0x9100**.

```
Ruijie(config-if-GigabitEthernet 1/2)#frame-tag tpid 9100
```

On the access switch, perform the following steps:

```
Ruijie(config)#vlan range 10,20
Ruijie(config-vlan-range)#exit
Ruijie(config)#interface range f0/1-12
Ruijie(config-if-range)#switchport access vlan 10
Ruijie(config-if-range)#exit
Ruijie(config)#interface range f0/13-24
Ruijie(config-if-range)#switchport access vlan 20
Ruijie(config-if-range)#exit
Ruijie(config-if-GigabitEthernet 0/25)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/25)#end
```

Note:

1. In a QinQ configuration model, if the uplink port connects edge devices to the service provider network is a Trunk port or Hybrid port, do not set the native VLAN of the Trunk port or Hybrid port to the default VLAN of the tunnel port, because when a packet is output on the Trunk port or Hybrid port, the tag containing its native VLAN ID is removed from the packet.
2. When the QinQ function is enabled, the device encapsulates user packets with the external VLAN tag, rather than forwarding the packets based on the original VLAN specified in the packets. Therefore, you do not have to create VLANs for users on the device. (The configuration of user VLANs has no influence on the network.)
3. An uplink port is a special Trunk port. The difference is that **packets sent from an uplink port are tagged**, while **packets sent from an Trunk port are untagged if they are forwarded by the native VLAN**.

4. In basic QinQ configuration, the port adds external tags no matter to the received packets no matter whether they are tagged or not. If the received packet **has a VLAN tag, the packet becomes a double-tag packet**. If the received packet **does not have a VLAN tag, the packet becomes a packet with a default VLAN tag**.

5. The basic QinQ function does not support the identification and retention of management VLAN tags without adding external tags during packet forwarding.

6. At present, all Ruijie switches do not support the termination of QinQ tags. That is, the two layers of tags cannot be resolved on one switch. To resolve two layers of tags, you need to add a switch.

V. Verification

1. Check whether the QinQ function is enabled on the port.

```
Ruijie(config)#show dot1q-tunnel interface g1/1
```

| Ports | Dot1q-tunnel |
|-------|--------------|
| Gi1/1 | Enable |

2. Check the TPID value on the port.

```
Ruijie#show frame-tag tpid interfaces gigabitEthernet 1/2
```

| Ports | Tpid |
|-------|--------|
| Gi1/2 | 0x9100 |

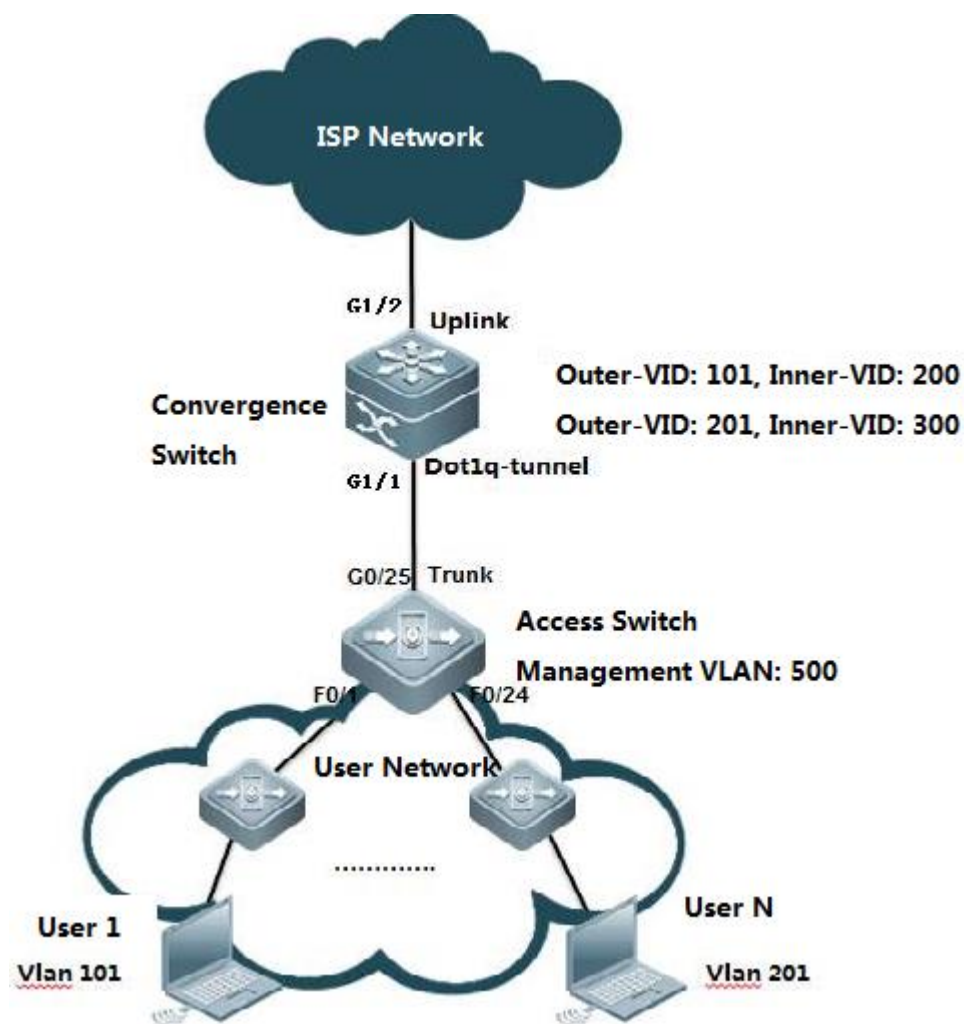
2.9.1.4.2 Flexible QinQ - VID-Based QinQ

I. Networking Requirements

1. The convergence switch implements flexible QinQ based on the user VLAN tag classification. Add data streams from user VLAN 101 to user VLAN 200 with external tags VLAN 101 and data streams from user VLAN 201 to user VLAN 300 with external tags VLAN 201.

2. Manage the access switches. The management VLAN is 500. Data streams from the VLAN are forwarded without adding external tags and their original tags are retained.

II. Network Topology



III. Configuration Tips

1. On the convergence switch, configure user VLAN tag-based flexible QinQ on the port that connects the floor distribution switch.

Flexible QinQ planning on user VLAN tag-based data stream tagging with external VLANs

| Device | Service | User VLAN Tag | External VLAN Tag | Classification Rules |
|--------------------|-----------------------------------|---------------|-------------------|----------------------|
| Convergence switch | Internet access service for users | 101-200 | 101 | User VLAN scope |
| Convergence switch | Internet access service for users | 201-300 | 201 | User VLAN scope |

2. Set the management VLAN on the floor distribution switch to a native VLAN and the management VLAN on the access switch to the native VLAN of dot1q-tunnel.

IV. Configuration Steps

On the convergence switch, perform the following steps:

1. Create ISP VLANs 101 and 201 to identify different service data types.

```
Ruijie#configure terminal
Ruijie(config)#vlan 101
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 201
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 500
Ruijie(config-vlan)#exit
```

2. On the downlink port of the convergence switch, configure the flexible QinQ function for adding external VLAN tags based on the user VLAN.

```
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-gigabitEthernet 1/1)# switchport mode dot1q-tunnel
Ruijie(config-if-gigabitEthernet 1/1)# switchport dot1q-tunnel allowed vlan add untagged 101,201,500
Ruijie(config-if-gigabitEthernet 1/1)# dot1q outer-vid 101 register inner-vid 101-200
Ruijie(config-if-gigabitEthernet 1/1)# dot1q outer-vid 201 register inner-vid 201-300
Ruijie(config-if-gigabitEthernet 1/1)# switchport dot1q-tunnel native vlan 500
Ruijie(config)# interface gigabitEthernet 1/2
Ruijie(config-if-GigabitEthernet 1/2)#switchport mode uplink
```

On the access switch, perform the following steps:

1. Create the user VLANs based on the user ports and configure the management VLAN and management IP address.
2. Set the uplink port as a Trunk port and set the native VLAN to VLAN 500.

```
Ruijie(config)# interface gigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/25)#switchport trunk native vlan 500
Ruijie(config-if-GigabitEthernet 0/25)#end
```

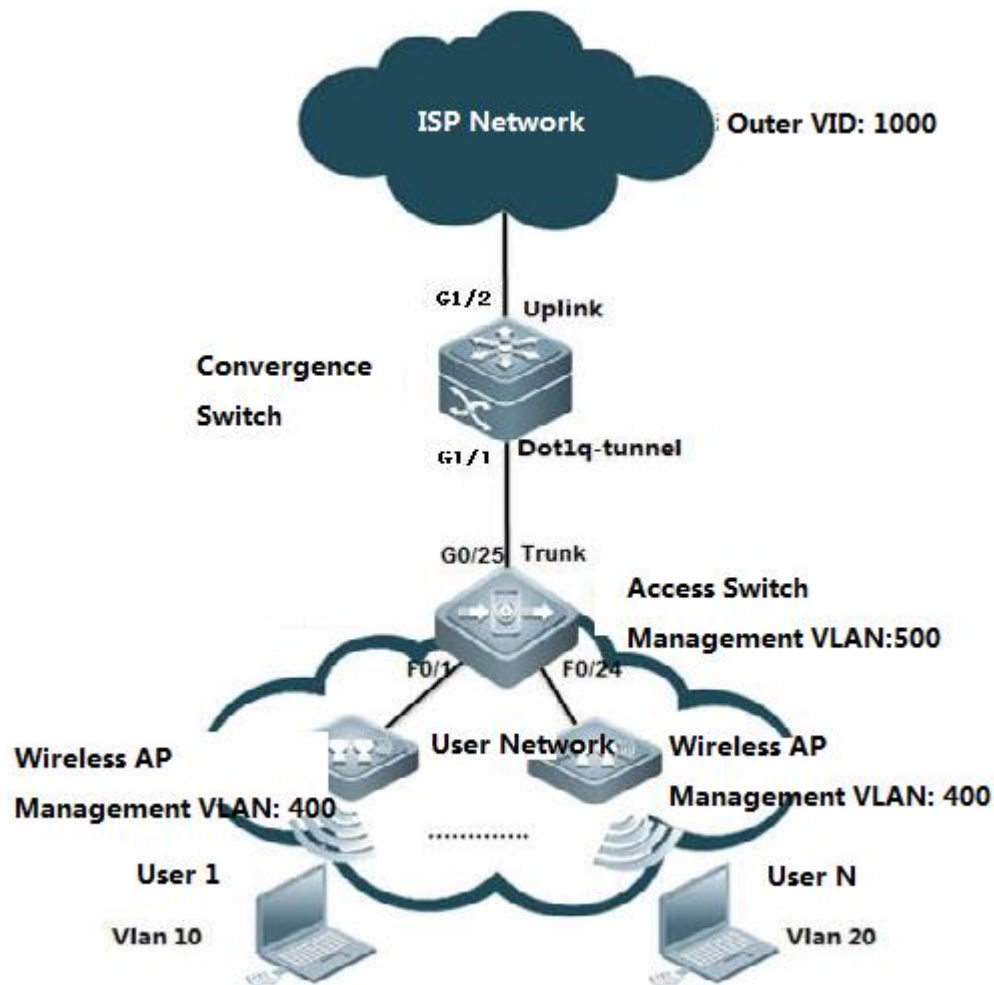
Note:

1. An uplink port is a special Trunk port. The difference is that packets sent from an uplink port are tagged. while **packets sent from an Trunk port are untagged if they are forwarded by the native VLAN.**
2. The flexible QinQ function allows the retention of management VLAN tags without adding external tags during packet forwarding.
3. At present, all Ruijie switches do not support the termination of QinQ tags. That is, the two layers of tags cannot be resolved on one switch. To resolve two layers of tags, you need to add a switch.

4. An external tag can be the same as or different from the internal tag. (For example, in the example, the internal tags ranges from 101 to 200 and the external tag is 101.)

5. If the customer has **two management VLANs**, and **tags of both management VLANs in the data streams are to be retained without adding the streams with external tags**, do as follows:

1. Network topology



2. Customer requirement

The customer has two management VLANs. One is the wireless AP management VLAN 400 and the other is the access switch management VLAN 500. Data streams with tags of either of the two VLAN are to be forwarded directly without being added with external tags.

For data streams tagged with user VLANs, add external tags VLAN 1000.

3. Run the switch configuration commands.

The convergence switch configuration commands are as follows:

```
vlan 400
vlan 500
vlan 1000
```

```
interface GigabitEthernet 1/1
switchport mode dot1q-tunnel
switchport dot1q-tunnel allowed vlan add tagged 400
switchport dot1q-tunnel allowed vlan add untagged 500,1000
switchport dot1q-tunnel native vlan 500
dot1q outer-vid 400 register inner-vid 400
dot1q outer-vid 1000 register inner-vid 10,20
interface GigabitEthernet 1/2
switchport mode hybrid
switchport hybrid allowed vlan add untagged 400
```

Tagged packet forwarding

1. Packets **tagged with the switch management VLAN 500** are processed in an original manner. The uplink port on the access switch removes the VLAN 500 tag. The convergence switch then adds the VLAN 500 tag and forwards the packet through the uplink port to the ISP network. In the reverse direction, the dotq-tunnel port removes the VLAN 500 tag and forwards the packet to the access switch.

2. Packets **tagged with the wireless AP management VLAN 400** are processed in a different manner. When the wireless AP management VLAN data streams reach the access switch, the data streams with VLAN 400 tags are forwarded directly to the dot1q-tunnel port on the convergence switch and are added with another VLAN 400 tag. Then, each AP management data packet has two VLAN 400 tags. When the double-tagged wireless AP management VLAN data streams are forwarded from the uplink port, their external tags are removed and the data streams contain only one layers of tags. This is because the uplink port is set as a Hybrid port and VLAN 400 is set to **untag**. The data streams returning from the ISP network contain one layer of VLAN 400 tags and the VLAN 400 tags are not removed before forwarding due to the configuration **switchport dot1q-tunnel allowed vlan add tagged 400**.

4. On the access switch, do as follows:

Create the user VLANs based on the user ports and configure the management VLAN and management IP address.

Set the uplink port as a Trunk port and set the native VLAN to VLAN 500.

```
Ruijie(config)# interface gigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/25)#switchport trunk native vlan 500
Ruijie(config-if-GigabitEthernet 0/25)#end
```

V. Verification

1. Check that the configurations are correct. Check whether the downlink port is a dot1q-tunnel port, whether the VLAN in the external tag is added to the approved VLAN list on the port, whether the mapping policy on the port is correct, and whether the uplink port configuration is correct.

```
Ruijie#show running-config interface gigabitEthernet 1/1
interface GigabitEthernet 1/1
```

```

switchport mode dot1q-tunnel
switchport dot1q-tunnel allowed vlan add untagged 101,201,500
dot1q outer-vid 101 register inner-vid 101-200
dot1q outer-vid 201 register inner-vid 201-300
switchport dot1q-tunnel native vlan 500
spanning-tree bpdudfilter enable

Ruijie#show running-config interface gigabitEthernet 1/2
interface GigabitEthernet 1/2
switchport mode uplink

```

3. Check the QinQ configuration on the port of the device again. The check items are the same as that of step 1.

```

Ruijie#show interfaces dot1q-tunnel

=====Interface Gi1/1=====
Native vlan: 500
Allowed vlan list:1,101,201,500
Tagged vlan list:

```

4. Check the mapping policies of internal tags and external tags and ensure that the **VLANs in the external tags map correct to the VLANs in the internal tags.**

```

Ruijie#show registration-table

```

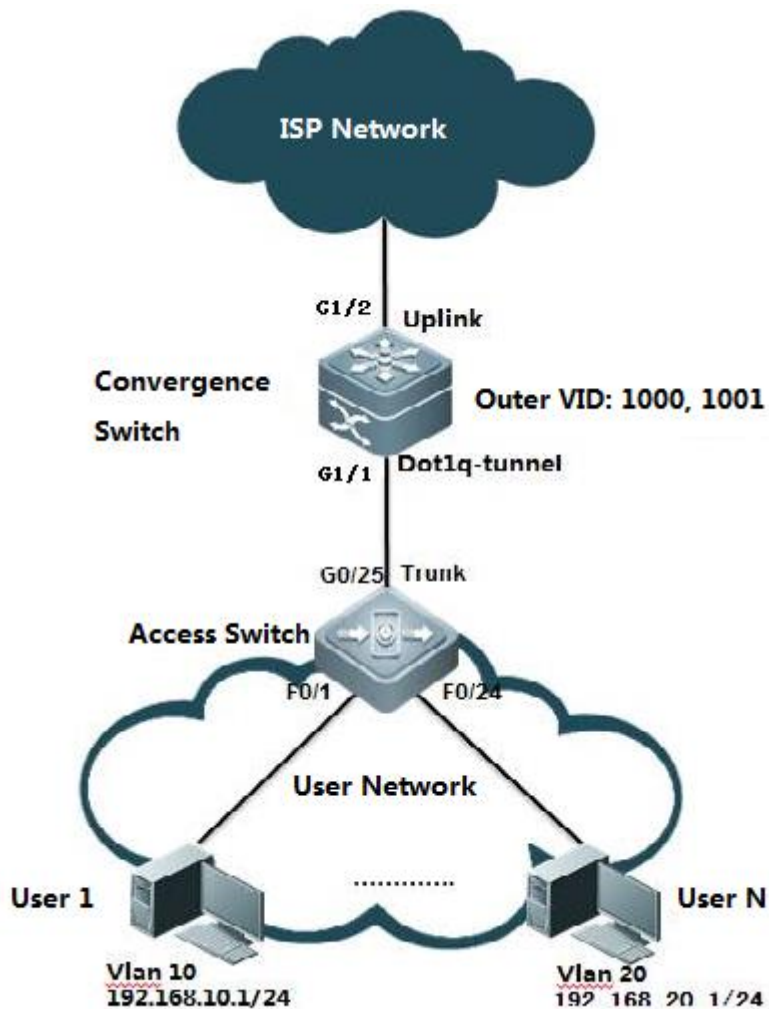
| Ports | Type | Outer-VID | Inner-VID-list |
|-------|-----------|-----------|----------------|
| Gi1/1 | Add-outer | 101 | 101-200 |
| Gi1/1 | Add-outer | 201 | 201-300 |

2.9.1.4.3 Flexible QinQ - Stream-based QinQ

I. Networking Requirements

1. The convergence switch implements flexible QinQ based on the user data stream classification. For user data streams of the network segment 192.168.10.0/24, add external tags VLAN 1000. For user data streams of the network segment 192.168.20.0/24, add external tags VLAN 1001.
2. Manage the access switches. The management VLAN is 500. Data streams from the VLAN are forwarded without adding external tags and their original tags are retained.

II. Network Topology



III. Configuration Tips

1. On the access switch, configure the user data stream-based flexible QinQ on the port that connects the floor distribution switch. For user data streams of the network segment 192.168.10.0/24, add external tags VLAN 1000. For user data streams of the network segment 192.168.20.0/24, add external tags VLAN 1001.
2. Set the management VLAN on the floor distribution switch to a native VLAN and the management VLAN on the access switch to the native VLAN of dot1q-tunnel.
3. At present, all Ruijie switches do not support the termination of QinQ tags. That is, the two layers of tags cannot be resolved on one switch. To resolve two layers of tags, you need to add a switch.

IV. Configuration Steps

On the convergence switch, perform the following steps:

1. Create ISP VLANs 1000 and 1001 to identify different service data types.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Ruijie(config)#vlan 1000
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 1001
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 500
Ruijie(config-vlan)#exit
```

2. Create the user data stream-based ACL.

```
Ruijie(config)#ip access-list standard vlan10
Ruijie(config-std-nacl)#permit 192.168.10.0 0.0.0.255
Ruijie(config-std-nacl)#exit
Ruijie(config)#ip access-list standard vlan20
Ruijie(config-std-nacl)#permit 192.168.20.0 0.0.0.255
Ruijie(config-std-nacl)#exit
Ruijie(config)#
```

3. Enable the data-stream based flexible QinQ function on the convergence switch.

```
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# switchport mode dot1q-tunnel
Ruijie(config-if-GigabitEthernet 1/1)# switchport dot1q-tunnel allowed vlan add untagged 1000,1001,500
Ruijie(config-if-GigabitEthernet 1/1)# traffic-redirect access-group vlan10 nested-vlan 1000 in
Ruijie(config-if-GigabitEthernet 1/1)# traffic-redirect access-group vlan20 nested-vlan 1001 in
Ruijie(config-if-GigabitEthernet 1/1)# switchport dot1q-tunnel native vlan 500
```

4. Configure the uplink port.

```
Ruijie(config)# interface gigabitEthernet 1/2
Ruijie(config-if-GigabitEthernet 1/2)#switchport mode uplink
```

On the access switch, perform the following steps:

1. Create the user VLANs based on the user ports and configure the management VLAN and management IP address.
2. Set the uplink port as a Trunk port and set the native VLAN to VLAN 500.

```
Ruijie(config)# interface gigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/25)#switchport trunk native vlan 500
Ruijie(config-if-GigabitEthernet 0/25)#end
```

V. Verification

1. Check that the configurations are correct. Check whether the downlink port is a dot1q-tunnel port, whether the VLAN in the external tag is added to the approved VLAN list on the port, whether the mapping policy on the port is correct, and whether the uplink port configuration is correct.

```
Ruijie#show running-config interface gigabitEthernet 1/1
interface GigabitEthernet 1/1
switchport mode dot1q-tunnel
switchport dot1q-tunnel allowed vlan add untagged 500,1000-1001
switchport dot1q-tunnel native vlan 500
traffic-redirect access-group vlan10 nested-vlan 1000 in
traffic-redirect access-group vlan20 nested-vlan 1001 in
spanning-tree bpdufilter enable

Ruijie#show running-config interface gigabitEthernet 1/2
interface GigabitEthernet 1/2
switchport mode uplink
```

2. Check the QinQ configuration on the port of the device again. The check items are the same as that of step 1.

```
Ruijie#show interfaces dot1q-tunnel
=====Interface Gi1/1=====
Native vlan: 500
Allowed vlan list:1,1000,1001,500
Tagged vlan list:
```

3. Check whether the ACL is correct.

```
Ruijie#show access-lists

ip access-list standard vlan10
 10 permit 192.168.10.0 0.0.0.255

ip access-list standard vlan20
 10 permit 192.168.20.0 0.0.0.255
```

3. Check the mapping policies for stream-based tagging.

```
Ruijie#show traffic-redirect
PortsTypeVID Match-filter
-----
Gi1/1Nested-vid 1000 vlan10
Gi1/1Nested-vid 1001 vlan20
```

2.9.2 IP addressing and Application

2.9.2.1 DHCP Server

Scenario

The DHCP (Dynamic Host Configuration Protocol), specified in RFC 2131, provides configuration parameters for hosts over the Internet. The DHCP works in the client/server mode. The DHCP server assigns IP addresses for the hosts dynamically and provides configuration parameters.

The DHCP assigns IP address in three ways:

Assign IP addresses automatically. The DHCP server assigns permanent IP addresses to the clients;

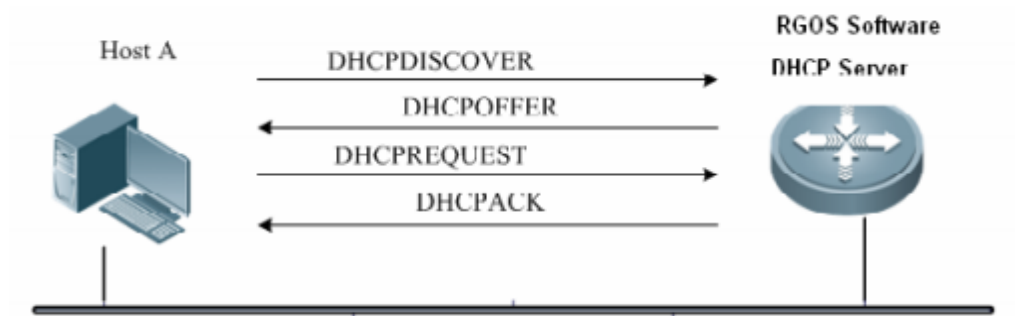
Assign IP addresses dynamically. The DHCP server assigns IP addresses that will expire after a period of time to the clients (or the clients can release the addresses by themselves);

Configure IP addresses manually. Network administrators specify IP addresses and send the specified IP addresses to the clients through the DHCP.

Among the above mentioned three methods, only dynamic assignment allows reuse of the IP address that the client does not need any more.

The format of DHCP message is based on that of BOOTP (Bootstrap Protocol) message. Hence, it is necessary for the device to be able to act as the BOOTP relay agent and interact with the BOOTP client and the DHCP server. The function of BOOTP relay agent eliminates the need of deploying a DHCP server in every physical network. The DHCP is detailed in RFC 2131 and RFC 2132.

The DHCP protocol is widely used to dynamically assign reusable network resources, for example, IP addresses. A DHCP client sends DISCOVER broadcast packets to a DHCP server. After receiving the DISCOVER packets, the DHCP server will assign resources, e.g. IP addresses, by a certain policy in OFFER packets sent to the client. Once receiving the OFFER packets, the DHCP client verifies the availability of the resource. If the resource is available, it will send a REQUEST packet; otherwise, it will re-send the DISCOVER packet. Once the server receives the REQUEST packet, it will verify whether the IP address or other limited resource can be assigned. If so, the server will send an ACK packet; otherwise, it will send a NAK packet. Once the DHCP client receives the ACK packet, it will start using the resource assigned by the server; if the NAK packet is received, the client may re-send the DISCOVER packet.

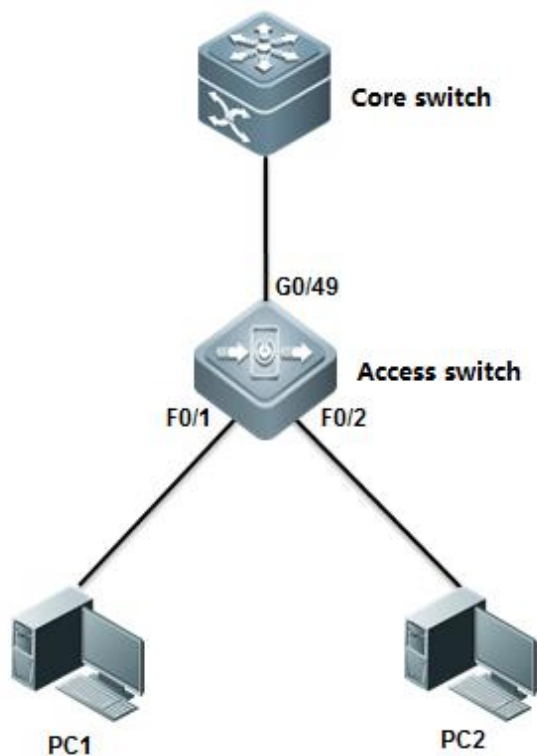


Generally, common switch support to allocate at most 2000 IP address. S86E support to allocate at most 8000 IP address.

I. Requirements

All users are on Vlan 10 and their gateway is on Core switch. Core switch acts as DHCP Server and assigns IP address to all users.

II. Network Topology



III. Configuration Tips

1. Assign ports connected to users on access switch to Vlan 10
2. Configure Core switch as DHCP Server and it assigns IP address to users.

3. DHCP Server allocates IP gateway (itself) , DNS server and lease(24H by default) to users.

IV. Configuration Steps

Core switch:

1. Enable DHCP service

```
Ruijie(config)#service dhcp ----->DHCP service is disabled by default.
```

2. Assign IP address to Vlan 10

```
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-VLAN 10)#exit
```

3. Create DHCP pool and configure DHCP parameters ---gateway , DNS , subnets.

```
Ruijie(config)#ip dhcp pool vlan10
Ruijie(dhcp-config)#network 192.168.1.0 255.255.255.0 ----->Network subnets
Ruijie(dhcp-config)#dns-server 218.85.157.99 ----->DNS server
Ruijie(dhcp-config)#default-router 192.168.1.254 ----->User Gateway
Ruijie(dhcp-config)#end
Ruijie#wr
```

Access switch:

Assign ports connected to users to Vlan 10

```
Ruijie(config)#int range fastEthernet 0/1-2
Ruijie(config-if-range)#switchport access vlan 10
```

V. Verification

1. How to display DHCP assignments

```
Ruijie#show ip dhcp binding
```

| IP address | Client-Identifier/ Hardware address | Lease expiration | Type |
|-------------|--|---------------------------|-----------|
| 192.168.1.1 | 0100.21cc.cf6f.70 | 000 days 23 hours 42 mins | Automatic |
| 192.168.1.2 | 0100.1aa9.c405.f347. 6967.6162.6974.4574. 6865.726e.6574.302f. 31 | 000 days 23 hours 44 mins | Automatic |

01 indicates ethernet and following 12 bits indicate client MAC address

2. To display NIC information on a station, execute "run----->cmd----->ipconfig /all"

```

Ethernet adapter ...

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : 00-21-CC-CF-6F-70 → MAC address
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::248b:c4f7:acc4:8ec1%13 (Preferred)
IPv4 Address. . . . . : 192.168.1.1 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 2013.3.8 9:38:56
Lease Expires . . . . . : 2013.3.9 9:39:40
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 352330188
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-5B-95-3B-60-67-20-AE-75-E4
DNS Servers . . . . . : 218.85.157.99
NetBIOS over Tcpip. . . . . : Enabled

```

2.9.2.2 DHCP Relay

Overview

The DHCP relay agent forwards DHCP packets between the DHCP server and the DHCP clients. When the DHCP clients and the server are not located in the same subnet, a DHCP relay agent must be available for forwarding the DHCP request and response messages. Data forwarding by the DHCP relay agent is different from general forwarding. In general forwarding, IP packets are unaltered and the transmission is transparent. However, upon receiving a DHCP message, the DHCP relay agent regenerates and forwards a DHCP message.

From the perspective of the DHCP client, the DHCP relay agent works like a DHCP server. From the perspective of the DHCP server, the DHCP relay agent works like a DHCP client.

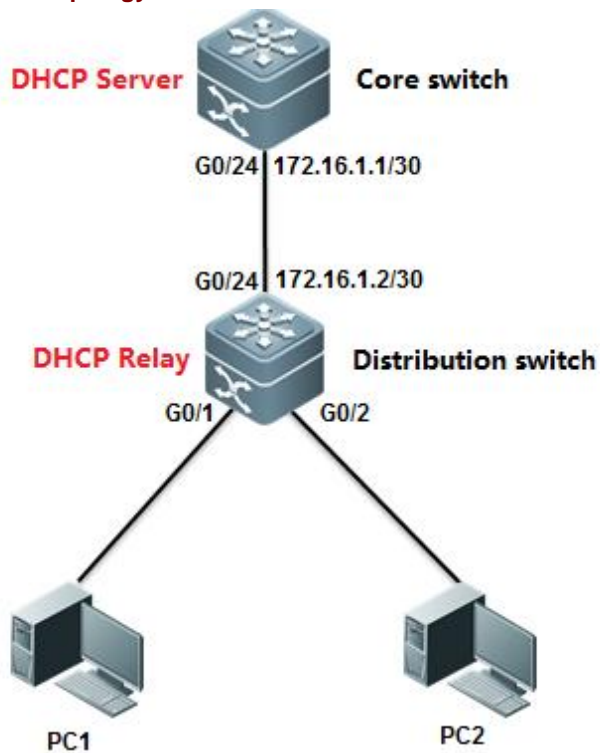
The DHCP relay forwards the DHCP request packet received in the form of unicast to the DHCP server, at the same time, forwards the DHCP response packet received to the DHCP client. The DHCP relay serves as a forwarding station, responsible for the communication between the DHCP clients and the DHCP servers at different network segments. In this way, only one DHCP server can dynamically manage IP addresses at multiple segments, that is, the DHCP dynamic IP management in the Client-Relay-Server mode, as shown below:



I. Requirements

Distribution switch is the user gateway which have enabled DHCP relay. Core switch acts as DHCP Server. Connect core switch and distribution switch through Layer 3 link.

II. Network Topology



III. Configuration Tips

1. Enable DHCP relay on distribution switch
2. Enable DHCP Service on Core switch

IV. Configuration Steps

Core switch:

1. Convert the port connected to distribuion switch to L3 port and assign a IP address to it.

```
Ruijie(config)#interface gigabitEthernet 0/24
Ruijie(config-if-GigabitEthernet 0/24)#no switchport
Ruijie(config-if-GigabitEthernet 0/24)#ip address 172.16.1.1 255.255.255.252
Ruijie(config-if-GigabitEthernet 0/24)#exit
```

2. Configure a static route.

```
Ruijie(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.2
```

3. Enable DHCP service

```
Ruijie(config)#service dhcp ----->DHCP service is disabled by default.
```

4. Create DHCP pool and configure DHCP parameters ---gateway , DNS , subnets

```
Ruijie(config)#ip dhcp pool vlan10
Ruijie(dhcp-config)#network 192.168.1.0 255.255.255.0 ----->Network subnet
Ruijie(dhcp-config)#dns-server 218.85.157.99 ----->DNS Server
Ruijie(dhcp-config)#default-router 192.168.1.254 ----->User Gateway
Ruijie(dhcp-config)#exit
```

5. Save configuration

```
Ruijie(config)#end
Ruijie#wr
```

Aggregation switch:

1. Assign IP address to Vlan 10 and SVI 10 is user gateway

```
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-VLAN 10)#exit
```

2. Convert port connected to Core switch to layer 3 port and assign IP address to it

```
Ruijie(config)#interface gigabitEthernet 0/24
Ruijie(config-if-GigabitEthernet 0/24)#no switchport
Ruijie(config-if-GigabitEthernet 0/24)#ip address 172.16.1.2 255.255.255.252
Ruijie(config-if-GigabitEthernet 0/24)#exit
```

3. Configure default route

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

4. Enable DHCP service

```
Ruijie(config)#service dhcp ----->DHCP service is disabled by default
```

5. Enable DHCP relay

```
Ruijie(config)#ip helper-address 172.16.1.1 ----->172.16.1.1 is the DHCP Server
```

6. Save configuration

```
Ruijie(config)#end
Ruijie#wr
```

V. Verification

1. How to display DHCP assignments

```

Ruijie#show ip dhcp binding
IP address      Client-Identifier/  Lease expiration      Type
                Hardware address
192.168.1.1     0100.21cc.cf6f.70   000 days 23 hours 42 mins Automatic
192.168.1.2     0100.1aa9.c405.f347. 000 days 23 hours 44 mins Automatic
                6967.6162.6974.4574.
                6865.726e.6574.302f.
                31

```

allocated IP address

01 indicates ethernet and following 12 bits indicate client MAC address

2. To display NIC information on a station, execute "run----->cmd----->ipconfig /all"

```

Ethernet adapter ...

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : 00-21-CC-CF-6F-70 -> MAC address
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::248b:c4f7:acc4:8ec1%13 (Preferred)
IPv4 Address. . . . . : 192.168.1.1 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 2013.3.8 9:38:56
Lease Expires . . . . . : 2013.3.9 9:39:40
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 Iaid . . . . . : 352330188
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-5B-95-3B-60-67-20-AE-75-E4
DNS Servers . . . . . : 218.85.157.99
NetBIOS over Tcpip. . . . . : Enabled

```

3. How to display status of DHCP relay

```

Ruijie#show ip dhcp relay-statistics
Cycle mode                0

Message                    Count
Discover                  18
Offer                     19
Request                   7
Ack                       4
Nak                       0
Decline                   0
Release                   1
Info                      1
Bad                       0

Direction                 Count
Rx client                  27
Rx client uni              1
Rx client bro              26
Tx client                  23
Tx client uni              12
Tx client bro              11
Rx server                  23
Tx server                  27

```

2.9.2.3 GRE Tunnel

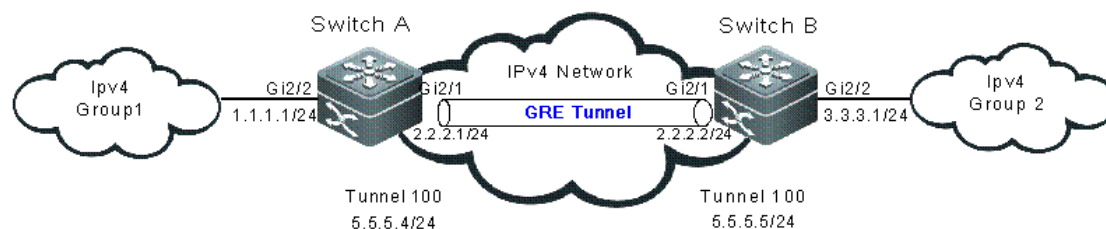
Function Overview

Generic Routing Encapsulation (GRE) is a protocol that encapsulates data packets of certain network layer protocols (for example, IP and IPX) so that encapsulated data packets can be transmitted in another network layer protocol (IP). The path where the encapsulated data packets are transmitted on the network are called a GRE tunnel. A GRE tunnel is a virtual point-to-point connection, with the devices on its two end encapsulating and decapsulating the data packets.

I. Networking Requirements

Switch A and Switch B are connected to each other over the Internet. The two subnets Group 1 and Group 2 of the private network that runs the IP are connected to each other through a GRE tunnel between two switches.

II. Network Topology



III. Configuration Tips

The configuration of a GRE tunnel covers the following:

1. Tunnel interface No.
2. Tunnel mode (GRE IP mode in this example)
3. Source address of the tunnel
4. Destination address of the tunnel
5. Route of the tunnel

Note: If the addresses of the tunnel interfaces at the two ends of the tunnel are not in the same network segment, configure the forwarding route of the tunnel from the one end to the remote end so that the encapsulated packets can be forwarded properly. You can configure a static route or a dynamic one. Configure the route on both ends of the tunnel. For two or more tunnel interfaces complying with the same encapsulation protocol, do not use the same source address or destination address. If the source address is configured in the source interface format for the tunnel interface, the source address is the main IP address of the source interface.

IV. Configuration Steps

Note: The IPv4 packet route between Switch A and Switch B is configured and reachable.

1. On Switch A, configure the following items:

Interface that connects the IPv4 external network

```
SwitchA#configureterminal
SwitchA(config)#interface GigabitEthernet 2/1
SwitchA(config-if)#ip address 2.2.2.1 255.255.255.0
```

Interface that connects the IPv4 internal network

```
SwitchA#configure terminal
SwitchA(config)#interface GigabitEthernet 2/2
SwitchA(config-if)#ip address 1.1.1.1 255.255.255.0
```

Interface of the GRE IP tunnel

```
SwitchA#configure terminal
SwitchA(config)#interface Tunnel 100
SwitchA(config-if-Tunnel 100)#tunnel mode gre ip
SwitchA(config-if-Tunnel 100)#ip address 5.5.5.4 255.255.255.0
SwitchA(config-if-Tunnel 100)#tunnel source 2.2.2.1
SwitchA(config-if-Tunnel 100)#tunnel destination 2.2.2.2
```

Route for entering the tunnel

```
SwitchA#configureterminal
SwitchA(config)#ip route 3.3.3.0 tunnel 100
```

3. On Switch B, configure the following items:

```
SwitchB#configure terminal
SwitchB(config)#interface GigabitEthernet 2/1
SwitchB(config-if)#ip address 2.2.2.2 255.255.255.0
SwitchB#configure terminal
SwitchB(config)#interface GigabitEthernet 2/2
SwitchB(config-if)#ip address 3.3.3.1 255.255.255.0
SwitchB#configure terminal
SwitchB(config)#interface Tunnel 100
SwitchB(config-if-Tunnel 100)#tunnel mode gre ip
SwitchB(config-if-Tunnel 100)#ip address 5.5.5.5 255.255.255.0
SwitchB(config-if-Tunnel 100)#tunnel source 2.2.2.2
SwitchB(config-if-Tunnel 100)#tunnel destination 2.2.2.1
SwitchB#configure terminal
SwitchB(config)#ip route 1.1.1.0 tunnel 100
```

V. Verification

1. Check the tunnel interface status on Switch A and Switch B.

```
SwitchA#show interface tunnel 100
Index(dec):9 (hex):9
Tunnel 100 is UP , line protocol is UP
  Hardware is Tunnel
  Interface address is: 5.5.5.4/24
  Interface IPv6 address is:
    No IPv6 address
  MTU 1476 bytes, BW 9 Kbit
  Encapsulation protocol is Tunnel, loopback not set
  Keepalive interval is 10 sec ,retries 0.
  Carrier delay is 2 sec
Tunnel attributes:
  Tunnel source 2.2.2.1, destination 2.2.2.2, routable
  Tunnel TOS/Traffic Class not set, Tunnel TTL 254
  Tunnel config nested limit is 4, current nested number is 0
  Tunnel protocol/transport is greip
  Tunnel transport VPN is no set
  Key disabled, Sequencing disabled
Checksumming of packets disabled
RX packets
  Drop reason(Down: 0, Checksum error: 0, sequence error: 0, routing: 0)
```

TX packets

Drop reason(Too big: 0, Payload Type error: 0, Nested-limit: 0)

Rxload is 1/255, Txload is 1/255

10 seconds input rate 0 bits/sec, 0 packets/sec

10 seconds output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer, 0 dropped

Received 0 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort

0 packets output, 0 bytes, 0 underruns , 0 dropped

0 output errors, 0 collisions, 0 interface resets

SwitchB#show interface tunnel 100

Index(dec):9 (hex):9

Tunnel 100 is UP , line protocol is UP

Hardware is Tunnel

Interface address is: 5.5.5.5/24

Interface IPv6 address is:

No IPv6 address

MTU 1476 bytes, BW 9 Kbit

Encapsulation protocol is Tunnel, loopback not set

Keepalive interval is 10 sec ,retries 0.

Carrier delay is 2 sec

Tunnel attributes:

Tunnel source 2.2.2.2, destination 2.2.2.1, routable

Tunnel TOS/Traffic Class not set, Tunnel TTL 254

Tunnel config nested limit is 4, current nested number is 0

Tunnel protocol/transport is greip

Tunnel transport VPN is no set

Key disabled, Sequencing disabled

Checksumming of packets disabled

RX packets

Drop reason(Down: 0, Checksum error: 0, sequence error: 0, routing: 0)

TX packets

Drop reason(Too big: 0, Payload Type error: 0, Nested-limit: 0)

Rxload is 1/255, Txload is 1/255

10 seconds input rate 0 bits/sec, 0 packets/sec

10 seconds output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer, 0 dropped

Received 0 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort

0 packets output, 0 bytes, 0 underruns , 0 dropped

```
0 output errors, 0 collisions, 0 interface resets
```

3. Ping to the IPv4 address of the remote interface on Switch A.

```
SwitchA#ping2.2.2.2
Sending 5, 100-byte ICMP Echoes to 2.2.2.2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10ms
```

2.9.3 IP Routing

2.9.3.1 Static Routes

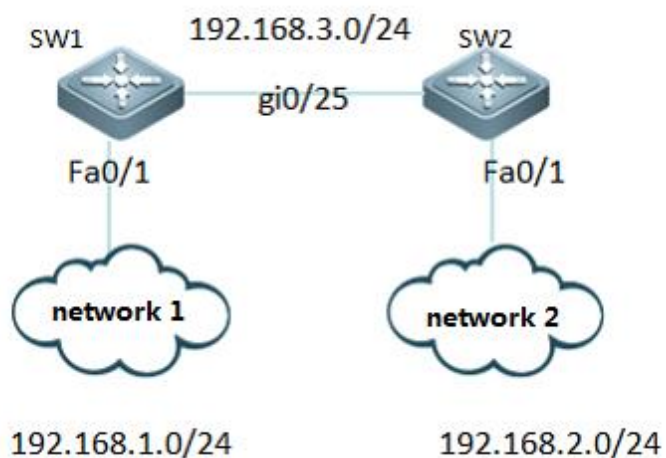
Overview

Static routes are manually configured so that the packets can be sent to the specified destination network go through the specified route. Static routes can be very important if the switch don't support dynamic routing protocol(RIP,OSPF etc.) and are useful for specifying a gateway of last resort to which all unroutable packets are sent.

I. Requirements

Configure the switch with static routes and ensure that users in network 1 can communicate with users in network 2

II. Network Topology



III. Configuration Tips

1. Assign IP addresses to SW1 and SW2

2. Configure Static Routes on SW1
3. Configure Static Routes on SW2
4. Save Configuration

IV. Configuration Steps

1. Assign IP address to SW1

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)#no switchport
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)#interface GigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#no switchport
Ruijie(config-if-GigabitEthernet 0/25)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/25)#exit
```

2. Assign IP address to SW2

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)#no switchport
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.2.254 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)#interface GigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#no switchport
Ruijie(config-if-GigabitEthernet 0/25)#ip address 192.168.3.2 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/25)#exit
```

3. Configure Static Routes on SW1

Note:

1. When you configure static routes, there're two ways to specify next hop. You can specify an IP address, or you can specify a local outgoing interface.
2. We suggest you to use IP address as next hop

```
Ruijie(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2 -----> configure static routes to destination subnet 192.168.2.0/24 and nexthop is 192.168.3.2
```

3. Configure Static Routes on SW2

```
Ruijie(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1 ----->configure static routes to destination subnet 192.168.1.0/24 and nexthop is 192.168.3.1
```

4. Save Configuration

```
Ruijie(config)#end
Ruijie#write
```

V. Verification

1. You can use "ping" on a station in network 1 to verify network connectivity
"run"-->"cmd"-->"ping x.x.x.x" (x.x.x.x is a host in network 2)

3. How to display ip routing table

```
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
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/25
C    192.168.3.1/32 is local host.
C    192.168.1.0/24 is directly connected, FastEthernet 0/1
C    192.168.1.254/32 is local host.
```

Scenario

Information about Floating Static Routes

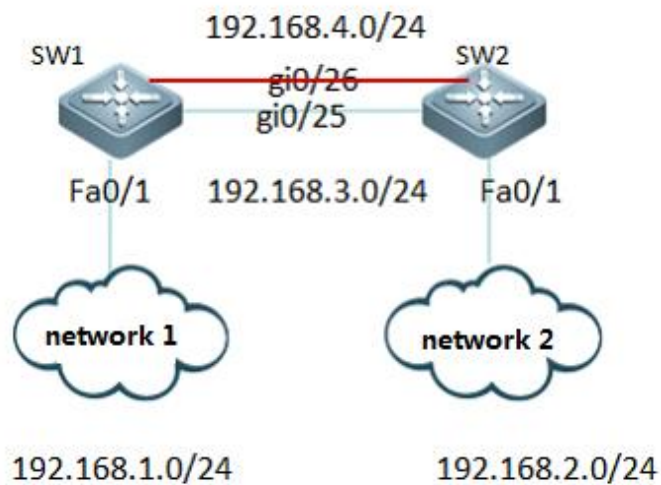
If there're two WAN accesses to two different service providers on your network, you can configure two static routes for each service provider and one route can be floating static route to ensure a backup or redundant path.

You must configure a floating static route with a higher administrative distance than the primary route that it backs up

I. Requirements

1. There're two accesses to the same destination on switch.
2. Switch switches to the backup route(through G0/26) when the primary route (through G0/25)comes down.

II. Network Topology



III. Configuration Tips

1. Assign IP address to SW1 and SW2
2. Configure Floating Static Routes with higher administrator distance than the route it backs up

IV. Configuration Steps

1. Assign IP address to SW1

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)#no switchport
Ruijie(config-if-FastEthernet 0/1)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)#interface GigabitEthernet 0/26
Ruijie(config-if-GigabitEthernet 0/26)#ip address 192.168.4.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/26)#interface GigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/25)#exit
```

2. Assign IP address to SW2

```
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 GigabitEthernet 0/26
Ruijie(config-if-GigabitEthernet 0/26)#no switchport
Ruijie(config-if-GigabitEthernet 0/26)#ip address 192.168.4.2 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/26)#interface GigabitEthernet 0/25
```

```
Ruijie(config-if-GigabitEthernet 0/25)#no switchport
Ruijie(config-if-GigabitEthernet 0/25)#ip address 192.168.3.2 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/25)#exit
```

3. Configure Static Routes on SW1

Note:

1. When you configure static routes , there're two ways to specify next hop.You can specify an IP address ,or you can specify a local outgoing interface.
2. We suggest you to use IP address as next hop

```
Ruijie(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2      ---->configure static routes to destination
subnet 192.168.2.0/24 and nexthop is 192.168.3.2
Ruijie(config)#ip route 192.168.2.0 255.255.255.0 192.168.4.2 10  ---->configure floating static routes to
destination subnet 192.168.2.0/24 with adminstrtror distance 10 and nexthop is 192.168.4.2 (by default , the
administrator distance is 1.The smaller the number , the more likely the route will be installed in the ip route table)
```

3. Configure Static Routes on SW2

```
Ruijie(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1  ---->configure static routes to destination subnet
192.168.1.0/24 and nexthop is 192.168.3.1
Ruijie(config)#ip route 192.168.1.0 255.255.255.0 192.168.4.1 10  ---->configure floating static routes to
destination subnet 192.168.1.0/24 with adminstrtror distance 10 and nexthop is 192.168.4.1 (by default , the
administrator distance is 1.The smaller the number , the more likely the route will be installed in the ip route table)
Ruijie(config)#end
Ruijie#write      ---->confirm and save
```

V. Verification

1. This example displays the ip route table on SW1 when port G0/25 comes up
SW1:

```
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
C    192.168.4.0/24 is directly connected, GigabitEthernet 0/26
C    192.168.4.1/32 is local host.
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/25
C    192.168.3.1/32 is local host.
C    192.168.1.0/24 is directly connected, FastEthernet 0/1
```

C 192.168.1.1/32 is local host.

2. This example displays the ip route table on SW1 after removing the cable on port G0/25. The floating route has been installed in ip route table.

SW1:

```
Ruijie#sho 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 not set
S    192.168.2.0/24 [10/0] via 192.168.4.2
C    192.168.4.0/24 is directly connected, GigabitEthernet 0/26
C    192.168.4.1/32 is local host.
C    192.168.1.0/24 is directly connected, FastEthernet 0/1
C    192.168.1.1/32 is local host.
```

2.9.3.2 RIP

Overview

The RIP (Routing Information Protocol) is a relatively old routing protocol, which is widely used in small or homogeneous networks. The RIP uses the distance-vector algorithm, and so is a distance-vector protocol. The RIPv1 is defined in RFC 1058 and the RIPv2 is defined in RFC 2453. Ruijie RGOS supports both two versions.

The RIP exchanges the routing information by using the UDP packets, with the UDP port number to be 520. Usually, RIPv1 packets are broadcast packets, while RIPv2 packets are multicast packets with the multicast address of 224.0.0.9. The RIP sends the update packet at the interval of 30 seconds. If the device has not received the route update packets from the peer within 180 seconds, it will mark all the routes from that device unreachable. After that, the device will delete these routes from its routing table if it still has not received any update packets from the peer within 120s.

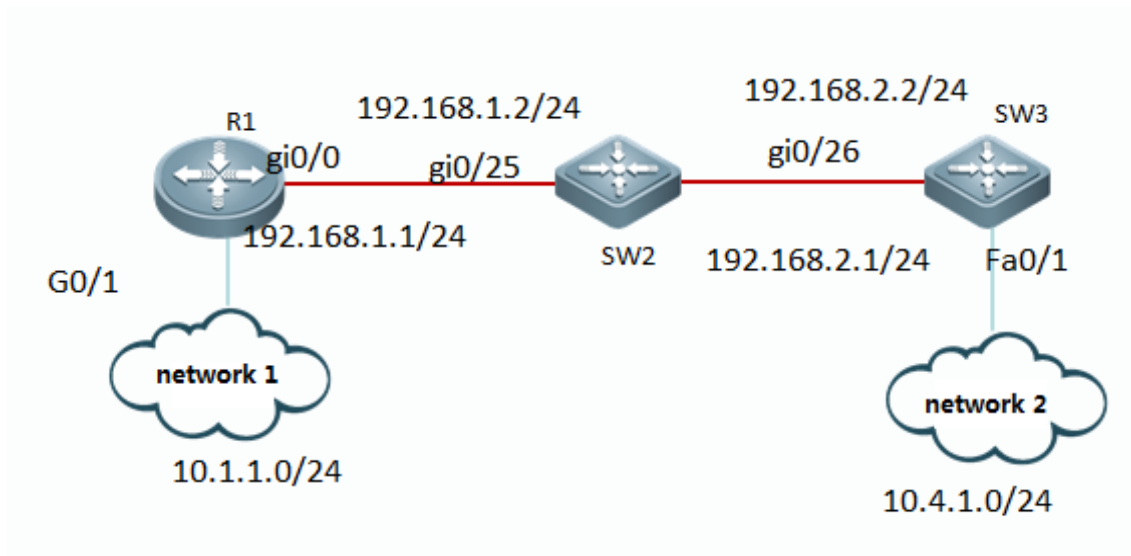
The RIP measures the distance to the destination in hop, known as route metric. As specified in the RIP, Zero hop exists when the router directly connects to the network. One hop exists when the router connects to the network through one device and so on. Up to 16 hops are supported in a network.

Note: We suggest you to build your network with OSPF rather than RIP if possible.

I. Requirements

Configure the switch with RIP and ensure that users in network 1 can communicate with users in network 2

II. Network Topology



III. Configuration Tips

1. Assign IP address to R1, SW2 and SW3.
2. Initialize RIP process and define the corresponding interface on which RIP runs

IV. Configuration Steps

1. Assign IP addresses to R1, SW2 and SW3

```
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 SW2
SW2(config)#interface gigabitEthernet 0/25
SW2(config-if-GigabitEthernet 0/25)#no switchport
SW2(config-if-GigabitEthernet 0/25)#ip address 192.168.1.2 255.255.255.0
SW2(config-if-GigabitEthernet 0/25)#exit
SW2(config)#interface gigabitEthernet 0/26
SW2(config-if-GigabitEthernet 0/26)#no switchport
SW2(config-if-GigabitEthernet 0/26)#ip address 192.168.2.1 255.255.255.0
SW2(config-if-GigabitEthernet 0/26)#exit

Ruijie(config)#hostname SW3
SW3(config)#interface gigabitEthernet 0/26
```

```
SW3(config-if-GigabitEthernet 0/26)#no switchport
SW3(config-if-GigabitEthernet 0/26)#ip address 10.4.1.1 255.255.255.0
SW3(config-if-GigabitEthernet 0/26)#exit
SW3(config)#interface fastEthernet 0/1
SW3(config-if-FastEthernet 0/1)#no switchport
SW3(config-if-FastEthernet 0/1)#ip address 192.168.2.2 255.255.255.0
SW3(config-if-FastEthernet 0/1)#exit
```

2. Initialize RIP process and define the the corresponding interface on which RIP runs

Note:

1. There're two RIP version: version 1 and version 2. RIPv2 utilizes multicast to propagate routing update instead of broadcast which RIPv1 utilizes. In addition, RIPv2 routing update carries routing mask information which RIPv1 doesn't carry.
2. When you enter "network" command in RIP configuration mode to define interfaces on RIP, **you can only define classful ip address range**, such as 10.0.0.0/8 or 172.16.0.0/16, and all interfaces belongs to the classful ip address range are defined on RIP.
- 3) By default, RIP auto summary is enabled and the switch **auto summarizes** subprefixes when **crossing classful network boundaries**. We suggest you to disable auto summary and summarize routes manually in case that switch learns incorrect routes when crossing incontinuous network.

```
R1(config)#router rip
R1(config-router)#version 2           ----->specify RIP version 2
R1(config-router)#no auto-summary     ----->disable auto-summary
R1(config-router)#network 192.168.1.0 ----->define ip address range 192.168.1.0 on RIP
R1(config-router)#network 10.0.0.0
R1(config-router)#exit

SW2(config)#router rip
SW2(config-router)#version 2
SW2(config-router)#no auto-summary
SW2(config-router)#network 192.168.1.0
SW2(config-router)#network 192.168.2.0
SW2(config-router)#exit

SW3(config)#router rip
SW3(config-router)#version 2
SW3(config-router)#no auto-summary
SW3(config-router)#network 192.168.2.0
SW3(config-router)#network 10.0.0.0
SW3(config-router)#exit
```

V. Verification

This example shows how to display IP route table and RIP routing information is propagated all over the network 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
```

2.9.3.3 OSPF

Overview

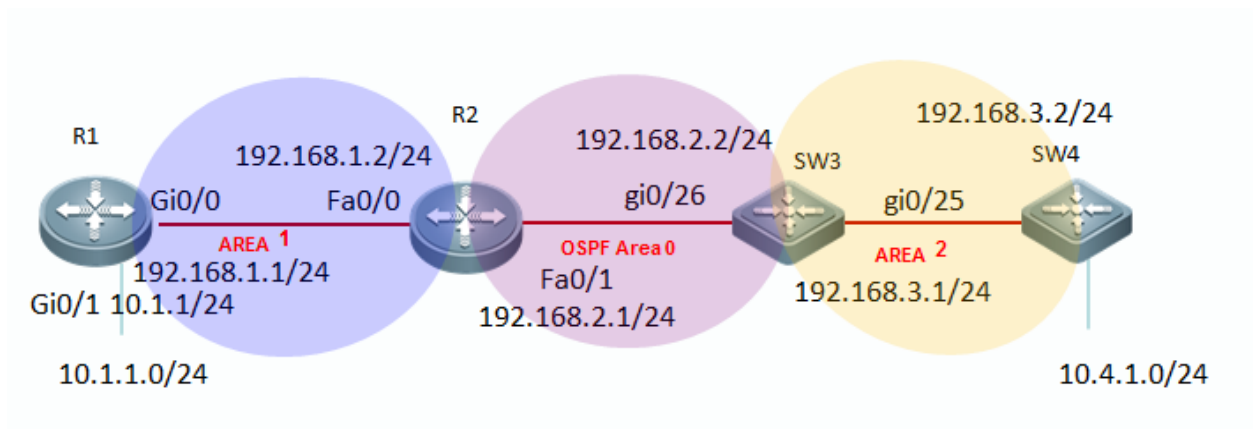
OSPF (Open Shortest Path First) is an internal gateway routing protocol based on link status developed by the IETF OSPF work group. OSPF, a routing protocol specific for IP, directly runs on the IP layer. Its protocol number is 89. OSPF packets are exchanged in multicast form using the multicast address 224.0.0.5 (for all OSPF routers) and 224.0.0.6 (for specified routers).

Note: we recommend that you can give priority to OSPF to build your network

I. Requirements

Use OSPF to build your network and every node in the network can communicate with each other.

II. Network Topology



III. Configuration Tips

1. Assign IP addresses to R1, R2 SW3 and SW4
2. Initialize OSPF process on all devices and define corresponding interfaces which OSPF runs and define the area ID for those interfaces.
3. (Optional) Modify network type on interfaces that have OSPF enabled

IV. Configuration Steps

1. Assign IP addresses to R1, R2 SW3 and SW4

```
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
R1(config-if-Loopback 0)#ip address 1.1.1.1 255.255.255.255
R1(config-if-Loopback 0)#exit
```

----->configure IP address of Loopback 0 as OSPF Router-id

```
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 SW3
SW3(config)#interface GigabitEthernet 0/26
SW3(config-if-GigabitEthernet 0/26)#no switchport
SW3(config-if-GigabitEthernet 0/26)#ip address 192.168.2.2 255.255.255.0
SW3(config-if-GigabitEthernet 0/26)#exit
SW3(config)#interface GigabitEthernet 0/25
SW3(config-if-GigabitEthernet 0/25)#no switchport
SW3(config-if-GigabitEthernet 0/25)#ip address 192.168.3.1 255.255.255.0
SW3(config-if-GigabitEthernet 0/25)#exit
SW3(config)#interface loopback 0
SW3(config-if-Loopback 0)#ip address 3.3.3.3 255.255.255.255
SW3(config-if-Loopback 0)#exit

Ruijie(config)#hostname SW4
SW4(config)#interface gigabitEthernet 0/25
SW4(config-if-GigabitEthernet 0/25)#no switchport
SW4(config-if-GigabitEthernet 0/25)#ip address 192.168.3.2 255.255.255.0
SW4(config-if-GigabitEthernet 0/25)#exit
SW4(config)#interface gigabitEthernet 0/1
SW4(config-if-GigabitEthernet 0/1)#no switchport
SW4(config-if-GigabitEthernet 0/1)#ip address 10.4.1.1 255.255.255.0
SW4(config-if-GigabitEthernet 0/1)#exit
SW4(config)#interface loopback 0
SW4(config-if-Loopback 0)#ip address 4.4.4.4 255.255.255.255
SW4(config-if-Loopback 0)#exit

```

2. Initialize OSPF process on all devices and define corresponding interfaces which OSPF runs and define the area ID for those interfaces.

Note:

1) OSPF doesn't propagate process ID to neighbor, so process ID can be different in an OSPF area.

2) OSPF detects peer neighbor area ID in hello packet while establishing OSPF neighbor. **OSPF area ID of OSPF neighbor must match.**

```

R1(config)#router ospf 1                                     ----->enable OSPF globally , and
process ID is 1
R1(config-router)#network 192.168.1.1 0.0.0.0 area 1         ----->OSPF area 1 runs on interface 192.168.1.1
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

SW3(config)#router ospf 1
SW3(config-router)#network 192.168.2.2 0.0.0.0 area 0
SW3(config-router)#network 192.168.3.1 0.0.0.0 area 2
SW3(config-router)#exit

SW4(config)#router ospf 1
SW4(config-router)#network 192.168.3.2 0.0.0.0 area 2
SW4(config-router)#network 10.4.1.1 0.0.0.0 area 2
SW4(config-router)#exit

```

3. (Optional) Modify network type on interfaces that have OSPF enabled

Note: By default, OSPF interface network type is broadcast in Ethernet and it costs about 40 seconds to elect DR/BDR. We recommend that you modify network type to point-to-point type in Ethernet to accelerate OSPF neighbor convergence.

```

R2(config)#interface fastEthernet 0/1
R2(config-if-FastEthernet 0/1)#ip ospf network point-to-point      ----->modify OSPF interface network type to
point-to-point  ( you must configure both OSPF peers at the same time)
R2(config-if-FastEthernet 0/1)#exit

SW3(config)#interface fastEthernet 0/1
SW3(config-if-FastEthernet 0/1)#ip ospf network point-to-point
SW3(config-if-FastEthernet 0/1)#exit

```

V. Verification

1. How to display OSPF neighbor table

```
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 |

peer address local port

2. How to display IP route table

```

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

```

Redistribution

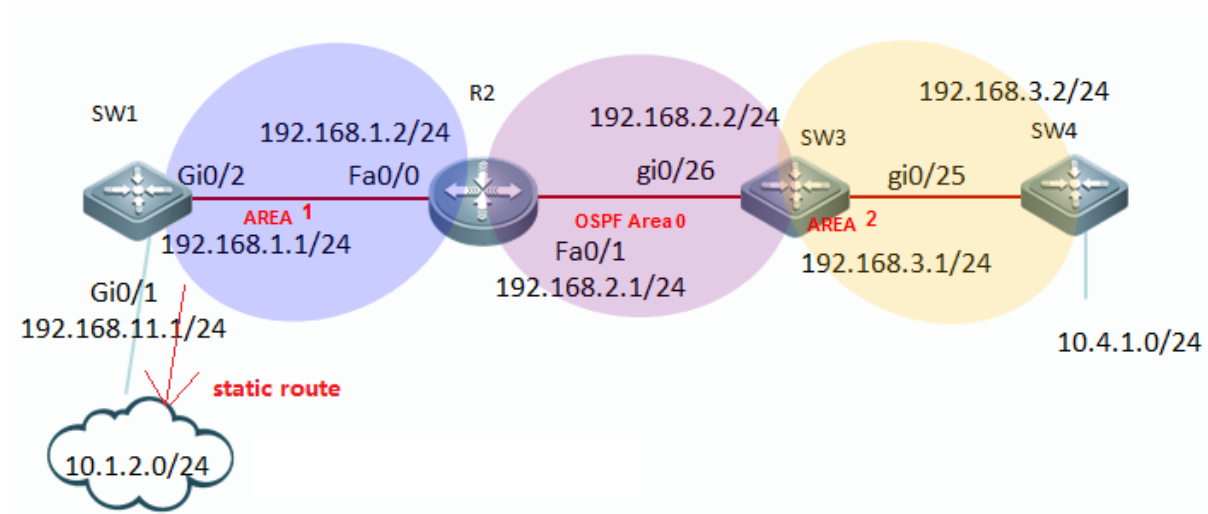
Overview

To support the routers to run multiple routing protocol processes, Ruijie product provides the function for redistributing the route information from one routing process to another routing process. For example, you can redistribute the routes in the OSPF routing area to the RIP routing area, or those in the RIP routing area to the OSPF routing area. Routes can be redistributed among all the IP routing protocols.

I. Requirements

Redistribute static route into OSPF process. All nodes in OSPF area can communicate with nodes in 10.1.2.0/24

II. Network Topology



III. Configuration Tips

1. Assign IP address and initialize OSPF process
2. Configure a static route on SW1 pointing to subnet 10.1.2.0/24
3. Redistribute static route into OSPF process

IV. Configuration Steps

1. Assign IP addresss and initialize OSPF process

see [Chapter OSPF](#) ----> [Configuring basic OSPF](#)

2. Configure a static route on SW1 pointing to subnet 10.1.2.0/24

```
SW1(config)#ip route 10.1.2.0 255.255.255.0 192.168.11.2
```

3. Redistribute static route into OSPF

Note:

- 1) This example shows the OSPF redistribution commands:

```
SW1(config)#router ospf 1
SW1(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 2 types of redistributing external routes --- type 1 and type 2. The caculation method for route metic of Type 1 and Type 2 is different.

- a. The metric of type 1 is the addition of the external cost and the internal cost used to reach that route. A type 1 route is always preferred over a type 2 route for the same destination.
- b. The metric of a type 2 route is always the external cost, irrespective of the interior cost to reach that route. By default, the redistributed external routes is type 2

```
SW1(config)#router ospf 1
SW1(config-router)#redistribute static metric-type ?
1 Set OSPF External Type 1 metrics
2 Set OSPF External Type 2 metrics
```

- 3) Only the routes that has been installed in IP route table can be redistribute into OSPF process. You can use "show ip route" EXEC command to verify it.
- 4) You **must** add keyword "**subnets**" when you redistribute routes into OSPF, otherwise only classful routes will be redistributed.

This example shows how to redistribute static route into OSPF process.

```
SW1(config)#router ospf 1
SW1(config-router)#redistribute static subnets ----->redistribute static routes
SW1(config-router)#exit
```

V. Verification

How to display IP route table and verify the reditributed routes

```
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
```

Summary

Overview

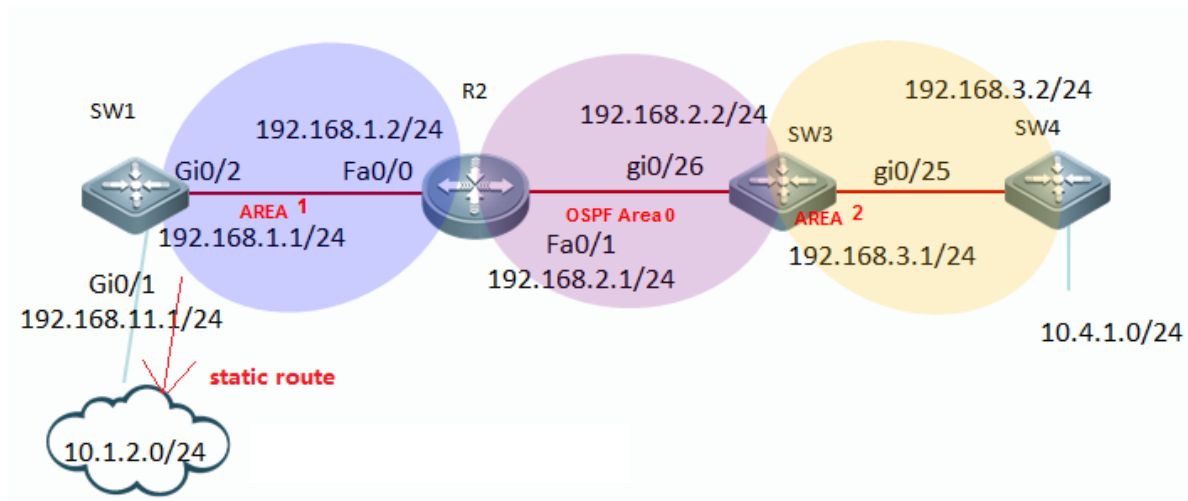
You can configure OSPF summary to reduce route numbers, decrease load of device resources.

Note: You can enable OSPF summary on ABR and ASBR ONLY

I. Requirements

Configure OSPF summary to reduce routes number on SW1

II. Network Topology



III. Configuration Tips

You can configure OSPF summary on ABR (area border router) or ASBR (Autonomous System Border Router).

IV. Configuration Steps

1. Assign IP addresses and initial OSPF process

see [Chapter OSPF ----> Configuring basic OSPF](#)

2. Redistribute static routes that pointing to subnet 10.1.2.0/24 into OSPF on SW1

see [Chapter OSPF ----> Redistribution](#)

3. Configure OSPF inter-area summary

This example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.4.0.0/16

```
SW3(config)#router ospf 1
SW3(config-router)#area 2 range 10.4.0.0 255.255.0.0 ----->summarised internal routes(2 indicates the
identifier of the area about which routes are to be summarized)
SW3(config-router)#exit
```

4. External routes summary

This example specifies one summary route to be advertised by the ASBR to other areas for all subnets on network 10.1.0.0/16

```
SW1(config)#router ospf 1
SW1(config-router)#summary-address 10.1.0.0 255.255.0.0 ----->summarise external routes
SW1(config-router)#exi
```

V. Verification

How to display IP route table and verify summarised routes

```
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
```

Stub area

Overview

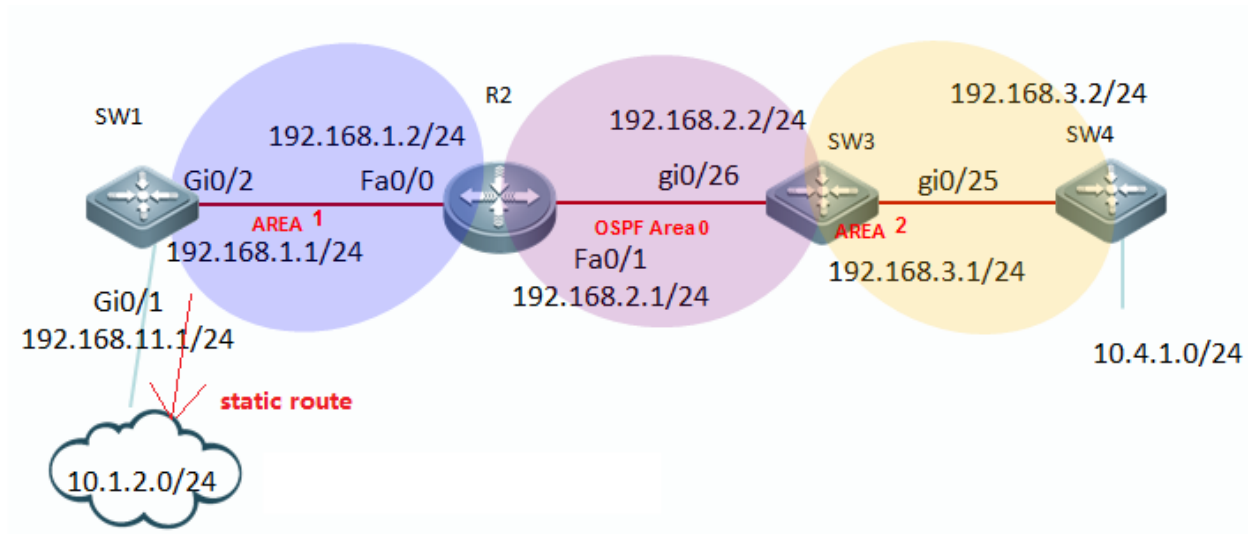
If an area is the OSPF leaf area (not a backbone area or Transit area) and no routes are imported on the devices in the area, configure the area to a STUB area. The STUB area can learn only three kinds of routes: inter-area routes, ABR advertised default routes, and routes from other areas. Without a large number of external routes, the routing tables of the devices in the STUB area are small, which reduce device resources. The devices in the STUB area are medium and low end devices.

Routers in Stub area don't propagate class 4 and class 5 LSA(external routes), so this action reduces the size of LSA database and route table . ABR of stub area also creates a class 3 inter-area (O *IA) default route automatically to ensure nodes in stub area can communicate with nodes in other areas.

I. Requirements

1. Configure area 2 as a Stub Area to filter class 4 and class 5 LSA.
2. Configure area 2 as a Totally Stub Area to filter class3, 4 and 5 LSA.

II. Network Topology



III. Configuration Tips

1. ABR of a Stub area filters class 4 and 5 LSA and creates a class 3 default route
2. ABR of a Totally Stub area filters class 3, 4 and 5 LSA and creates a class 3 default route.
3. You cannot redistribute routes into a stub area.

IV. Configuration Steps

1. Configuring Stub area

- 1.1. Assign IP addresses and configure initial OSPF

See [Chapter OSPF ----> Configuring basic OSPF](#)

- 1.2. Configure a static route on SW1 and redistribute the static route into OSPF

See [Chapter OSPF ----> Redistribution](#)

- 1.3. Configuring area 2 as Stub area

Note:

- 1) You must configure all routes in Stub area with the "stub" command
- 2) You cannot configure area 0 as Stub area.

```
SW3(config)#router ospf 1
SW3(config-router)#area 2 stub      ----->specify SW3 in stub area 2
SW3(config-router)#exit

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

2. Configuring Totally stub area

2.1. Assign IP addresses and configure basic OSPF parameters

See [Chapter OSPF ----> Configuring basic OSPF](#)

2.2. Configuring a static route on SW1 and redistribute static route into OSPF

See [Chapter OSPF ----> Redistribution](#)

2.3. Configuring area 2 as Totally Stub area

Note: You must configure all routes in Totally Stub area with the **"stub no-summary"** command

```
SW3(config)#router ospf 1
SW3(config-router)#area 2 stub no-summary ----->specify SW3 in Totally Stub area 2
SW3(config-router)#exit

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

V. Verification

1. In a stub area, display IP route table and verify that no external route is installed and ABR creates a class-3 default route.

```
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. In a totally stub area, display IP route table and verify that no inter-area route and external route are installed and ABR creates a class-3 default route.

```
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.
```

NSSA area

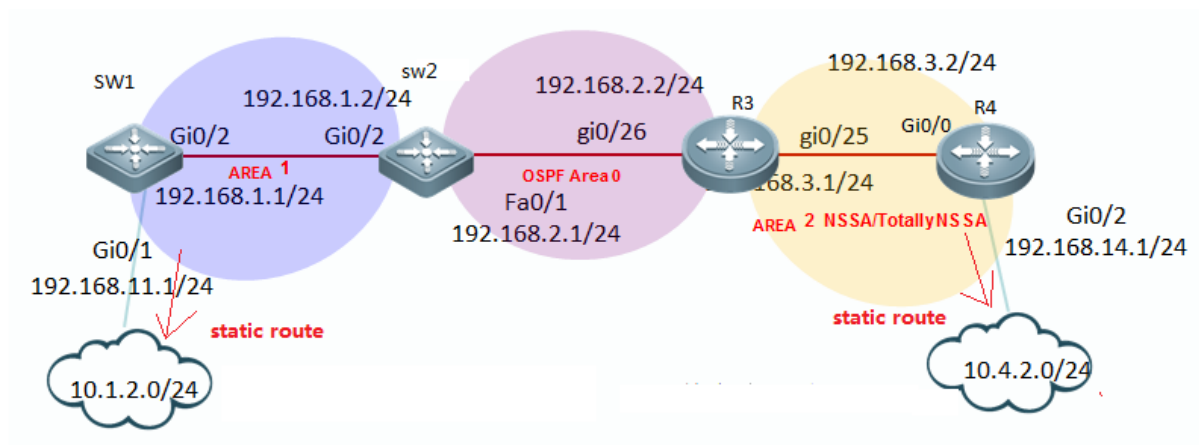
Overview

Routers in NSSA (not so stub area) don't propagate class 4 and class 5 LSA, so this action reduces the size of LSA database and route table. **In addition, you can redistribute routes into a NSSA.**

I. Requirements

1. Configure area 2 as a NSSA to filter class 4 and 5 LSA, then redistribute external static routes into NSSA.
2. Configure area 2 as a Totally Stub Area to filter class 3, 4 and 5 LSA , then redistribute external static routes into Totally NSSA Area.

II. Network Topology



III. Configuration Tips

1. ABR of a NSSA filters class 4 and 5 LSA, but **doesn't** creates a class 3 default route
2. ABR of a Totally NSSA filters class 3, 4 and 5 LSA and creates a class 3 default route .
3. You can redistribute routes into a NSSA or totally NSSA.

IV. Configuration Steps

1. Configuring NSSA area

- 1.1. Assign IP addresss and configure basic OSPF parameters

See Chapter [OSPF ----> Configuring basic OSPF](#)

- 1.2 Configure static routes on SW1 and R4, then redistribute static routes into OSPF

See [Chapter OSPF ----> Redistribution](#)

- 1.3 Configure Area 2 as NSSA

Note:

- 1) You must configure all routes in NSSA with the "**nssa**" command
- 2) You cannot configure area 0 as Stub area.

```
R3(config)#router ospf 1
R3(config-router)#area 2 nssa      ---->specify R3 in NSSA area 2
R3(config-router)#exit

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

2. Configuring Totally NSSA area

- 2.1 Assign IP addresss and configure basic OSPF parameters

see [Chapter OSPF ----> Configuring basic OSPF](#)

- 2.2 Configure static routes on SW1 and R4 ,then redistribute static routes into OSPF

see [Chapter OSPF ----> Redistribution](#)

- 2.3 Configure Area 2 as Totally NSSA area

Note:

You must configure all routes in totally NSSA with the "**nssa no-summary**" command

```
R3(config)#router ospf 1
R3(config-router)#area 2 nssa no-summary  -----> specify R3 in totally NSSA area 2
R3(config-router)#exit

R4(config)#router ospf 1s
```

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

V. Verification

1. In NSSA , display IP route table and verify that no external route (O E1 and O E2)is installed and ABR doesn't creates a class-3 default route.In addition ,you can redistribute routes into NSSA in the format (O N1 and O N2)

```
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. In totally NSSA , display IP route table and verify that no external route (O E1 and O E2) ,or inter-area route(O IA)are installed and ABR creates a class-3 default route.In addition ,you can redistribute routes into totally NSSA in the format (O N1 and O N2)

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.
```

2.9.3.4 BGP

2.9.3.4.1 Basic iBGP Configuration

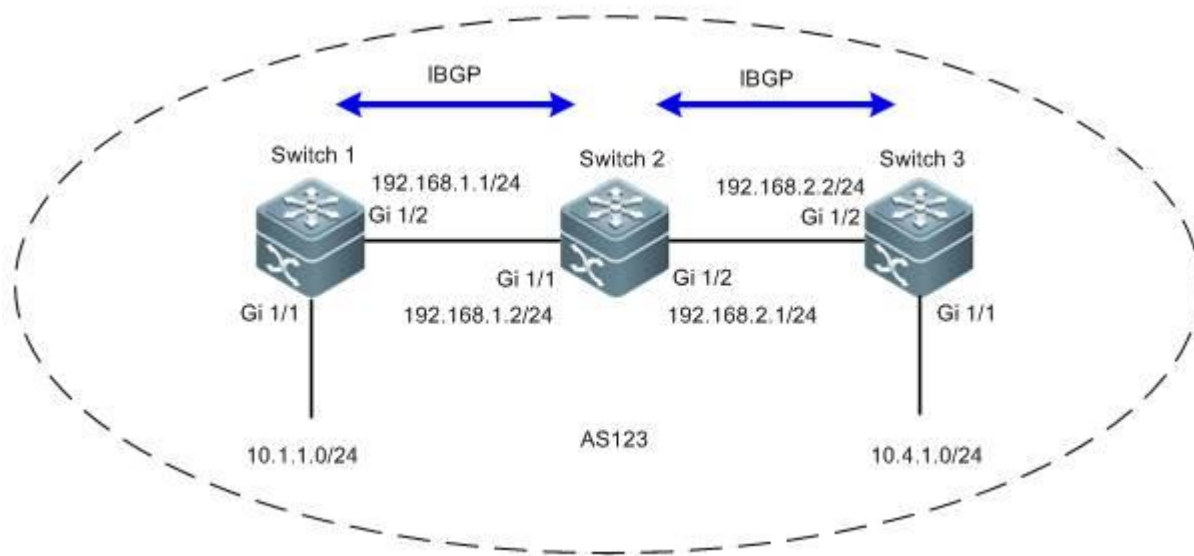
Scenario

External gateway protocols such as the BGP are mainly applied on large-scale networks for the transmission of large-quantity IGP routes. In addition, the BGP flexibly provides some properties for routing control. Major scenarios include networks of telecom operators and secondary or tertiary ISPs, provincial backbone networks of financial industries, and municipal e-government networks. Generally, the BGP is not independently deployed in these scenarios, but is deployed together with the MPLS in BGP + MPLS VPN networking mode. The iBGP is a routing protocol used in BGP connection setup between devices connected to the same AS.

I. Networking Requirements

- Switch 1, Switch 2, and Switch 3 are switches of AS123. Switch 1 and Switch 2 are configured as iBGP neighbors, and Switch 2 and Switch 3 are configured as iBGP neighbors.
- The route information is delivered to the neighbor over the iBGP.

II. Network Topology



III. Configuration Tips

- Determine the source address for BGP neighbor update.

Note:

- If the **eBGP neighbor** is on the edge of the AS, it is recommended that a **direct-connection interface** is used as the update source address. In this case, you do not have to setup an IGP route between the update source addresses.

2) If the **iBGP neighbor** is inside the AS, it is recommended that a **loopback address** be used as the update source address. A loopback address is more reliable (which will not cause BGP neighbor turbulence at a physical circuit failure). Generally, IGP routes between update source addresses are deployed within the AS.

2. The iBGP features horizontal segregation. That is, the route learned from one iBGP neighbor are not delivered to another iBGP neighbor (but will be delivered to an eBGP neighbor).

IV. Configuration Steps

Note:

Rename the devices as SW1, SW2, and SW3 according to the preceding topology and perform the following configurations:

1. Configure the basic IP addresses for the devices on the network.

```
Ruijie(config)#hostname SW1
SW1(config)#interface gigabitEthernet 1/2
SW1(config-if-GigabitEthernet 1/2)#no switchport
SW1(config-if-GigabitEthernet 1/2)#ip address 192.168.1.1 255.255.255.0
SW1(config-if-GigabitEthernet 1/2)#exit
SW1(config)#interface gigabitEthernet 1/1
SW1(config-if-GigabitEthernet 1/1)#no switchport
SW1(config-if-GigabitEthernet 1/1)#ip address 10.1.1.1 255.255.255.0
SW1(config-if-GigabitEthernet 1/1)#exit
SW1(config)#interface loopback 0
SW1(config-if-Loopback 0)#ip address 1.1.1.1 255.255.255.255
SW1(config-if-Loopback 0)#exit

Ruijie(config)#hostname SW2
SW2(config)#interface gigabitEthernet 1/1
SW2(config-if-GigabitEthernet 1/1)#no switchport
SW2(config-if-GigabitEthernet 1/1)#ip address 192.168.1.2 255.255.255.0
SW2(config-if-GigabitEthernet 1/1)#exit
SW2(config)#interface gigabitEthernet 1/2
SW2(config-if-GigabitEthernet 1/2)#no switchport
SW2(config-if-GigabitEthernet 1/2)#ip address 192.168.2.1 255.255.255.0
SW2(config-if-GigabitEthernet 1/2)#exit
SW2(config)#interface loopback 0
SW2(config-if-Loopback 0)#ip address 2.2.2.2 255.255.255.255
SW2(config-if-Loopback 0)#exit

Ruijie(config)#hostname SW3
SW3(config)#interface gigabitEthernet 1/1
SW3(config-if-GigabitEthernet 1/1)#no switchport
SW3(config-if-GigabitEthernet 1/1)#ip address 10.4.1.1 255.255.255.0
SW3(config-if-GigabitEthernet 1/1)#exit
```

```
SW3(config)#interface gigabitEthernet 1/2
SW3(config-if-GigabitEthernet 1/2)#no switchport
SW3(config-if-GigabitEthernet 1/2)#ip address 192.168.2.2 255.255.255.0
SW3(config-if-GigabitEthernet 1/2)#exit
SW3(config)#interface loopback 0
SW3(config-if-Loopback 0)#ip address 3.3.3.3 255.255.255.255
SW3(config-if-Loopback 0)#exit
```

2. Enable OSPF for the entire network and set to notify the corresponding interface to the OSPF process so that the loopback interfaces on the entire network are reachable.

```
SW1(config)#router ospf 1
SW1(config-router)#network 192.168.1.1 0.0.0.255 area 0
SW1(config-router)#network 1.1.1.1 0.0.0.0 area 0
SW1(config-router)#exit

SW2(config)#router ospf 1
SW2(config-router)#network 192.168.1.2 0.0.0.255 area 0
SW2(config-router)#network 2.2.2.2 0.0.0.0 area 0
SW2(config-router)#exit

SW3(config)#router ospf 1
SW3(config-router)#network 192.168.2.2 0.0.0.255 area 0
SW3(config-router)#network 3.3.3.3 0.0.0.0 area 0
SW3(config-router)#exit
```

3. Configure iBGP neighbors.

Note:

- 1) If the BGP neighbor is of the same AS ID, it is created as an iBGP neighbor. If the BGP neighbor is of a different AS ID, it is created as an eBGP neighbor.

```
SW1(config)#router bgp 123
SW1(config-router)#neighbor 2.2.2.2 remote-as 123
SW1(config-router)#neighbor 2.2.2.2 update-source loopback 0
SW1(config-router)#exit

SW2(config)#router bgp 123
SW2(config-router)#neighbor 1.1.1.1 remote-as 123
SW2(config-router)#neighbor 1.1.1.1 update-source loopback 0
SW2(config-router)#neighbor 3.3.3.3 remote-as 123
SW2(config-router)#neighbor 3.3.3.3 update-source loopback 0
```

```
SW2(config-router)#exit

SW3(config)#router bgp 123
SW3(config-router)#neighbor 2.2.2.2 remote-as 123
SW3(config-router)#neighbor 2.2.2.2 update-source loopback 0
SW3(config-router)#exit
```

4. Notify the BGP process about the route information.

Note:

Run the **network** command to notify the BGP process about the routes in the BGP. The command does not enable BGP on these interfaces, which is different from the **rip** and **ospf** commands. The routes conveyed in the **network** command must **exist locally (that is, can be returned by the **show ip route** command) and its mask is consistent with the mask parameter**. Otherwise, the BGP process is not notified.

```
SW1(config)#router bgp 123
SW1(config-router)#network 10.1.1.0 mask 255.255.255.0
SW1(config-router)#exit

SW3(config)#router bgp 123
SW3(config-router)#network 10.4.1.0 mask 255.255.255.0
SW2#show ip route

Codes: C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is no set
O    1.1.1.1/32 [110/1] via 192.168.2.1, 16:07:50, GigabitEthernet 1/1
C    2.2.2.2/32 is local host.
O    3.3.3.3/32 [110/1] via 192.168.2.2, 16:07:50, GigabitEthernet 1/2
B    10.1.1.0/24 [200/0] via 1.1.1.1, 00:10:12
B    10.4.1.0/24 [200/0] via 3.3.3.3, 00:08:44
C    192.168.1.0/24 is directly connected, GigabitEthernet 1/1
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, GigabitEthernet 1/2
C    192.168.2.1/32 is local host.
```

V. Verification

1. Check whether the BGP neighboring relationship is established between routers and the neighbor status. If the BGP neighboring relationship can be established properly and the status is **Established**, the iBGP runs properly.

```
SW2(config)#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 123
BGP table version is 3
1 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 |
|----------|---|-----|---------|---------|--------|-----|------|----------|--------------|
| 1.1.1.1 | 4 | 123 | 15 | 14 | 3 | 0 | 0 | 00:11:20 | 1 |
| 3.3.3.3 | 4 | 123 | 11 | 11 | 3 | 0 | 0 | 00:08:37 | 1 |

```
Total number of neighbors 2
```

2. Check the route of the iBGP neighbor router. If the route delivered by the neighbor can be learned, the iBGP configuration is correct.

Basic eBGP Configuration

```
SW2#show ip route
```

Codes: C - Connected, L - Local, S - Static

R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

IA - Inter area, * - candidate default

Gateway of last resort is no set

```
O    1.1.1.1/32 [110/1] via 192.168.2.1, 16:07:50, GigabitEthernet 1/1
C    2.2.2.2/32 is local host.
O    3.3.3.3/32 [110/1] via 192.168.2.2, 16:07:50, GigabitEthernet 1/2
B    10.1.1.0/24 [200/0] via 1.1.1.1, 00:10:12
B    10.4.1.0/24 [200/0] via 3.3.3.3, 00:08:44
C    192.168.1.0/24 is directly connected, GigabitEthernet 1/1
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, GigabitEthernet 1/2
C    192.168.2.1/32 is local host.
```

2.9.3.4.2 Basic eBGP Configuration

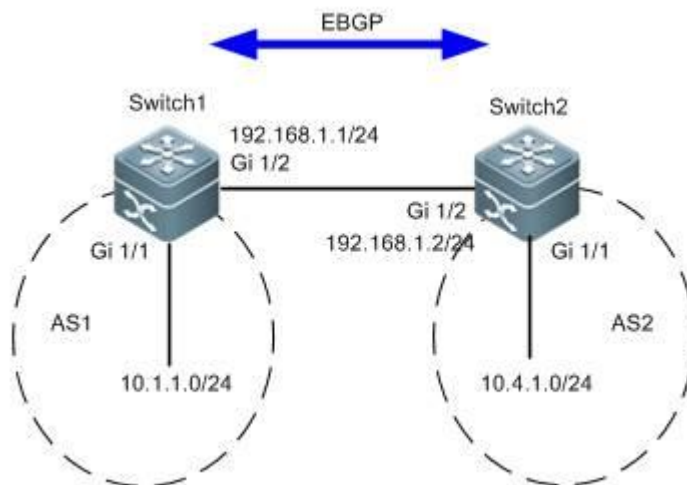
Scenario

External gateway protocols such as the BGP are mainly applied on large-scale networks for the transmission of large-quantity IGP routes. In addition, the BGP flexibly provides some properties for routing control. Major scenarios include networks of telecom operators and secondary or tertiary ISPs, provincial backbone networks of financial industries, and municipal e-government networks. Generally, the BGP is not independently deployed in these scenarios, but is deployed together with the MPLS in BGP + MPLS VPN networking mode. The eBGP is a routing protocol used in BGP connection setup between devices connected to different ASs.

I. Networking Requirements

1. Set Switch 1 to AS 1, Switch 2 to AS 2, and establish eBGP neighboring relationships between Switch 1 and Switch 2.
2. The route information is delivered to the neighbor over the eBGP.

II. Network Topology



III. Configuration Tips

1. Configure the basic IP addresses.
2. Configure eBGP neighbors.
3. Notify the BGP process about the route information.

IV. Configuration Steps

Note:

Rename the devices as SW1 and SW2 according to the preceding topology and perform the following configurations:

1. Configure the basic IP addresses.

```
Ruijie(config)#hostname SW1
```

```
SW1(config)#interface gigabitEthernet 1/2
SW1(config-if-GigabitEthernet 1/2)#no switchport
SW1(config-if-GigabitEthernet 1/2)#ip address 192.168.1.1 255.255.255.0
SW1(config-if-GigabitEthernet 1/2)#exit
SW1(config)#interface gigabitEthernet 1/1
SW1(config-if-GigabitEthernet 1/1)#no switchport
SW1(config-if-GigabitEthernet 1/1)#ip address 10.1.1.1 255.255.255.0
SW1(config-if-GigabitEthernet 1/1)#exit

Ruijie(config)#hostname SW2
SW2(config)#interface gigabitEthernet 1/2
SW2(config-if-GigabitEthernet 1/2)#no switchport
SW2(config-if-GigabitEthernet 1/2)#ip address 192.168.1.2 255.255.255.0
SW2(config-if-GigabitEthernet 1/2)#exit
SW2(config)#interface gigabitEthernet 1/1
SW2(config-if-GigabitEthernet 1/1)#no switchport
SW2(config-if-GigabitEthernet 1/1)#ip address 10.4.1.1 255.255.255.0
SW2(config-if-GigabitEthernet 1/1)#exit
```

2. Configure eBGP neighbors.

Note:

- 1) If the BGP neighbor is of the same AS ID, it is created as an iBGP neighbor. If the BGP neighbor is of a different AS ID, it is created as an eBGP neighbor.

```
SW1(config)#router bgp 1
SW1(config-router)#neighbor 192.168.1.2 remote-as 2
SW1(config-router)#exit

SW2(config)#router bgp 2
SW2(config-router)#neighbor 192.168.1.1 remote-as 1
SW2(config-router)#exit
```

2. Notify the BGP process about the route information.

```
SW1(config)#router bgp 1
SW1(config-router)#network 10.1.1.0 mask 255.255.255.0
SW1(config-router)#exit

SW2(config)#router bgp 2
SW2(config-router)#network 10.4.1.0 mask 255.255.255.0
SW2(config-router)#exit
```

Note:

Run the **network** command to notify the BGP process about the routes in the BGP. The command does not enable BGP on these interfaces, which is different from the **rip** and **ospf** commands. The routes conveyed in the **network** command must exist locally (that is, can be returned by the **show ip route** command) and its mask is consistent with the mask parameter. Otherwise, the BGP process is not notified.

V. Verification

1. Check whether the BGP neighboring relationship is established between routers and the neighbor status. If the BGP neighboring relationship can be established properly and the status is **Established**, the eBGP runs properly.

```
SW2(config)#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 |

```
Total number of neighbors 1
```

3. Check the route of the eBGP neighbor router. If the route delivered by the neighbor can be learned, the eBGP configuration is correct.

```
SW2#show ip route
```

```
Codes: C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - 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, GigabitEthernet 1/1
C    10.4.1.1/32 is local host.
C    192.168.1.0/24 is directly connected, GigabitEthernet 1/2
C    192.168.1.2/32 is local host.
```

2.9.3.4.3 Route Reflector

Scenario

A route reflector is mainly used to solve the horizontal route segregation issue in side an iBGP. (As a switch does not deliver the route received from an iBGP neighbor to another iBGP neighbor, routes are not comprehensively learned and blackholes may result in.) To solve the horizontal segregation issue for the iBGP, iBGP neighbor full mesh must be adopted. However, if a large number of iBGP neighbors are configured in full mesh, the number of iBGP neighbor pairs will increase exponentially. Maintenance of these neighboring information and route information will be very complicated and consume a large volume of device resources. To solve the issue, route reflectors are used. With route reflectors, the number of iBGP peer connections in an AS is reduced. A route reflector is similar to the DR and BDR of the OSPF in a broadcasting environment. It can be deployed to reduce resource consumption in an iBGP network environment with a large number of neighbors in full mesh or to aid the repeated configuration of a large number of iBGP neighbors.

Function Overview

To speed up route information convergence, generally, all BGP speakers in an AS are configured in a full mesh, that is, every two BGP speakers are configured into a neighboring pair. When the AS has a large number of GBP speakers, the BGP speaker resource consumption increases greatly, as well as the configuration task volume and complexity for the network administrator. The network scaling performance is undermined.

A route reflector can effectively reduce the number of iBGP peer connections in an autonomous system (AS). You can set an BGP speaker as a route reflector and classify all iBGP peers in the AS into route reflector clients and non-clients. The rules for implementing the route reflector in an AS include the following:

1. Configure the route reflector and specify its clients. The route reflector and its clients form a group. Connection is established between the route reflector and its clients.
2. A route reflector client in one group does not establish connection with BGP speakers not in the group.
3. Within the AS, set up full-mesh connections between non-client iBGP peers. An pair of non-client iBGP peers can be two route reflectors in one group, a route reflector in one group and a BGP speaker not configured with the route reflector function, and a route reflector in one group and a route reflector in another group.

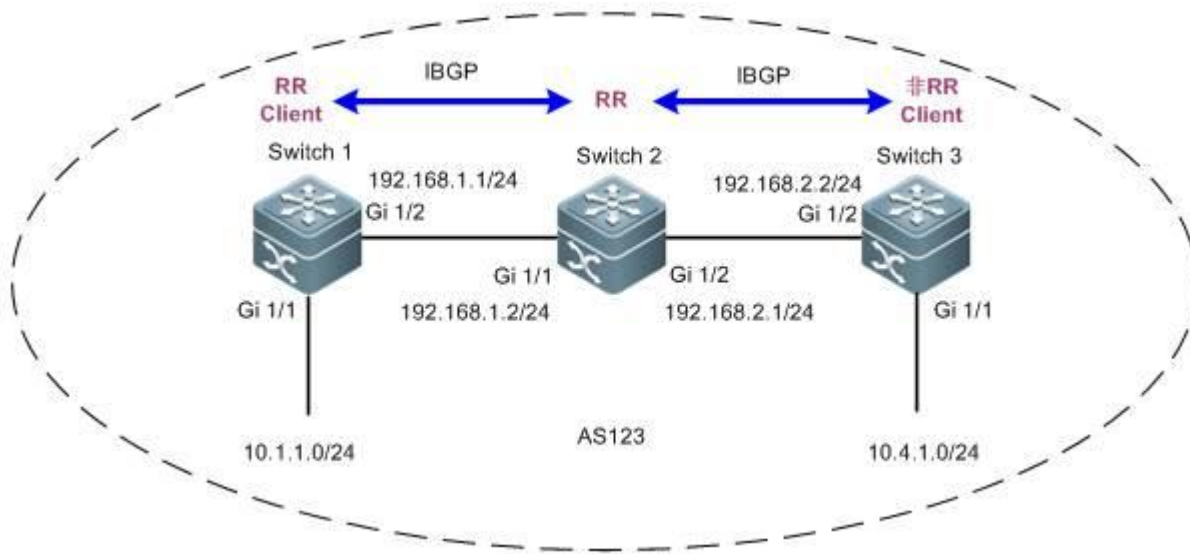
The route received by a route reflector is processed as follows:

1. The route update received from an eBGP speaker is sent to all clients and non-clients.
2. The route update received from a client is sent to all other clients and all clients.
3. The route update received from an iBGP non-client and is sent to all clients.

I. Networking Requirements

As shown in the following topology, due to the horizontal segregation feature of the iBGP, SW1 and SW3 cannot learn BGP routes from each other. The route reflector must be configured to solve the issue.

II. Network Topology



III. Configuration Tips

1. Configure the IP addresses of the routers or switches on the entire network and perform basic iBGP configurations.
2. Configure the route reflector function.

IV. Configuration Steps

1. Configure the IP addresses of the routers on the entire network and perform basic iBGP configurations.

See the section "Basic iBGP Configuration."

2. Configure the route reflector function.

Set SW2 as the route reflector and specify R1 as the route reflector client.

```
SW2(config)#router bgp 123
SW2(config-router)#neighbor 1.1.1.1 route-reflector-client
SW2(config-router)#exit
```

Note:

1. When a switch is configured as a route reflector client, its BGP neighboring relationship no longer exists.
2. A route reflector needs to propagate routes, therefore, it must be provided with chances to learn corresponding iBGP routes.
3. A non-client can reflect routes to a client and vice versa. Clients can reflect routes to clients. **However, routes learned from a non-client cannot be reflected to another non-client.**

V. Verification

Check the routes on the entire network. If SW1 can learn the routes of SW3 and vice versa, the route reflector function is configured correctly.

```
SW1#show ip route
Codes: C - Connected, L - Local, S - Static
```

R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 IA - 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 1/2
O    3.3.3.3/32 [110/2] via 192.168.1.2, 00:07:13, GigabitEthernet 1/2
C    10.1.1.0/24 is directly connected, GigabitEthernet 1/1
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 1/2
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 1/2
```

2.9.3.5 Route Control

2.9.3.5.1 Route Control

ACL and Prefix List

Similarity

Both the ACL and the prefix list can be used to match the route prefix.

Difference

The ACL can be used to filter data packets and match the five elements of IP packets, while the prefix list can be used to match the route prefix only.

Tips for selection

To match the route prefix, use either the ACL or prefix list. To match the route prefix with masks in different lengths in a large network segment, the prefix list is recommended.

Distribute list and route map

Similarity

Both the distribute list and the route map can be used for route filtering.

Difference

1. The distribute list can only filter route entries and cannot modify route properties. The route map can filter route entries as well as modify route properties.
2. The route map can change the next hop of a data packet in force for policy routing.

3. The distribute list can be used in **route protocol redistribution**, **route propagation between Routing Information Protocol (RIP) neighbors** (route filtering is supported because routes are delivered between RIP neighbors), and **route submission to route tables in OSPF areas** (ISAs rather than routes are delivered between OSPF neighbors and ISAs between OSPF neighbor cannot be filtered).

4. The route map can be applied in route protocol redistribution and route propagation between BGP neighbors.

Tips for selection

If the application scenario supports both the distribute list and the route map, use the route map if route properties need to be modified, and use either approach if route property modification is not necessary.

Distribute List

2.9.3.5.2 Distribute List

Scenario

The filter control points are generally deployed on the ABR and ASBR in an OSPF area for route convergence, because these two points are where link state advertisements (LSAs) such as type 3, 4, 5, and 7 LSAs are generated. The common measures include the area range, summary-address, and route-map commands. However, as the LSAs received and sent by common routers in common areas are not controllable, the route learning results are not controllable on these routers. In this case, you can use the distribute list to control route learning and LSA results on these points for on-demand route learning on feature network segments for network administrators.

The distribute list is generally used in an OSPF area, and can also be used on any router (including ABR or ASBR) for route entry filter. The distribute list tool is invoked based on the whole OSPF process rather than the interface.

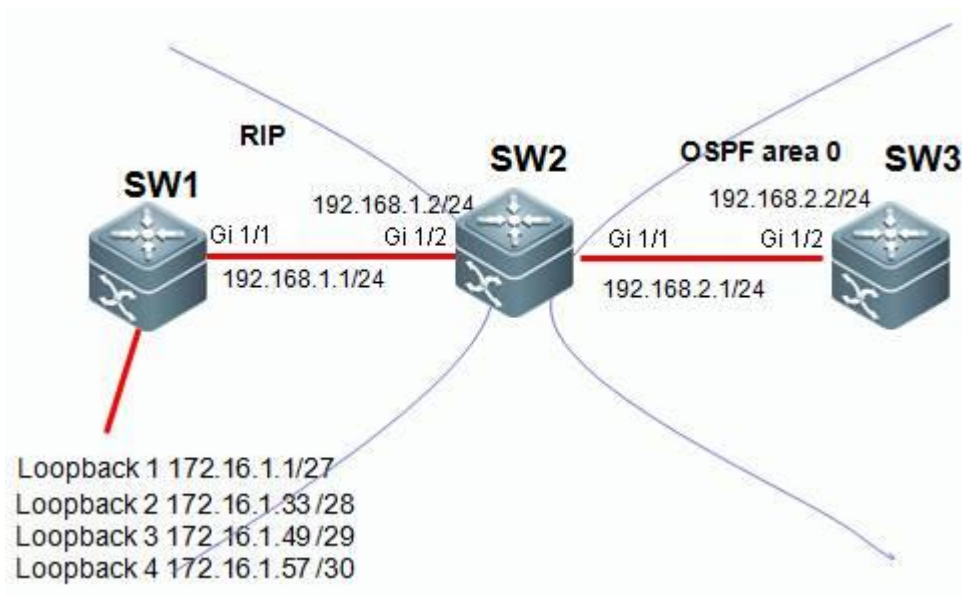
Function Overview

The distribute list tool controls route updates, carries out route entry filter only, and **does not support route property modification**.

I. Networking Requirements

On SW2, redistribute the RIP routes to the OSPF area and implement route filter on redistribution to allow only routes 172.16.1.32/28, 172.16.1.48/29, and 172.16.1.56/30 be redistributed to the OSPF area.

II. Network Topology



III. Configuration Tips

1. Configure the basic IP addresses.
2. On SW1 and SW2, enable the RIP and propagate the corresponding interface to the RIP process.
3. On SW2 and SW3, enable the OSPF and propagate the corresponding interface to the OSPF process.
4. On SW2, redistribute the route learned over RIP to the OSPF area.
5. Match the routes to be learned through the ACL or prefix list.
6. On SW2, redistribute the route learned over RIP to the OSPF area and filter the routes using the distribute list tool.

III. Configuration Steps

1. Configure the basic IP addresses.

```
Ruijie(config)#hostname SW1
SW1(config)#interface GigabitEthernet 1/1
SW1(config-if-GigabitEthernet 1/1)#no switchport
SW1(config-if-GigabitEthernet 1/1)#ip address 192.168.1.1 255.255.255.0
SW1(config-if-GigabitEthernet 1/1)#exit
SW1(config)#interface loopback 1
SW1(config-if-Loopback 1)#ip address 172.16.1.1 255.255.255.224
SW1(config-if-Loopback 1)#exit
SW1(config)#interface loopback 2
SW1(config-if-Loopback 2)#ip address 172.16.1.33 255.255.255.240
SW1(config-if-Loopback 2)#exit
SW1(config)#interface loopback 3
SW1(config-if-Loopback 3)#ip address 172.16.1.49 255.255.255.248
```

```
SW1(config-if-Loopback 3)#exit
SW1(config)#interface loopback 4
SW1(config-if-Loopback 4)#ip address 172.16.1.57 255.255.255.252
SW1(config-if-Loopback 4)#exit

Ruijie(config)#hostname SW2
SW2(config)#interface GigabitEthernet 1/2
SW2(config-if-GigabitEthernet 1/2)#no switchport
SW2(config-if-GigabitEthernet 1/2)#ip address 192.168.1.2 255.255.255.0
SW2(config-if-GigabitEthernet 1/2)#exit
SW2(config)#interface GigabitEthernet 1/1
SW2(config-if-GigabitEthernet 1/1)#no switchport
SW2(config-if-GigabitEthernet 1/1)#ip address 192.168.2.1 255.255.255.0
SW2(config-if-GigabitEthernet 1/1)#exit

Ruijie(config)#hostname SW3
SW3(config)#interface GigabitEthernet 1/2
SW3(config-if-GigabitEthernet 1/2)#no switchport
SW3(config-if-GigabitEthernet 1/2)#ip address 192.168.2.2 255.255.255.0
SW3(config-if-GigabitEthernet 1/2)#exit
```

2. On SW1 and SW2, enable the RIP and propagate the corresponding interface to the RIP process.

```
SW1(config)#router rip
SW1(config-router)#version 2
SW1(config-router)#no auto-summary
SW1(config-router)#network 172.16.0.0
SW1(config-router)#network 192.168.1.0
SW1(config-router)#exit

SW2(config)#router rip
SW2(config-router)#version 2
SW2(config-router)#no auto-summary
SW2(config-router)#network 192.168.1.0
SW2(config-router)#exit
```

3. On SW2 and SW3, enable the OSPF and propagate the corresponding interface to the OSPF process.

```
SW2(config)#router ospf 1
SW2(config-router)#network 192.168.2.1 0.0.0.0 area 0
SW2(config-router)#exit
```

```
SW3(config)#router ospf 1
SW3(config-router)#network 192.168.2.2 0.0.0.0 area 0
SW3(config-router)#exit
```

4. On SW2, redistribute the route learned over RIP to the OSPF area.

```
SW2(config)#router ospf 1
SW2(config-router)#redistribute rip subnets
SW2(config-router)#exit
```

5. Match the routes to be learned through the ACL or prefix list.

Note:

- 1) The tools for matching route entries include the ACL and the prefix list. **Choose one of the tools.**

```
SW2(config)#ip access-list standard 1
SW2(config-std-nacl)#10 permit 172.16.1.32 0.0.0.0
SW2(config-std-nacl)#20 permit 172.16.1.48 0.0.0.0
SW2(config-std-nacl)#30 permit 172.16.1.56 0.0.0.0
SW2(config-std-nacl)#exit
```

- 2) To match the route prefix with masks in different lengths in a large network segment, the prefix list is recommended. You can also use the ACL, which requires a few more entries to be written.

For example, to match route entries 172.16.1.32/27, 172.16.1.48/28, and 172.16.1.56/29, the ACL approach requires you to write three access control entries (ACEs) while the prefix list tool requires you to write only one entry.

- 1) Use the ACL to match route entries.

Note:

In this example, the ACL matches the route entries. Therefore, you can use the mask 0.0.0.0 to exactly match the corresponding route entries.

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

Note:

- a. The prefix list matches route entries only and does not filter data packets.
- b. The prefix list matches the subnet of a network segment. **ge** indicates the minimal number of bits and **le** indicates the maximal number of bits.
- c. The prefix list is matched from top to bottom with the last one being an implicit **deny any** entry.

```
SW2(config)#ip prefix-list ruijie seq 10 permit 172.16.1.0/24 ge 28 le 30
```

----->Define a prefix list ruijie to match route entries whose prefix is 172.16.1.0/24 and subnet mask equals or is greater than 28 and equals or is smaller than 30.

6. On SW2, redistribute the route learned over RIP to the OSPF area and filter the routes using the distribute list tool.

Note:

1. The distribute list filters route entries matched by the ACL or prefix list. That is, the ACL and prefix list determine which route entries are filtered.
2. The distribute list can be used in **route protocol redistribution**, **route propagation between Routing Information Protocol (RIP) neighbors** (route filtering is supported because routes are delivered between RIP neighbors), and **route submission to route tables in OSPF** (ISAs rather than routes are delivered between OSPF neighbors and ISAs between OSPF neighbors cannot be filtered).

The following describes how the distribute list uses the ACL and the prefix list with examples respectively.

1. The distribute list invokes the ACL for route filtering.

```
SW2(config)#router ospf 1
SW2(config-router)#distribute-list 1 out rip
SW2(config-router)#exit
```

2. The distribute list invokes the prefix list for route filtering.

```
SW2(config)#router ospf 1
SW2(config-router)#distribute-list prefix ruijie out rip
SW2(config-router)#exit
```

Supplements:

1. To filter route entries delivered between RIP neighbors by using the distribute list, run the following command:

```
SW2(config)#router rip
SW2(config-router)#distribute-list 1 in GigabitEthernet 1/2---->1 indicates the ACL 1. You can also use the prefix list. in indicates a route entry learned from a neighbor. out indicates a route entry delivered to a neighbor. You can also add the specific interface.
```

2. To filter route entries delivered to the route table in OSPF by using the distribute list, run the following command:

```
SW2(config)#router ospf 1
SW2(config-router)#distribute-list 1 in---->1 indicates the ACL 1. You can also use the prefix list. The direction must be set to in.
```

V. Verification

Check the route entries on SW3. If the route entries learned by SW3 include 172.16.1.32/28, 172.16.1.48/29, and 172.16.1.56/30, the distribute list is configured correctly.

```
SW3#show ip route
```

Codes: C - Connected, L - Local, S - Static
 R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 IA - 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, GigabitEthernet 1/2

O E2 172.16.1.48/29 [110/20] via 192.168.2.1, 00:02:29, GigabitEthernet 1/2

O E2 172.16.1.56/30 [110/20] via 192.168.2.1, 00:02:21, GigabitEthernet 1/2

C 192.168.2.0/24 is directly connected, GigabitEthernet 1/2

C 192.168.2.2/32 is local host.

2.9.3.5.3 Route Map

Scenario

To run a dynamic route protocol, such as the OSPF, on your network, you need to redistribute external routes, such as static routes, RIP routes, and BGP routes to the OSPF area on an ASBR. In this case, you may want to filter out desired route entries or redistribute routes with special requirements through route control and filter, or you may want to modify some properties of the external route entries when being redistributed into an OSPF area, for example, the metric value, next hop, and metric type (O E1, E2, O N1, or N2), and add special tags to some route entries so that a downstream router may perform route selection based on these tags accordingly. The route map is recommended for these application scenarios.

To run a dynamic route protocol, such as the BGP, on your network, route exchange and learning between BGP peers are necessary, or external routes, such as static routes, RIP routes, and OSPF routes may need be redistributed into the BGP area. In this case, you may want to learn or delivery only desired route entries through route control and filter. In this case, the route map is recommended for route redistribution.

You may want to modify some properties, such as the metric, value, next hop, local preference, MED value, and AS path of the route entries when they are learned or delivered to BGP peers or redistributed into the BGP area as external routes, or tag some route entries so that a downstream router may perform route selection based on these tags accordingly. The route map is recommended for these application scenarios.

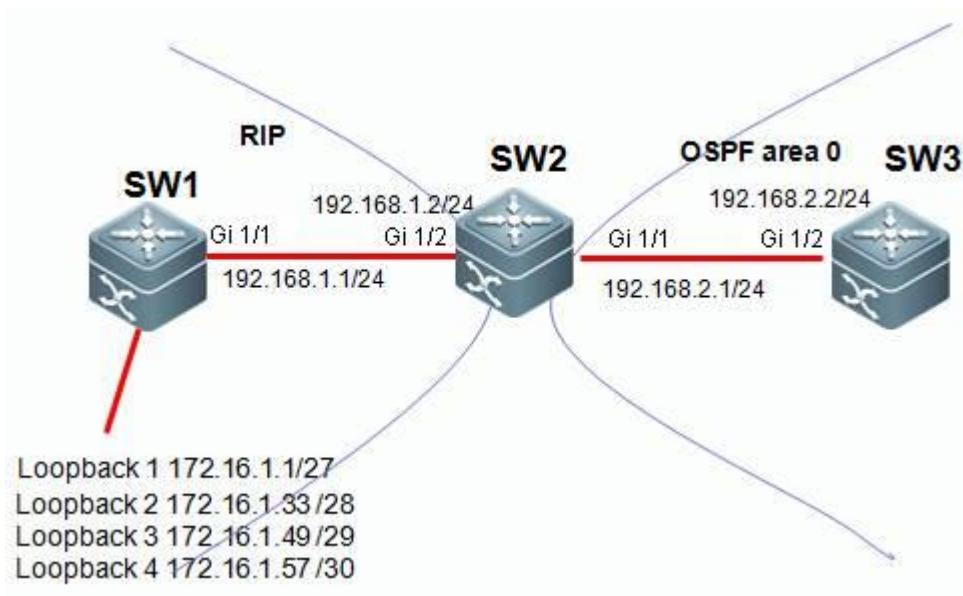
Function Overview

You can control route update and **modify route properties** using the route map tool.

I. Networking Requirements

On SW2, redistribute the RIP routes to the OSPF area and implement route filter on redistribution to allow only routes 172.16.1.32/28, 172.16.1.48/29, and 172.16.1.56/30 be redistributed to the OSPF area. The external routes to be redistributed into the OSPF area are of route type **OE1** and metric value **50**.

II. Network Topology



III. Configuration Tips

1. Configure the basic IP addresses.
2. On SW1 and SW2, enable the RIP and propagate the corresponding interface to the RIP process.
3. On SW2 and SW3, enable the OSPF and propagate the corresponding interface to the OSPF process.
4. On SW2, redistribute the route learned over RIP to the OSPF area.
5. Match the routes to be learned through the ACL or prefix list.
6. Configure the route map.
7. On SW2, redistribute RIP routes into the OSPF area and invoke the route map for route control.

III. Configuration Steps

1. Configure the basic IP addresses.

```
Ruijie(config)#hostname SW1
SW1(config)#interface GigabitEthernet 1/1
SW1(config-if-GigabitEthernet 1/1)#no switchport
SW1(config-if-GigabitEthernet 1/1)#ip address 192.168.1.1 255.255.255.0
SW1(config-if-GigabitEthernet 1/1)#exit
SW1(config)#interface loopback 1
SW1(config-if-Loopback 1)#ip address 172.16.1.1 255.255.255.224
SW1(config-if-Loopback 1)#exit
SW1(config)#interface loopback 2
SW1(config-if-Loopback 2)#ip address 172.16.1.33 255.255.255.240
SW1(config-if-Loopback 2)#exit
SW1(config)#interface loopback 3
SW1(config-if-Loopback 3)#ip address 172.16.1.49 255.255.255.248
```

```
SW1(config-if-Loopback 3)#exit
SW1(config)#interface loopback 4
SW1(config-if-Loopback 4)#ip address 172.16.1.57 255.255.255.252
SW1(config-if-Loopback 4)#exit

Ruijie(config)#hostname SW2
SW2(config)#interface GigabitEthernet 1/2
SW2(config-if-GigabitEthernet 1/2)#no switchport
SW2(config-if-GigabitEthernet 1/2)#ip address 192.168.1.2 255.255.255.0
SW2(config-if-GigabitEthernet 1/2)#exit
SW2(config)#interface GigabitEthernet 1/1
SW2(config-if-GigabitEthernet 1/1)#no switchport
SW2(config-if-GigabitEthernet 1/1)#ip address 192.168.2.1 255.255.255.0
SW2(config-if-GigabitEthernet 1/1)#exit

Ruijie(config)#hostname SW3
SW3(config)#interface GigabitEthernet 1/2
SW3(config-if-GigabitEthernet 1/2)#no switchport
SW3(config-if-GigabitEthernet 1/2)#ip address 192.168.2.2 255.255.255.0
SW3(config-if-GigabitEthernet 1/2)#exit
```

2. On SW1 and SW2, enable the RIP and propagate the corresponding interface to the RIP process.

```
SW1(config)#router rip
SW1(config-router)#version 2
SW1(config-router)#no auto-summary
SW1(config-router)#network 172.16.0.0
SW1(config-router)#network 192.168.1.0
SW1(config-router)#exit

SW2(config)#router rip
SW2(config-router)#version 2
SW2(config-router)#no auto-summary
SW2(config-router)#network 192.168.1.0
SW2(config-router)#exit
```

3. On SW2 and SW3, enable the OSPF and propagate the corresponding interface to the OSPF process.

```
SW2(config)#router ospf 1
SW2(config-router)#network 192.168.2.1 0.0.0.0 area 0
```

```
SW2(config-router)#exit

SW3(config)#router ospf 1
SW3(config-router)#network 192.168.2.2 0.0.0.0 area 0
SW3(config-router)#exit
```

4. On SW2, redistribute the route learned over RIP to the OSPF area.

```
SW2(config)#router ospf 1
SW2(config-router)#redistribute rip subnets
SW2(config-router)#exit
```

5. Match the routes to be learned through the ACL or prefix list.

Note:

- 1) The tools for matching route entries include the ACL and the prefix list. **Choose one of the tools.**

```
SW2(config)#ip access-list standard 1
SW2(config-std-nacl)#10 permit 172.16.1.32 0.0.0.0
SW2(config-std-nacl)#20 permit 172.16.1.48 0.0.0.0
SW2(config-std-nacl)#30 permit 172.16.1.56 0.0.0.0
SW2(config-std-nacl)#exit
```

2) To match the sub-routes of one network segment, the prefix list offers more convenience than the ACL. You can also use the ACL, which requires a few more entries to be written.

For example, to match route entries 172.16.1.32/27, 172.16.1.48/28, and 172.16.1.56/29, the ACL approach requires you to write three access control entries (ACEs) while the prefix list tool requires you to write only one entry.

- 1) Use the ACL to match route entries.

Note:

In this example, the ACL matches the route entries. Therefore, you can use the mask 0.0.0.0 to exactly match the corresponding route entries.

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

Note:

- a. The prefix list matches route entries only and does not filter data packets.
 - b. The prefix list matches the subnet of a network segment. **ge** indicates the minimal number of bits and **le** indicates the maximal number of bits.
3. The prefix list matches routes from top to bottom, which is the same as the ACL.

```
SW2(config)#ip prefix-list ruijie seq 10 permit 172.16.1.0/24 ge 28 le 30
```

----->Define a prefix list ruijie to match route entries whose prefix is 172.16.1.0/24 and subnet mask equals or is greater than 28 and equals or is smaller than 30.

6. Configure the route map.

Note:

- a. The route map can be used for route filter and route property modification.
- b. The route map can match routes with more conditions than the distribute list. The route map supports the match of route entries, metric values, metric types, and so on, while the distribute list matches only route entries.
3. The route map is executed from top to bottom **with the last one being an implicit deny any entry.**
4. The route map execution logics are as follows:

```
route-map aaa permit 10
    match x y z
    match a
    set b
    set c
route-map aaa permit 20
    match p
    match q
    set r
```

----->Multiple match conditions listed from left to right indicate "or", that is, that once one condition is matched, the whole statement is matched.

----->Multiple set statements listed from top to bottom indicate that these set actions are executed simultaneously.

----->Multiple match conditions listed from top to bottom indicate "and", that is, that only all conditions are met, the whole statement is matched.

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

The execution logics are as follows:

```
If (x or y or z)
    then set ( b and c )
else if ( p and q )
    then set r
else deny
```

The match ip address statement in the route map can match the ACL or the prefix list. Choose either of the two methods. See the following examples:

1. Using the ACL in the match ip address statement

```
SW2(config)#route-map aaa permit 10
SW2(config-route-map)#match ip address 1
SW2(config-route-map)#set metric-type type-1
```

```
SW2(config-route-map)#set metric 50
SW2(config-route-map)#exit
```

2. Using the prefix list in the match ip address statement

```
SW2(config)#route-map aaa permit 10
SW2(config-route-map)#match ip address prefix-list ruijie
SW2(config-route-map)#set metric-type type-1
SW2(config-route-map)#set metric 50
SW2(config-route-map)#exit
```

7. On SW2, redistribute RIP routes into the OSPF area and invoke the route map for route control.

Note:

```
SW2(config)#router ospf 1
SW2(config-router)#redistribute rip subnets route-map aaa
SW2(config-router)#exit
```

Supplements:

The configuration command for invoking the route map on a BGP neighbor is as follows:

```
SW2(config)#router bgp 1
SW2(config-router)#neighbor 10.1.1.1 route-map aaa in----->in indicates controlling routes learned from the BGP
neighbor and out indicates controlling routes propagated to the BGP neighbor. (To implement route control on a BGP
neighbor using the route map, soft delete the routes of the BGP to make the configurations take effect after the route
map is configured. Do not perform the operation at service peaks.)
```

V. Verification

Check the route entries on SW3. If SW3 has learned route entries 172.16.1.32/28, 172.16.1.48/29, 172.16.1.56/30 of OE1 and the internal costs are covered, the route map is configured correctly for route control.

```
SW3#show ip route
Codes: C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - 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, GigabitEthernet 1/2
O E1 172.16.1.48/29 [110/51] via 192.168.2.1, 00:03:14, GigabitEthernet 1/2
```

```
O E1 172.16.1.56/30 [110/51] via 192.168.2.1, 00:03:14, GigabitEthernet 1/2
C      192.168.2.0/24 is directly connected, GigabitEthernet 1/2
C      192.168.2.2/32 is local host.
```

2.9.3.6 Policy Routing

Scenario

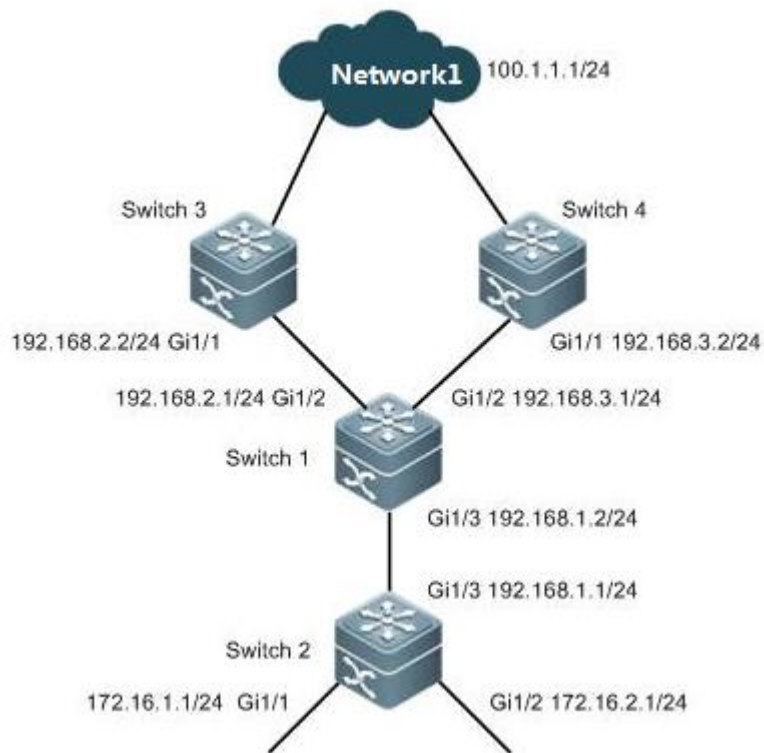
If there are multiple interconnected links between the convergence and core devices or between the core and egress routers on your network, a common route table may not satisfy the load or redundancy requirement; or, new route access requirements emerge with deployment of new services on the network, and you do not want to adjust the complicated OSPF route control and selection policies previously planned, you can use the policy routing technology to arrange new route selection for the new requirements. You can choose a designated link to forward data rather than using the traditional route table.

The policy routing technology is also recommended for another common application scenario: There are multiple routers or firewalls between the core devices and the network egress devices. They corresponds to links of different ISPs, for example, China Telecom (100M), China Unicom (50M), and CERNET (1G). You may want to distribute your Intranet traffic to the three links based on the link load and bandwidth usage, for example, distribute the traffic of teaching buildings, research institutions, and office buildings to the CERNET egress, the traffic of the library, audio-visual education center, and administration building to the China Unicom egress, and all other traffic (for example, traffic of student dormitories) to the China Telecom egress. In addition, data traffic accessing CERNET resources is distributed to the CERNET egress. Traffic is distributed based on the service type. The Telecom, Unicom, and CERNET links serve as a backup link of each other at link failure.

I. Networking Requirements

As shown in the following topology, there are two egress switches, Switch 3 and Switch 4, between Switch 1 and the Internet. Distribute the Internet access traffic from the Intranet 172.16.1.0/24 to Switch 3 and the Internet access traffic from the Intranet 172.16.2.0/24 to Switch 4.

II. Network Topology



III. Configuration Tips

1. Configure the basic IP addresses.
2. Configure the basic IP routes to enable full reachability through the entire network.
3. On Switch 1, configure the ACL to match the Intranet traffic.
4. Configure the policy routing.
5. Apply policy routing.

IV. Configuration Steps

1. Configure the basic IP addresses.

```
Ruijie(config)#hostname SW1
SW1(config)#interface gigabitEthernet 1/3
SW1(config-if-GigabitEthernet 1/3)#no switchport
SW1(config-if-GigabitEthernet 1/3)#ip address 192.168.1.1 255.255.255.0
SW1(config-if-GigabitEthernet 1/3)#exit
SW1(config)#interface gigabitEthernet 1/2
SW1(config-if-GigabitEthernet 1/2)#no switchport
SW1(config-if-GigabitEthernet 1/2)#ip address 192.168.2.1 255.255.255.0
SW1(config-if-GigabitEthernet 1/2)#exit
SW1(config)#interface gigabitEthernet1/2
SW1(config-if-GigabitEthernet 1/2)#no switchport
```

```
SW1(config-if-GigabitEthernet 1/2)#ip address 192.168.3.1 255.255.255.0
SW1(config-if-GigabitEthernet 1/2)#exit

Ruijie(config)#hostname SW2
SW2(config)#interface gigabitEthernet 1/3
SW1(config-if-GigabitEthernet 1/3)#no switchport
SW2(config-if-GigabitEthernet 1/3)#ip address 192.168.1.2 255.255.255.0
SW2(config-if-GigabitEthernet 1/3)#exit
SW2(config)#interface gigabitEthernet 1/1
SW2(config-if-GigabitEthernet 1/1)#no switchport
SW2(config-if-GigabitEthernet 1/1)#ip address 172.16.1.1 255.255.255.0
SW2(config-if-GigabitEthernet 1/1)#exit
SW2(config)#interface gigabitEthernet 1/2
SW2(config-if-GigabitEthernet 1/2)#no switchport
SW2(config-if-GigabitEthernet 1/2)#ip address 172.16.2.1 255.255.255.0
SW2(config-if-GigabitEthernet 1/2)#exit

Ruijie(config)#hostname SW3
SW3(config)#interface gigabitEthernet 1/1
SW3(config-if-GigabitEthernet 1/1)#no switchport
SW3(config-if-GigabitEthernet 1/1)#ip address 192.168.2.2 255.255.255.0
SW3(config-if-GigabitEthernet 1/1)#exit

Ruijie(config)#hostname SW4
SW4(config)#interface gigabitEthernet 1/1
SW4(config-if-GigabitEthernet 1/1)#no switchport
SW4(config-if-GigabitEthernet 1/1)#ip address 192.168.3.2 255.255.255.0
SW4(config-if-GigabitEthernet 1/1)#exit
```

2. Configure the basic IP routes to enable full reachability through the entire network.

```
SW1(config)#ip route 172.16.0.0 255.255.0.0 192.168.1.2
SW2(config)#ip route 100.1.1.0 255.255.255.0 192.168.1.1
SW3(config)#ip route 172.16.0.0 255.255.0.0 192.168.2.1
SW4(config)#ip route 172.16.0.0 255.255.0.0 192.168.3.1
```

3. On Switch 1, configure the ACL to match the Intranet traffic.

```
SW1(config)#ip access-list standard 10
SW1(config-std-nacl)#10 permit 172.16.1.0 0.0.0.255
SW1(config-std-nacl)#exit
SW1(config)#ip access-list standard 20
```

```
SW1(config-std-nacl)#10 permit 172.16.2.0 0.0.0.255
SW1(config-std-nacl)#exit
```

4. Configure the policy routing.

```
SW1(config)#route-map ruijie permit 10
SW1(config-route-map)#match ip address 10
SW1(config-route-map)#set ip next-hop 192.168.2.2
SW1(config-route-map)#exit
SW1(config)#route-map ruijie permit 20
SW1(config-route-map)#match ip address 20
SW1(config-route-map)#set ip next-hop 192.168.3.2
SW1(config-route-map)#exit
```

Note:

1. The route map executes policy matching from top to bottom. When the data traffic matches a policy, it is forwarded based on the matched policy and is not longer matched to the follow-up policies.
2. The route map has a **deny any** statement on the bottom, which **enables normal IP route forwarding** for data traffic that does **not match any policies** and avoids discarding such Intranet traffic.
3. The set ip next-hop statement allows you to set the IP address of the next hop or the egress interface of the data packet. The IP address of the next hop is recommended.

5. Apply policy routing.

```
SW1(config)#interface gigabitEthernet 1/3
SW1(config-if-GigabitEthernet 1/3)#ip policy route-map ruijie
SW1(config-if-GigabitEthernet 1/3)#exit
```

Note:

Policy routing must be applied on the **in** direction interface of the data packets, not the interface in the **out** direction. This is because policy routing sets the next hop of the data packet in force when it passes through the router. As the router has completed IP route modification on the data packet on the interface in the out direction, the data packet is sent from the interface directly and policy routing applied on the out direction does not take effect.

V. Verification

Perform route tracking with data packets destined for the Internet 100.1.1.0/24 with source addresses on SW2. If the data packet sourced from 172.16.1.0/24 reaches the Internet through R3 and the data packet sourced from 172.16.2.0/24 reaches the Internet through Switch 4, policy routing is configured correctly.

```
SW2#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
```

```
SW2#traceroute 100.1.1.1 source 172.16.2.1
```

```
< press Ctrl+C to break >
```

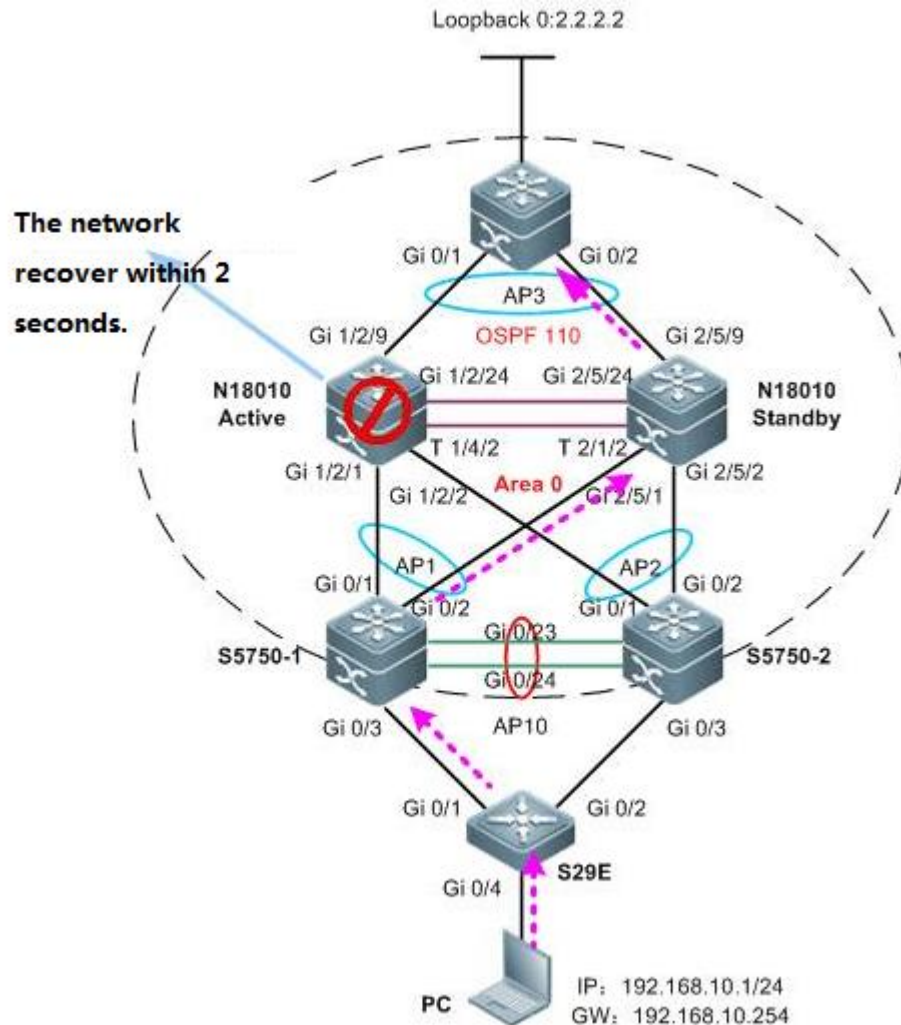
```
Tracing the route to 100.1.1.1
```

```
1    192.168.1.1 0 msec 0 msec 0 msec
2    192.168.3.2 10 msec 0 msec 10 msec
```

2.9.3.7 GR

Scenario

The Graceful Restart (GR) mechanism is suitable for the following application scenario: The core switch N18010 is equipped with two main control engines, or two N18010s are deployed to form a virtual switching unit (VSU). The switch interconnects with neighboring devices (such as convergence device 5750E over the convergence AP port) in double links. The dynamic routing protocol (such as OSPF or BGP) is enabled for routing interactions with neighboring devices. In such a scenario, the GR function is strongly recommended. If services are switched to the backup engine on the failure of the active engine, or services are switched to the backup switch on the failure of the active switch in the VSU, the GR function ensures that the OSPF and BGP route entries are retained on the switch and its neighbors and that only the neighboring relationship reconvergence is established. In this way, data are forwarded without stop. (One data packet may be lost during the process, determined by the actual test environment.)



Function Overview

Development background

1. To support non-stop forwarding in a distributed architecture, the control plane must be separated from the data plane.
2. Route computing and table entry issuing are performed on the control plane while the data plane forwards data according to the forwarding entries issued by the control plane.
3. During active/standby engine switchover, the data plane information on the backup engine enables it to quickly take over data forwarding tasks on the active engine. However, as the backup engine does not have the control plane information (for example, the dynamic routing database and neighboring relationship information), its neighboring devices will detect a dynamic routing protocol interrupt on the switch and thereby start dynamic route reconvergence. In this way, a routing backhole or routing bypass may result in on the entire network.
4. The dynamic route convergence period is in minute grade and does not satisfy the non-stop forwarding requirement.

Working principle

The purpose of the GR technology is to carry out non-stop forwarding during routing protocol restart. The GR mechanism retains the route forwarding entries on the dynamic routing neighbors during active/standby switchover of the management board and updates entries after the new neighboring negotiation convergence completes. This approach keeps the network topology stable, retains the forwarding table, and ensures service continuity.

Two roles of GR

Restarter: executes the GR function.

Helper: A neighboring device of the restarter. It helps the restarter to complete GR.

Configuration

Note: GR is enabled on the N18010 switch by default. If GR is disabled, enable the function as follows:

1. For RIP configuration, configure the GR Restarter on the local end. You do not have to configure the neighboring devices, as the RIP supports GR Helper.

```
Ruijie(config)#router rip
Ruijie(config-router)#graceful-restart
```

2. For OSPF configuration, configure the GR Restarter on the local end, and configure the GR Helper on neighboring devices. (The GR Helper function is enabled on Ruijie devices by default. The function is enabled on most devices of other vendors. You are recommended to read the corresponding configuration manual and make sure the function is enabled.)

```
Ruijie(config)#router ospf 1
Ruijie(config-router)#graceful-restart
```

3. For BGP configuration, configure the GR Restarter on both the local end and the neighboring devices.

```
Ruijie(config)#router bgp 1
Ruijie(config-router)#bgp graceful-restart
```

4. For LDP configuration, configure the GR Restarter on the local end, and configure the GR Helper on neighboring devices. (The GR Helper function is enabled on Ruijie devices by default. The function is enabled on most devices of other vendors. You are recommended to read the corresponding configuration manual and make sure the function is enabled.)

```
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#graceful-restart
```

2.9.4 IPv6

2.9.4.1 IPv6 Stateless Auto Configuration

Scenario

Stateless Auto Configuration is an important feature offered by the IPv6 protocol. It allows the various devices attached to an IPv6 network to connect to the Internet using the Stateless Auto Configuration without requiring any intermediate IP support in the form of a Dynamic Host Configuration Protocol (DHCP) server.

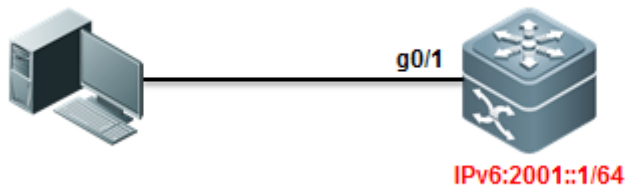
With IPv6, a device on the link advertises any global prefixes in Router Advertisement (RA) messages, as well as its willingness to function as a default device for the link. RA messages are sent periodically and in response to device solicitation messages, which are sent by hosts at system startup.

A node on the link can automatically configure global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages.

I. Requirements

Use stateless auto configuration to assign IPv6 prefix(64 bits) and use EUI-64 to assign IPv6 interface identifier(64 bits).

II. Network Topology



III. Configuration Tips

1. Enable IPv6 on Core switch and configure stateless autoconfiguration.
2. Enable RA (Router Advertisement) on Core switch.

IV. Configuration Steps

1. Enable IPv6 Routing:

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#ipv6 unicast-routing
Ruijie(config)#end
```

----->enable IPv6 Routing

2. Assign IPv6 address to interface and enable RA

```
Ruijie#conf t
```

```

Ruijie(config)#
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#no switchport
Ruijie(config-if-GigabitEthernet 0/1)#ipv6 address 2001::1/64      ----->assign IPv6 address
Ruijie(config-if-GigabitEthernet 0/1)#ipv6 enable                ----->enable IPv6
Ruijie(config-if-GigabitEthernet 0/1)#no ipv6 nd suppress-ra     ----->enable RA
Ruijie(config-if-GigabitEthernet 0/1)#end
Ruijie#wr

```

V. Verification

How to verify NIC status on a station

```

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter {GUID}:

    Connection-specific DNS Suffix . . . : 
    IPv6 Address . . . . . : 2001:1::143d:d208:1a79:fe4e
    IPv6 Temporary Address . . . . . : 2001:1::41a4:149a:b360:f94e
    Link-local IPv6 Address . . . . . : fe80::143d:d208:1a79:fe4e%1
    IPv4 Address. . . . . : 169.254.254.78
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : fe80::2d0:f8ff:fe37:1931%12

```

Note: System creates one more random IPv6 temporary address after enabling IPv6.

We suggest you to disable this feature in order to control user unique ID and reduce network consumption etc.

Following sample shows how to disable temporary address :

run->cmd->netsh->int ipv6->set privacy state=disable

```

C:\Users\Administrator>netsh
netsh>int ipv6
netsh interface ipv6>set privacy state=disable
Ok.

netsh interface ipv6>exit

C:\Users\Administrator>

```

For more information about IPv6 temporary address , see <http://technet.microsoft.com/zh-cn/magazine/2007.08.cableguy.aspx>

2.9.4.2 IPv6 Stateful Auto Configuration

2.9.4.2.1 DHCPv6 Server

Scenario

Stateful auto Configuration is the IPv6 equivalent of DHCP. A new protocol, called DHCPv6 (and based closely on DHCP), is used to pass out addressing and service information in the same way that DHCP is used in IPv4. This is called "stateful" because the DHCP server and the client must both maintain state information to keep addresses from conflicting, to handle leases, and to renew addresses over time.

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is carried in client identifier and server identifier options. The DUID is unique across all DHCP clients and servers, and it is stable for any specific client or server. DHCPv6 uses DUIDs based on link-layer addresses for both the client and server identifier. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device.

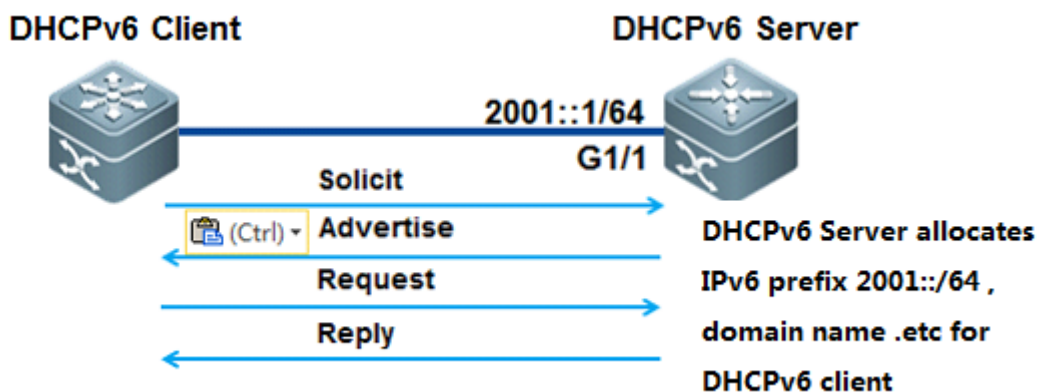
When a DHCPv6 client requests two prefixes with the same DUID but with different IAIDs on two different interfaces, these prefixes are considered to be for two different clients, and the interface information is maintained for both.

I. Requirements

Switch acts as DHCPv6 client and acquires from DHCPv6 Server for IPv6 prefix, DNS, and domain name.

Note: If station wants to acquire a IPv6 address from a DHCPv6 Server, it must be running DHCPv6 client
So far Windows 7, VISTA and Windows Server 2008 have built-in DHCPv6 client, but Windows XP and Windows Server 2003 don't, so you must install additional DHCPv6 client.

II. Network Topology



III. Configuration Tips

1. Configure switch as DHCPv6 Server and assign IPv6 address 2001::1/64 to port G1/1 connected to PC on switch
2. DHCPv6 Server assign IPv6 prefix 2001::/64 to DHCPv6 client.
3. DNS Server IPv6 address is 2003::1/64
4. Domain name is "www.example.com.cn"

IV. Configuration Steps

Configuring DHCPv6 Server

1. Enable IPv6 routing:

```
server>enable
server#configure terminal
server(config)#ipv6 unicast-routing
server(config)#end
```

2. Assign IPv6 addresses to interfaces

```
server#conf t
server(config)#
server(config)#interface gigabitEthernet 1/1
server(config-if-GigabitEthernet 1/1)#no switchport
server(config-if-GigabitEthernet 1/1)#ipv6 address 2001::1/64
server(config-if-GigabitEthernet 1/1)#ipv6 enable
server(config-if-GigabitEthernet 1/1)#end
```

3. Enable RA function and set M and O bits

- ①. DHCPv6 client acquires gateway information via RA, not DHCPv6 Server
- ②. Set "managed address configuration" flag in RA packets which indicates that whether DHCPv6 client uses stateful autoconfiguration to acquire IPv6 address. By default, this flag doesn't been set.
- ③. Set "other stateful configuration" flag in RA packets which indicates that whether DHCPv6 client use stateful autoconfiguration to acquire other information. By default, this flag doesn't been set.

```
server>enable
server#configure terminal
server(config)#interface gigabitEthernet 1/1
server(config-if-GigabitEthernet 1/1)#no ipv6 nd suppress-ra          ----->enable RA function
server(config-if-GigabitEthernet 1/1)#ipv6 nd managed-config-flag    ----->set M flag in RA
server(config-if-GigabitEthernet 1/1)#ipv6 nd other-config-flag      ----->set O flag in RA
server(config-if-GigabitEthernet 1/1)#ipv6 nd prefix 2001::/64 no-autoconfig
server(config-if-GigabitEthernet 1/1)#end
```

3. Configuring DHCPv6 Server

```

server(config)#ipv6 dhcp pool ruijie ----->create DHCPv6
pool
server(dhcp-config)#domain-name www.example.com.cn ----->configure domain name
server(dhcp-config)#dns-server 2003::1 ----->configure DNS Server
server(dhcp-config)#prefix-delegation pool ruijie ----->associate DHCPv6 prefix pool
server(dhcp-config)#exit
server(config)#ipv6 local pool ruijie 2001::/64 64 ----->define local pool for clients
server(config)#end

```

4. Enable DHCPv6 Server on interface

```

client(config)#interface gigabitEthernet 1/1
client(config-if-GigabitEthernet 1/1)#ipv6 dhcp server ruijie ----->enable DHCPv6 service on interface
client(config-if-GigabitEthernet 1/1)#end

```

Configuring DHCPv6 Client

Enable DHCPv6 client under interface

```

client(config)#interface FastEthernet 0/11
client(config-FastEthernet 0/11)#no switchport
client(config-FastEthernet 0/11)#ipv6 enable
client(config-FastEthernet 0/11)#ipv6 dhcp client pd rj ----->enable DHCPv6 client and prefix solicitation on
the interface

```

V. Verification

1. How to display status of DHCPv6 pool

```

server#show ipv6 dhcp pool
DHCPv6 pool: ruijie
  Prefix pool: ruijie
    preferred lifetime 3600, valid lifetime 3600
  DNS server: 2003::1
  Domain name: www.example.com.cn

```

3. How to display DHCPv6 Server assignment

```

server#show ipv6 dhcp binding
Client  DUID: 00:03:00:01:00:1a:a9:7d:88:97
  IAPD: ia1d 11, T1 1800, T2 2880
  Prefix: 2001::/64
    preferred lifetime 3600, valid lifetime 3600
    expires at Jul 17 2011 18:30 (3570 seconds)

```

4. How to display DHCPv6 client status on interface

```

client#show ipv6 dhcp int f0/11

```

```
FastEthernet 0/11 is in client mode
State is IDLE
next packet will be send in : 1525 seconds
List of known servers:
  DUID: 00:03:00:01:00:1a:a9:15:c9:b5
  Reachable via address: FE80::21A:A9FF:FE15:C9B6
  Preference: 0
Configuration parameters:
  IA PD: IA ID 0xb, T1 1800, T2 2880
  Prefix: 2001::/64
    preferred lifetime 3600, valid lifetime 3600
    expires at Jul 17 2011 17:55 (3325 seconds)
Prefix name: ruijie
DNS server: 2003::1
Domain name: www.example.com.cn
Rapid-Commit: disable
```

2.9.4.2.2 DHCPv6 Relay

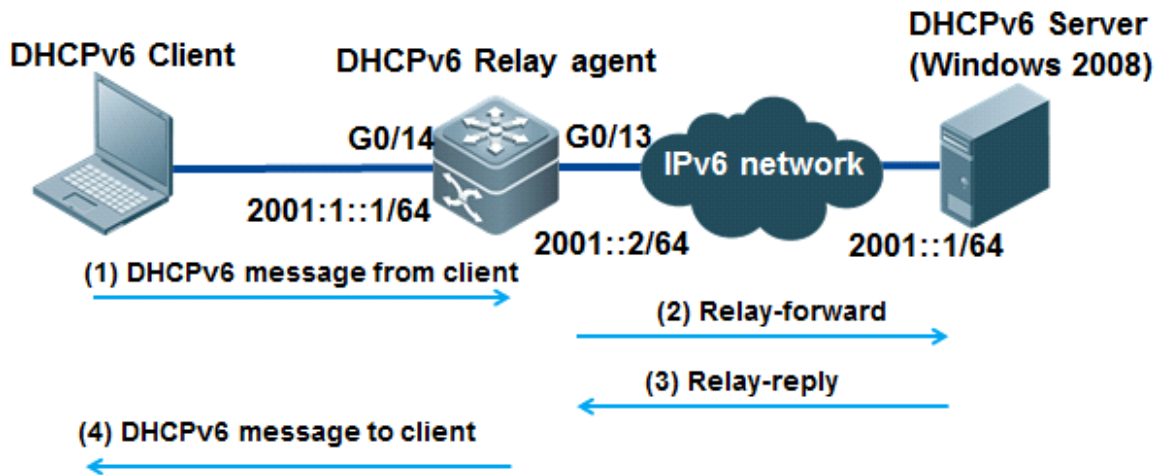
Scenario

The DHCPv6 relay forwards DHCPv6 messages between the DHCPv6 server and the DHCP client. When the DHCP server and the DHCP client are not in the same physical network, the DHCP relay is responsible for forwarding the DHCP solicit and reply messages. The forwarding process is different from routing forwarding, which features transparent transmission. Generally, the router will not modify the contents of IP packets. Upon receiving the DHCP message, the DHCP relay will regenerate and forward another one. The DHCP relay is just like a DHCP server for the DHCP clients and a DHCP client for the DHCP server.

I. Requirements

DHCPv6 Server Station(Windows 2008) assigns IPv6 prefix to DHCPv6 client(station) , and switch acts as DHCPv6 Relay

II. Network Topology



III. Configuration Tips

1. Configuring DHCPv6 Server
2. Enable IPv6 routing on DHCPv6 Relay agent

IV. Configuration Steps

Configuring DHCPv6 Relay agent

1. Enable IPv6 routing

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#ipv6 unicast-routing
Ruijie(config)#end
```

2. Assign IPv6 address to interface connected to DHCPv6 Server ,then enable IPv6 on that interface

```
Ruijie(config)#int g0/13
Ruijie(config-if-GigabitEthernet 0/13)#no switchport
Ruijie(config-if-GigabitEthernet 0/13)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/13)#ipv6 address 2001:1::1
Ruijie(config-if-GigabitEthernet 0/13)#end
```

3. Create VLAN for DHCPv6 client and assign interfaces connected to DHCPv6 client to that VLAN

```
Ruijie(config)#vlan 2
Ruijie(config-vlan)#exit
Ruijie(config)#int g0/14
Ruijie(config-if-GigabitEthernet 0/14)#switchport mode access
Ruijie(config-if-GigabitEthernet 0/14)#switchport access vlan 2
Ruijie(config-if-GigabitEthernet 0/14)#end
Ruijie#
```

4. Configure IPv6 Gateway for DHCPv6 client and then enable DHCPv6 Relay

```
Ruijie#conf t
Ruijie(config)#interface vlan 2
Ruijie(config-if-VLAN 2)# ipv6 address 2001:1::1/64
Ruijie(config-if-VLAN 2)# ipv6 enable
Ruijie(config-if-VLAN 2)# ipv6 dhcp relay destination 2001::1 ----->configure DHCPv6 Relay
```

3. Enable RA function and set M and O bits

- ①. DHCPv6 client acquires gateway information via RA , not DHCPv6 Server
- ②. Set "managed address configuration" flag in RA packets which indicates that whether DHCPv6 client uses stateful autoconfiguration to acquires IPv6 address . By default , this flag doesn't been set.
- ③. Set "other stateful configuration"flag in RA packets which indicates that whether DHCPv6 client use stateful autoconfiguration to acquires other infomation . By default , this flag doesn't been set.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config-if-VLAN 2)# no ipv6 nd suppress-ra ----->enable RA function
Ruijie(config-if-VLAN 2)# ipv6 nd managed-config-flag ----->set M flag of RA
Ruijie(config-if-VLAN 2)# ipv6 nd other-config-flag -----> set O flag of RA
Ruijie(config-if-VLAN 2)# end
```

6. Configuring DHCPv6 Server

Configure Windows 2008 as DHCPv6 Server , for detail information , see Microsoft corresponding guide.

V. Verification

How to display NIC status on station

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter {GUID}:

Connection-specific DNS Suffix . . : 
IPv6 Address . . . . . : 2001:1::143d:d208:1a79:fe4e
IPv6 Address . . . . . : 2001:1::ffff:ffff:ffff:f196
IPv6 Temporary Address . . . . . : 2001:1::41a4:149a:b360:f94e
Link-local IPv6 Address . . . . . : fe80::143d:d208:1a79:fe4e%12
IPv4 Address. . . . . : 169.254.254.78
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : fe80::2d0:f8ff:fe37:1931%12
```

2. Use Ping to test connectivity

```
C:\Users\Scott>ping 2001::1

Pinging 2001::1 with 32 bytes of data:
Reply from 2001::1: time<1ms
Reply from 2001::1: time<1ms
Reply from 2001::1: time<1ms
Reply from 2001::1: time<1ms

Ping statistics for 2001::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Scott>
```

Note: System creates one more random IPv6 temporary address after enabling IPv6.

Suggest to disable this function in order to control user unique ID and reduce network consumption etc.

Following sample shows how to disable temporary address :

run->cmd->netsh->int ipv6->set privacy state=disable

```
C:\Users\Administrator>netsh
netsh>int ipv6
netsh interface ipv6>set privacy state=disable
Ok.

netsh interface ipv6>exit

C:\Users\Administrator>
```

For more information about IPv6 temporary address , see <http://technet.microsoft.com/zh-cn/magazine/2007.08.cableguy.aspx>

2.9.4.3 IPv6 Tunnel

2.9.4.3.1 ISATAP Tunnel

Scenario

Intrasite Automatic Tunnel Addressing Protocol (ISATAP) is an automatic overlay tunneling mechanism that uses the underlying IPv4 network as a NBMA link layer for IPv6. ISATAP is designed for transporting IPv6 packets within a site where a native IPv6 infrastructure is not yet available; for example, when sparse IPv6 hosts are deployed for testing. ISATAP tunnels allow individual IPv4 or IPv6 dual-stack hosts within a site to communicate with other such hosts on the same virtual link, basically creating an IPv6 network using the IPv4 infrastructure.

ISATAP Address Format

ISATAP uses unicast addresses that include a 64-bit IPv6 prefix and a 64-bit interface identifier. The interface identifier is created in modified EUI-64 format in which the first 32 bits contain the value 000:5EFE to indicate that the address is an IPv6 ISATAP address. The table below describes an ISATAP address format.

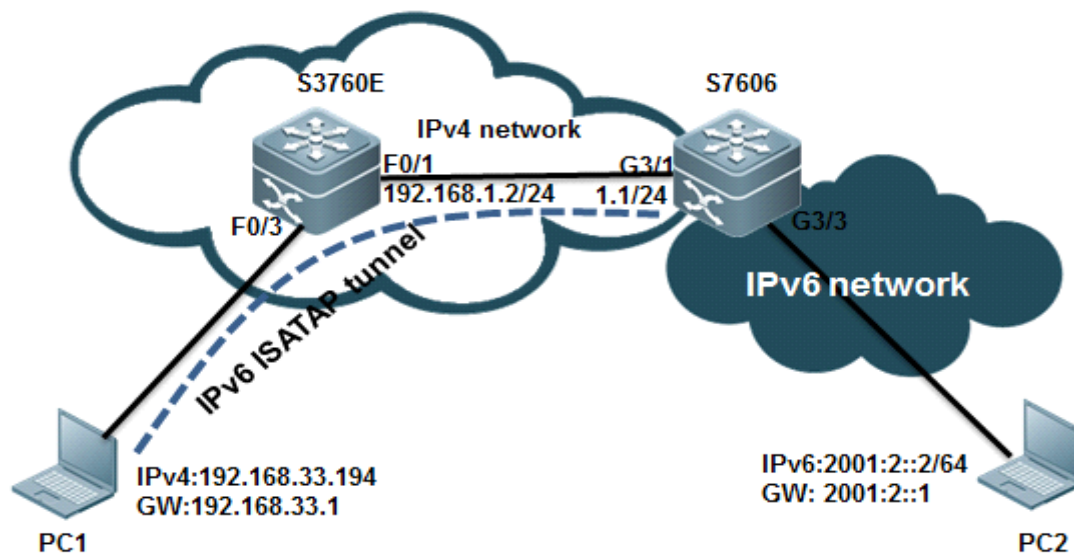
| 64 Bits | 32 Bits | 32 Bits |
|--|-----------|---------------------------------|
| link local or global IPv6 unicast prefix | 0000:5EFE | IPv4 address of the ISATAP link |

As shown in the table above, an ISATAP address consists of an IPv6 prefix and the ISATAP interface identifier. This interface identifier includes the IPv4 address of the underlying IPv4 link. The following example shows what an actual ISATAP address would look like if the prefix is 2001::/64 and the embedded IPv4 address is 192.168.1.1. In the ISATAP address, the IPv4 address is expressed in hexadecimal as C0A8:0101 and the ISATAP is 2001::0000:5EFE:C0A8:0101

I. Requirements

- PCs in IPv4 network want to visit IPv6 resource.
- Build ISATAP tunnel between PC1 and S7606 to reach that goal.

II. Network Topology



III. Configuration Tips

1. You must install IPv6 protocol on PC first (Win7 and Vista don't need) and then add an ISATAP tunnel route.
2. Configure tunnel interface tunnel mode, tunnel source IPv6 EUI address on ISATAP Device

IV. Configuration Steps

Configuring S7606

1. Create Tunnel Interface

```
S7606#conf t
S7606(config)#interface Tunnel 1
S7606(config-if-Tunnel 1)#
```

2. Enable IPv6 on interface and assign IPv6 address to that interface

```
S7606(config-if-Tunnel 1)#ipv6 enable
S7606(config-if-Tunnel 1)#ipv6 address 2001:1::/64 eui-64
```

3. Modify Tunnel mode

```
S7606(config-if-Tunnel 1)#tunnel mode ipv6ip isatap
```

4. Specify Tunnel source using interface ID or IPv4 address(use IPv4 address here)

```
S7606(config-if-Tunnel 1)#ip address 3.3.3.4 255.255.255.0
S7606(config-if-Tunnel 1)#tunnel source 3.3.3.4
```

5. Enable RA . It is disable by default.

```
S7606(config-if-Tunnel 1)#no ipv6 nd suppress-ra
```

6. Assign IPv6 address to Vlan 20 which is also gateway for PC2

```
S7606(config)#vlan 20
S7606(config-vlan)#int vlan 20
S7606(config-if-VLAN 20)# ipv6 address 2001:2::2/64
S7606(config-if-VLAN 20)# ipv6 enable
```

7. Configure interface conneted to S3760E and configure a static route pointing to 192.168.33.0/24

```
S7606(config)#interface GigabitEthernet 3/1
S7606(config-if-GigabitEthernet 3/1)# no switchport
S7606(config-if-GigabitEthernet 3/1)# ip address 192.168.1.1 255.255.255.0
S7606(config-if-GigabitEthernet 3/1)#exit
S7606(config)#ip route 192.168.33.0 255.255.255.0 192.168.1.2
S7606(config)#end
S7606#wr
```

Configuring S3760E

```
S3760E#conf t
S3760E(config)#vlan 10
S3760E(config-vlan)#interface VLAN 10
S3760E(config-if-VLAN 10)# ip address 192.168.33.1 255.255.255.0
S3760E(config-if-VLAN 10)#exit
S3760E(config)#interface FastEthernet 0/3
S3760E(config-if-FastEthernet 0/3)# switchport access vlan 10
```

```

S3760E(config)#interface FastEthernet 0/1
S3760E(config-if-FastEthernet 0/1)# no switchport
S3760E(config-if-FastEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
S3760E(config-if-FastEthernet 0/1)#exit
S3760E(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1

```

Configuring PC

1. Configure a static route pointing to 3.3.3.4 and enable ISATAP .

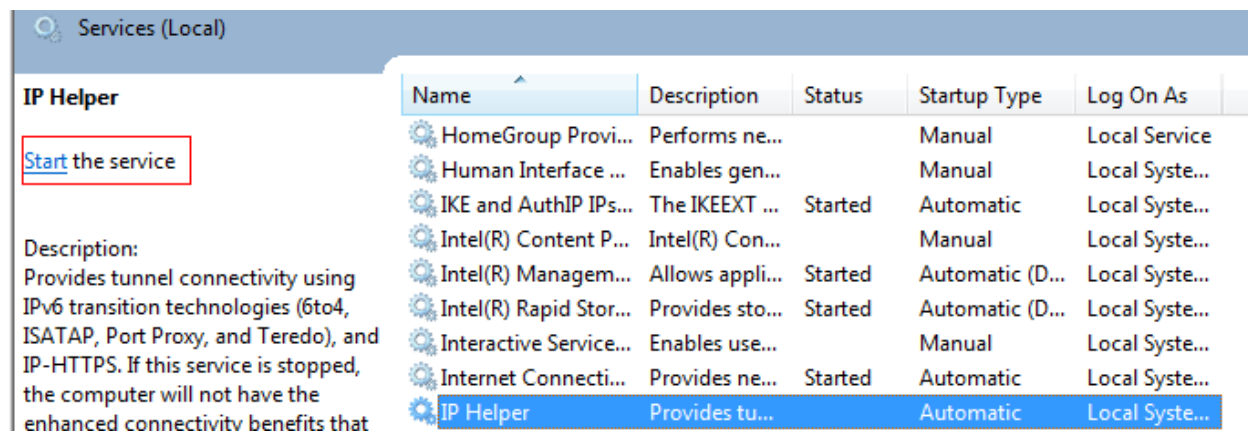
```

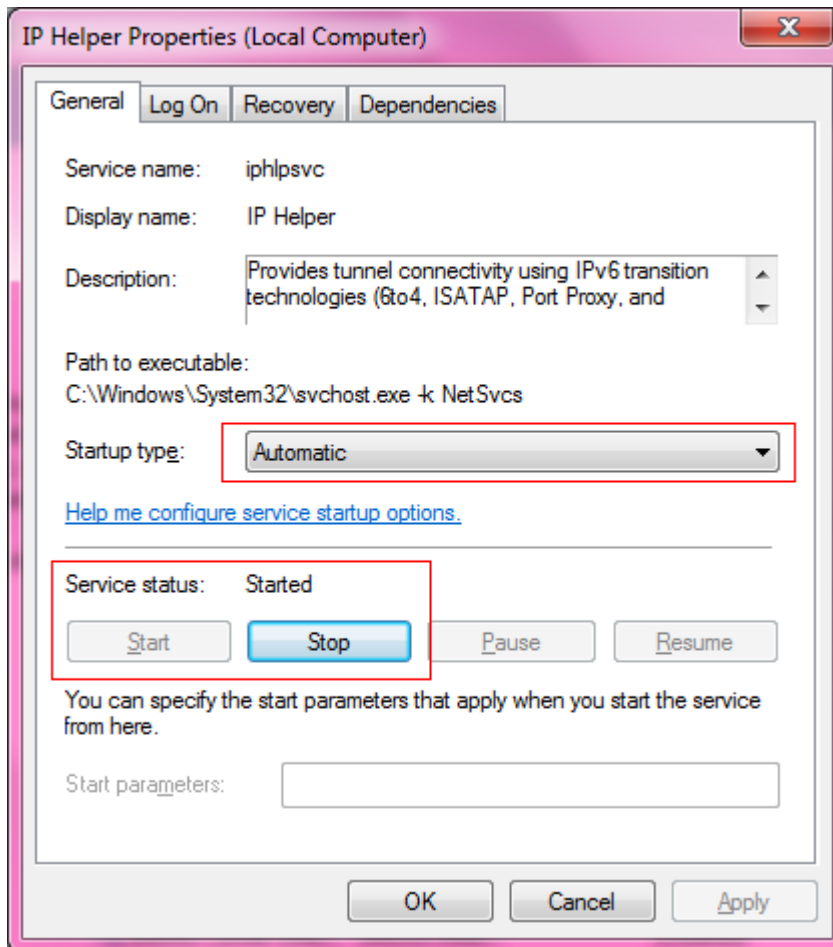
C:\Users\Administrator>netsh
netsh>int ipv6
netsh interface ipv6>isatap
netsh interface ipv6 isatap>set route 3.3.3.4
Ok.

netsh interface ipv6 isatap>set state enable
Ok.

```

2. click Start -> Run -> services.msc ,->enable "IP Helper" Service.





Note: You must double confirm that the steps above have been done, or PC will fail to create ISATAP Tunnel

V. Verification

1. How to display ISATAP status on PC

```
C:\Users\Scott>netsh
netsh>int ipv6
netsh interface ipv6>isatap
netsh interface ipv6 isatap>
netsh interface ipv6 isatap>show route
Router Name       : 3.3.3.4
Use Relay         : default
Resolution Interval : default

netsh interface ipv6 isatap>show state
ISATAP State      : enabled
```

```
Tunnel adapter isatap.{FEB3043-E31D-46B5-A2ED-FBFE18EFD8BC}:
Connection-specific DNS Suffix  . : www.ruijie.com.cn
IPv6 Address . . . . . : 2001:1::5efe:192.168.33.194
Link-local IPv6 Address . . . . . : fe80::5efe:192.168.33.194%14
Default Gateway . . . . . : fe80::5efe:3.3.3.4%14
```

As figure shown above, PC1 has established ISATAP Tunnel with S7606 successfully.

2. PC1 can use Ping to reach PC2 IPv6 address through ISATAP Tunnel.

```
C:\Users\Scott>ping 2001:2::2 -t

Pinging 2001:2::2 with 32 bytes of data:
Reply from 2001:2::2: time<1ms
Reply from 2001:2::2: time<1ms
Reply from 2001:2::2: time<1ms
Reply from 2001:2::2: time<1ms

Ping statistics for 2001:2::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Scott>
```

2.9.4.3.2 Manual Tunnel

Scenario

One manually configured tunnel is similar to one permanent link set up between two IPv6 domains via the backbone network of the IPv4. It is applicable for the relatively fixed connections that have a higher demand on security between two Area Border Routers or between an Area Border Router and a host.

On a tunnel interface, you must manually configure the IPv6 address, source IPv4 address (tunnel source) and destination IPv4 address (tunnel destination) of the tunnel. The nodes at the two end of the tunnel must support the IPv6 and IPv4 protocol stacks. In practical application, tunnels are always manually configured in pairs. You can think it as a point-to-point tunnel.

I. Requirements

1. The figure shown below simulates a scenario that two IPv6 networks connects through an IPv4 network.
2. Configure Manual Tunnel on two IPv6 boundary dual-stack switches to ensure that PC1 can communicate with PC2 through IPv4 network.

II. Network Topology

III. Configuration Tips

1. You must install IPv6 protocol on PC first (Win7 and Vista don't need) and then add an ISATAP tunnel route.
2. Ensure all IPv4 routes have propagated correctly first.

IV. Configuration Steps

1. Install IPv6 Protocol on Windows XP.

(Windows 7 and Windows Vista don't need)

2. Enable IPv6 on SVI 10 connected to customer, then configure basic IPv6 parameters.

```
S86E(config) #interface vlan 10
S86E(config-if- VLAN 10)#no shutdown
S86E(config-if- VLAN 10)#ipv6 enable
S86E(config-if- VLAN 10)# ipv6 address 2001:10::1/64
S86E(config-if- VLAN 10)# no ipv6 suppress-ra
```

Note: You cannot enable IPv6 between S3760-1 and S3760-2 because the link only forward IPv4 traffic in order to simulate two IPv6 networks is isolated by an IPv4 network.

3. Configure IPv6 Manual Tunnel

```
S86E(config) #interface Tunnel 1
S86E(config-if-Tunnel 1)#ipv6 enable
S86E(config-if-Tunnel 1)#tunnel source 10.1.1.1
S86E(config-if-Tunnel 1)#tunnel destination 10.1.1.2
S86E(config-if-Tunnel 1)#tunnel mode ipv6ip
```

4. Configure IPv6 Route

```
S86E(config) # ipv6 route 2001:20::/64 Tunnel 1
```

5. Show run on S3760-1

```
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.1 255.255.255.252
!
interface GigabitEthernet 0/12
 switchport access vlan 10
!
interface VLAN 10
```

```
no ip proxy-arp
ip address 192.168.10.254 255.255.255.0
ipv6 address 2001:10::1/64
ipv6 enable
no ipv6 nd suppress-ra
!
interface Tunnel 1
ipv6 enable
tunnel source 10.1.1.1
tunnel destination 10.1.1.2
!
ipv6 route 2001:20::/64 Tunnel 1
!
```

6. Configuration on S3760-2 is the same to S3760 except for the IPv6 address.

V. Verification

1. Use PING to test connectivity between PC1 and PC2

```
S3760-1#ping 2001:20::1 source 2001:10::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:20::1, timeout is 2 seconds:
Packet sent with a source address of 2001:10::1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/106/176 ms
```

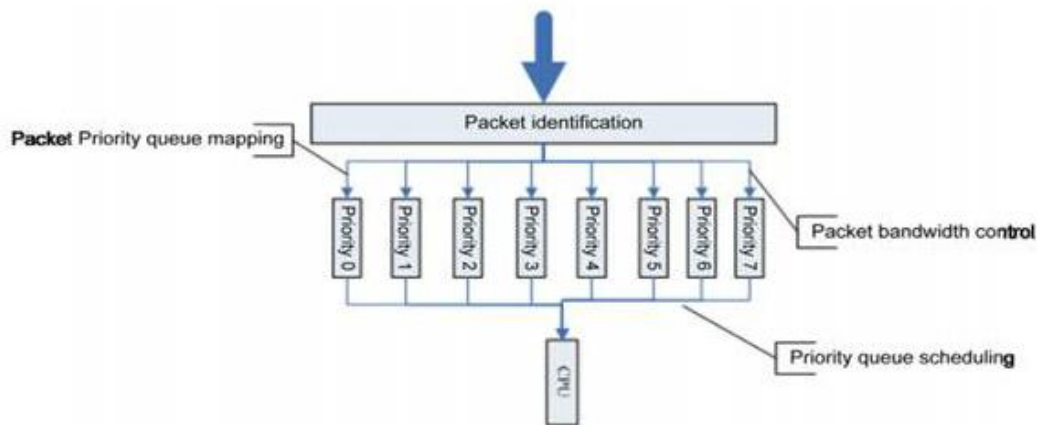
2.9.5 Security

2.9.5.1 CPP

Overview

CPU Protect Policy (CPP) can effectively prevent malicious attacks in the network by packet identification and attack packet suppression, which can:

1. Reduce the influence of attack packets on the switch (CPU protection)
2. Enable load balance for the packets of different priority queues.



CPP adopts packet identification, packet bandwidth control, priority queue mapping and queue scheduling to protect CPU and key packets.

1. Packet Identification

Packet identification classifies all the packets sent to the switch for processing, for example, ARP, BPDUs and GVRP etc.

2. Packet Bandwidth Control

Administrator can configure bandwidth for each type of packets to suppress attack packets at high rate in the network.

3. Priority Queue Mapping

Eight priority queues are supported. You can configure priority queue for each type of packets.

4. Queue Scheduling

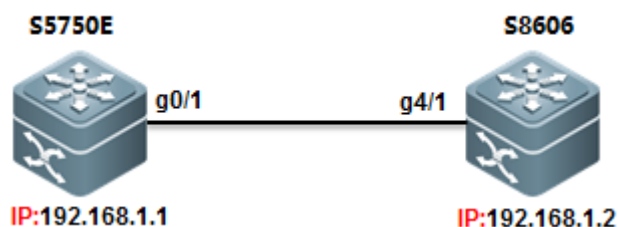
Poll scheduling algorithm is used to ensure that the protocol packets of different priority queues are sent to CPU for processing in time. Each queue is of the same scheduling weight.

Configuration

I. Requirements

As the figure shown below, administrator connects a S5750E switch to a S8606 switch through layer 3 port and is pinging S5750E with 18024 bytes ICMP packet on S8606, then he finds that there's a regular RTO (about 3 RTO every 1000 packets). Administrator has disabled NFPP ICMP-Guard on both switches but this issue still occurs. Later administrator finds that it is because of the default CPP setting that makes the RTO.

II. Network Topology



III. Configuration Tips

CPP commands on different series of switch varies, but you can enter "cpu-protect" global command and use "?" to display the details command.

This example shows how to set CPP ARP value to 200000 PPS on **S86E**:

```
Ruijie(config)#cpu-protect ?
cpu          Set cpu bandwidth
sub-interface Set globle control to packet
traffic-class Set traffic-class' configure
type         Set packet's configure
Ruijie(config)#cpu-protect type arp-request bandwidth 20000
Ruijie(config)#cpu-protect type arp-reply bandwidth 20000
```

How to display CPP configuration

```
Ruijie#show cpu-protect
%cpu port bandwidth: 10000(pps)
Traffic-class  Bandwidth(pps)  Rate(pps)
-----
0              1000          0
1              1000          0
2              1500          0
3              8000          0
4              1500          0
5              1500          0
6              3500          0
Packet Type    Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
-----
bpdu           6             1000           0          0
arp-request    2             20000          0          0
```

This example shows how to set CPP ARP value to 200000 PPS on **S8600** :

```
Ruijie(config)# cpu-protect ?
sub-interface  Config sub-interface pps or percent
type          Add an extend type
Ruijie(config)#cpu-protect type arp pps 20000
```

How to display CPP configuration

```
Ruijie#show cpu-protect summary
Type          Pps      Pri
-----
```

| | | |
|----------|-------|---|
| tp-guard | 128 | 7 |
| arp | 20000 | 3 |

IV. Configuration Steps

1) Configuring S86E

```
Ruijie(config)#cpu-protect type icmp bandwidth 5000 ----->set bandwidth of ICMP to 5000 PPS
Ruijie(config)#cpu-protect traffic-class id 3 bandwidth 8000 ----->set bandwidth of traffic-class id 3 to 8000 PPS because ICMP belongs to traffic-class id 3
Ruijie(config)#cpu-protect cpu bandwidth 10000 ----->set global cpu bandwidth to 10000
```

2) Configuring S8606

```
Ruijie(config)#cpu-protect type ipv4-icmp-local pps 10000 ----->set bandwidth of ICMP to 10000 PPS
```

V. Verification

1) How to display CPP configuration for ICMP on S86E

CPP bandwidth of ICMP is 5000 packets per second(pps) and ICMP belongs to Traffic-class id is 3

```
Ruijie#show cpu-protect type icmp
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
-----
icmp             3             5000           0          0
```

Bandwidth of traffic-class 3 is 8000 pps

```
S8600E-VSU#sh cpu-protect traffic-class 3
Traffic-class    Bandwidth(pps)  Rate(pps)  Drop(pps)
-----
3                20000          13         0
```

Maximum number of packets sent CPU to process is 10000 pps

```
Ruijie#show cpu-protect cpu
%cpu port bandwidth: 10000(pps)
```

2) How to display CPP configuration on S8600

```
Ruijie#show cpu-protect summary
Type            Pps      Pri
-----
tp-guard        128      7
```

Show CPP statistic of each type of packets in mainboard.

```
S8600E-VSU#sh cpu-protect mboard
%cpu port bandwidth: 100000(pps)
Traffic-class      Bandwidth(pps)    Rate(pps)    Drop(pps)
-----
0                   20000             0             0
1                   20000             282           256
2                   20000             299           0
```

Show CPP statistic of each type of packets in each slot.

```
S8600E-VSU#sh cpu-protect slot 4
%cpu port bandwidth: 100000(pps)
Traffic-class      Bandwidth(pps)    Rate(pps)    Drop(pps)
-----
0                   20000             0             0
1                   20000             181           0
2                   20000             99            0
3                   20000             14            0
4                   20000             1             0
5                   20000             0             0
6                   20000             0             0
7                   20000             0             0
Packet Type        Traffic-class      Bandwidth(pps)    Rate(pps)    Drop(pps)    Total      Total Drop
-----
bpdu                6                  128              0            0            37          0
arp                 1                  10000            53           0            18115740    0
tpp                 6                  128              0            0            0           0
dot1x               2                  1500             0            0            0           0
```

Show CPP statistic of a specific type of packet

```
S8600E-VSU#sh cpu-protect type local-ipv4
Packet Type        Traffic-class      Bandwidth(pps)    Rate(pps)    Drop(pps)    Total      Total Drop
-----
local-ipv4         3                  4000              1            0            280522     0
```

2.9.5.2 NFPP

Overview

(NFPP) protects switch itself from being attack and couldn't replace security feature that defend ARP spoofing. NFPP is enabled by default.

Recommend operation:

1. Actually, no need to tune NFPP parameter on access switch because on not-gateway equipment, there're no gateway IP address, no routing protocol, no administrator protocol, no extra cpu consumption, and less beeing attacked.
2. On aggregation switch, default NFPP port-base threshold -----rate-limit 100PPS / attack-detection 200PPS is small when there're many users and many ARP attacks, the small threshold may lead to normal ARP packets loss. Best practice is tune the threshold to rate-limit 500PPS / attack-detection 800PPS for each port and no need to adjust other ip/mac base parameters.
3. Not suggest to turn on isolation function except for the very often attacks that makes cpu utilization up to 80% ~90% and need to increase attack-threshold in case of misjudgement.

NFPP is the abbreviation of Network Foundation Protection Policy. In the network, some malicious attacks put too much burden on the switch, thus the CPU of the switch cannot operate normally.

DoS attack may lead to the consumption of a large amount of the switch memory, entries and other resources, resulting in the system service failure. A large amount of the packet traffic uses the CPU bandwidth, resulting in the handling failure of the protocol packet and manage packet by the CPU, influencing the data forwarding, the device management of the administrator and the normal device/network running. A large amount of the packet traffic consumes massive CPU resources,

making the CPU being in the high-load status and influencing the device management of the administrator and the normal device running. In the NFPP-enabled environment, **it prevents the system from being attacked**, releasing the CPU load and ensuring the normal and stable operation of various system services and the whole network.

Most important sub-function of NFPP Overview: (Suggest administrator to adjust ARP-Guard and IP-Guard function in daily maintenance and keep the default value for other NFPP sub-function, like ND Guard, DHCP Guard..)

ARP-Guard Overview:

The IP address is translated into the MAC address by ARP protocol in the local area network (LAN). ARP protocol plays an important role in the network security. ARP DoS attack sends a large amount of illegal ARP packets to the gateway, preventing the gateway from providing the services. To deal with this attack, on one hand, you can configure the rate-limit of the ARP packet, on the other hand, you can detect and isolate the attack source.

The ARP attack detection could be host-based or port-based. Host-based ARP attack detection could be classified into the following two types again: source IP address/VID/port-based and source MAC address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The ARP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

IP-Guard Overview:

As is known to all, many hacker attacks and the network virus invasions begin with the network scanning. To this end, a large amount of the scanning packets take up the network bandwidth, leading to the abnormal network communication.

Ruijie Layer-3 device provides the IP-guard function to prevent the attacks from the hacker and the virus such as “Blaster”, reducing the CPU burden of the layer-3 devices.

There are two types of the IP packet attack:

- 1) Scanning the destination IP address change: not only consumes the network bandwidth and increases the device burden, but also is a prelude of the hacker attack.
- 2) Sending the IP packets to the inexistent destination IP address at the high-rate: for the layer-3 device, the packets are directly forwarded by the switching chip without the consumption of the CPU resources if the destination IP address exists. While if the destination IP address is inexistent, the ARP request packets are sent from the CPU to ask for the corresponding MAC address for the destination IP address when the IP packets are sent to the CPU. It consumes the CPU resources if many IP packets are sent to the CPU.

The workaround for this attack: on one hand, you may configure the IP packet rate-limit; on the other hand, you may detect and isolate the attack source.

The IP attack detection could be host-based or port-based. Host-based ARP attack detection adopts the combination of source IP address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The IP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

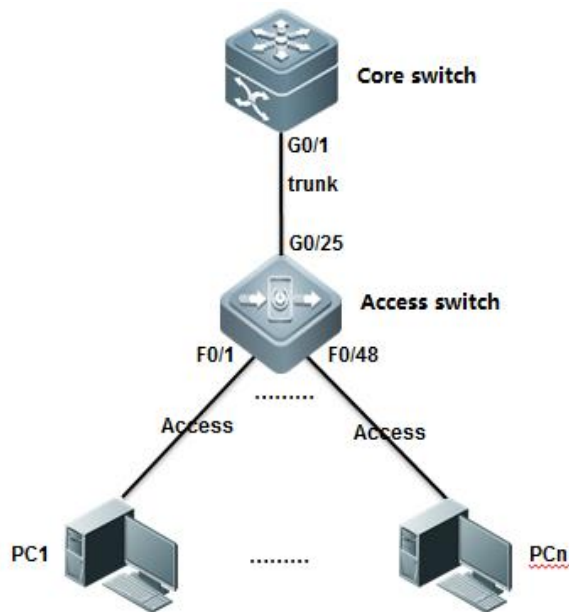
Configuring NFPP

Configuration

I. Requirements

Core switch carries 3000 users, and figure below only shows one of all the ports and this port carries about 200 users. As to Access switch, each port can carry maximum 6 users. Administrator can enable DHCP Snooping and DAI to ensure the stability of network and prevent ARP spoofing. In addition, administrator can enable NFPP to protect switch itself from being attacked.

II. Network Topology



III. Configuration Tips

1. Disable NFPP on uplink port on access switch and adjust CPP parameters (In a scenario that has DAI enabled, the default CPP ARP rate-limit 180PPS is not enough and can probably drop the exceeding but legal ARP packets)
2. Adjust NFPP parameters (Per Port, Per IP and Per MAC)
3. Adjust the printing rate of NFPP logs.

IV. Configuration Steps

Configuration Access Switch:

1. **Configure DAI**. For more information, see [Chapter ARP Spoofing Protection](#)

```

Ruijie#configure terminal
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exit
Ruijie(config)#ip arp inspection vlan 10
Ruijie(config)#ip dhcp snooping
Ruijie(config)#interface gigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#switchport mode trunk
  
```

```
Ruijie(config-if-GigabitEthernet 0/25)#ip dhcp snooping trust
Ruijie(config-if-GigabitEthernet 0/25)#ip arp inspection trust
Ruijie(config-if-GigabitEthernet 0/25)#exit
Ruijie(config)#interface range fastEthernet 0/1-24
Ruijie(config-if-range)#switchport access vlan 10
Ruijie(config-if-range)#end
Ruijie#
```

2. Configure NFPP :

1) Configuring global NFPP

NFPP is enabled by default , and you don't need to adjust default NFPP parameters and you can disable NFPP on uplink interface ,then adjust CPP ARP parameter if DAI is enabled in case that CPP and NFPP drop the exceeding but legal ARP packets received from Core switch .

```
Ruijie(config)#cpu-protect type arp pps 500 ----->no need to adjust CPP if DAI is disabled
```

Tune NFPP parameters as below :

```
Ruijie(config-nfpp)#log-buffer entries 1024 ----->set the NFPP log-buffer capability to
1024 (256 by default)
Ruijie(config-nfpp)#log-buffer logs 1 interval 300 ----->set the rate of printing syslog . NFPP prints
syslog every 300 seconds .
Ruijie(config-nfpp)#exit
Ruijie(config)#
```

2) Configuring NFPP in interface configuration mode

Disable NFPP on uplink interfaces

```
Ruijie(config)#int g0/25
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp arp-guard enable ----->disable ARP-Guard
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp dhcp-guard enable ----->disable DHCP-Guard
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp dhcpv6-guard enable ----->disable DHCPv6-Guard
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp icmp-guard enable ----->disable ICMP-Guard
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp ip-guard enable ----->disable IP-Guard
Ruijie(config-if-GigabitEthernet 0/25)#no nfpp nd-guard enable ----->disable ND-Guard
Ruijie(config-if-GigabitEthernet 0/25)#exit
Ruijie(config)#
```

Configuration on Core Switch :

```
Ruijie(config)#nfpp
Ruijie(config-nfpp)#arp-guard attack-threshold per-port 800 ----->set the ARP-Guard attack threshold to
800pps per-port. When the ARP packet sent from the port exceeds the attack threshold , the attack is detected and
system prompts.
```

```

Ruijie(config-nfpp)#arp-guard rate-limit per-port 500 ----->set the ARP-Guard rate limit to
500pps (100 by default) per-port and ARP-Guard drops the exceeding ARP packets when rate exceeds.
Ruijie(config-nfpp)#log-buffer entries 1024 ----->set the NFPP log-buffer capability to 1024 (256 by default)
Ruijie(config-nfpp)#log-buffer logs 1 interval 300 ----->set the rate of printing syslog . NFPP prints 1 syslog
every 300 seconds
Ruijie(config-nfpp)#exit
Ruijie(config)#

```

If you want to enable NFPP isolation, you should increase rate-limit and attack-threshold in case that NFPP isolates the legal hosts.

Note:

1. Don't enable NFPP isolation on access switch.
2. Usually, we don't suggest you to enable NFPP isolation , but you can enable NFPP isolation if there're too many malevolent attacks on **Distribution Switch (Gateway)** and CPU load is very heavy (above 90%) all the time.

```

Ruijie(config)#nfpp ----->enter NFPP configuration
mode
Ruijie(config-nfpp)#arp-guard isolate-period 600 ----->When ARP packet from a host exceeds the
attack threshold , ARP-guard isolates the host for 600 seconds (The default value is 0s, representing no isolation.)
Ruijie(config-nfpp)#arp-guard attack-threshold per-src-mac 30 ----->set the ARP-Guard attack threshold
to 30pps (8 by default ) based on the MAC address.
Ruijie(config-nfpp)#arp-guard attack-threshold per-src-ip 30 ----->set the ARP-Guard attack threshold
to 30pps (8 by default ) based on the IP address.
Ruijie(config-nfpp)#arp-guard rate-limit per-src-mac 20 ----->set the ARP-Guard rate limit to
20pps (4 by default) based on the MAC address and ARP-Guard drops the exceeding ARP packets.
Ruijie(config-nfpp)#arp-guard rate-limit per-src-ip 20 ----->set the ARP-Guard rate limit to
20pps (4 by default) based on the IP address and ARP-Guard drops the exceeding ARP packets.

Ruijie(config-nfpp)#ip-guard attack-threshold per-src-ip 80 ----->set the IP-Guard attack threshold to
80pps based on the IP address.
Ruijie(config-nfpp)#ip-guard isolate-period 600 ----->When IP packet from a host
exceeds the attack threshold , IP-guard isolates the host for 600 seconds (The default value is 0s, representing no
isolation.)

```

V. Verification

1. How to display NFPP ARP-Guard configuration

```
Ruijie#show nfpp arp-guard summary
```

(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)

| Interface | Status | Isolate-period | Rate-limit | Attack-threshold | Scan-threshold |
|-----------|---------|---------------------|------------|------------------|----------------|
| Global | Enable | 600 → isolate 10min | 6/6/200 | 10/10/400 | 2000 |
| Gi0/25 | Disable | - | -/-/- | -/-/- | - |

enable globally
Maximum count of monitored hosts: 1000
Monitor period: 600s

2. How to display ARP-Guard scan table

```
Ruijie#show nfpp arp-guard scan
```

| VLAN | interface | IP address | MAC address | timestamp |
|------|-----------|------------|----------------|-------------------|
| 1 | Gi0/6 | - | 00d0.f8aa.bb36 | 2013-3-16 9:23:43 |
| 1 | Gi0/6 | - | 001a.a942.f2df | 2013-3-16 9:24:41 |

3. How to display isolated user

```
Ruijie#show nfpp arp-guard hosts
```

If col_filter 1 shows '*', it means "hardware do not isolate host".

| VLAN | interface | IP address | MAC address | remain-time(s) |
|------|-----------|------------|----------------|----------------|
| 1 | Gi0/6 | - | 001a.a942.f2df | 133 |
| 1 | Gi0/6 | - | 00d0.f8aa.bb36 | 38 |

Total: 2 hosts

remain time of isolation, not isolateion time

4. How to display NFPP Logs in buffer

```
Ruijie#show nfpp log buffer
```

all illegal user would be in the log buffer

| Protocol | VLAN | Interface | IP address | MAC address | Reason | Timestamp |
|----------|------|-----------|------------|----------------|--------|-----------|
| ARP | 1 | Gi0/6 | - | 00d0.f8aa.bb36 | DoS | 2013-3-16 |
| ARP | 1 | Gi0/6 | - | 001a.a942.f2df | DoS | 2013-3-16 |
| ARP | 1 | Gi0/6 | - | 00d0.f8aa.bb36 | DoS | 2013-3-16 |
| ARP | 1 | Gi0/6 | - | 001a.a942.f2df | DoS | 2013-3-16 |
| ARP | 1 | Gi0/6 | - | 00d0.f8aa.bb36 | DoS | 2013-3-16 |
| ARP | 1 | Gi0/6 | - | 001a.a942.f2df | DoS | 2013-3-16 |
| ARP | 1 | Gi0/6 | - | 001a.a942.f2df | SCAN | 2013-3-16 |

6. Common NFPP Syslog information

- 1) *Dec 26 13:46:10:%NFPP_ARP_GUARD-4-SCAN_TABLE_FULL: ARP scan table is full.
 - a. ARP scan table contains only the latest 256 logs. When the ARP scan table is full, the latest record overwrite the oldest one. This log doesn't have any impact on switch performance.
 - b. Use "clear nfpp log" EXEC command to clear NFPP log buffer
 - c. Following example shows how to increase log buffer size and decrease printing rate:

```
Ruijie(config)#nfpp
Ruijie(config-nfpp)#log-buffer entries 1024
```

----->set NFPP log buffer capability to 1024

```
Ruijie(config-nfpp)#log-buffer logs 1 interval 300
seconds
```

```
----->NFPP print 1 log every 300
```

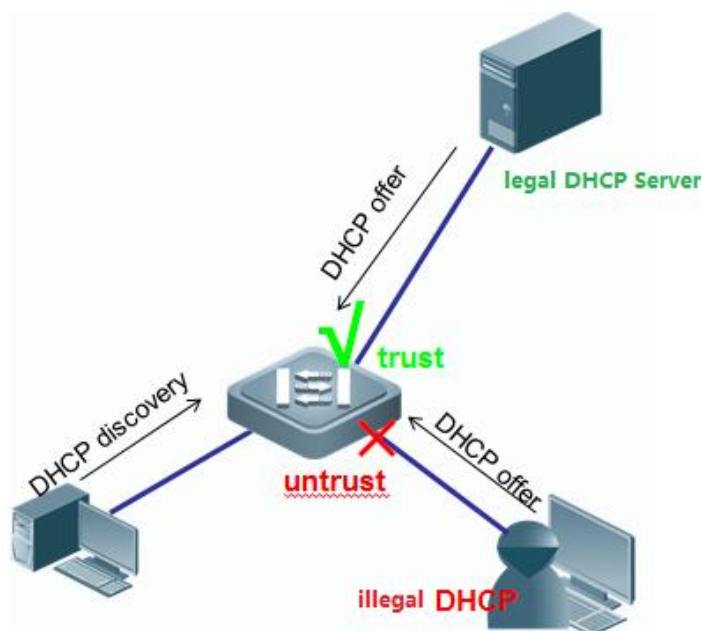
2.9.5.3 DHCP SNOOPING

Overview

DHCP Snooping: In the DHCP-enabled network, the general problem facing administrator is that some users use private IP addresses rather than dynamically obtaining IP addresses. As a result, some users using dynamic IP addresses cannot access the network, making network application more complex. In dynamic DHCP binding mode, the device records how legal users obtain IP addresses during the course of DHCP Snooping for security purpose. There are three ways of security control. The first one is to enable address binding for legal users in conjunction with the IP Source Guard function; the second one is to use DAI to check the validity of users by controlling ARP; the third one is to bind the ARP message of legal users in conjunction with the ARP Check function. It should be noted that given the limit of hardware entries in the first mode, the switch supports limited DHCP users. Where there are too many users on the switch, some legal users may not access the network for they cannot add hardware entries. In addition, the second method will influence the performance of the switch at a large extent, because all ARP messages are forwarded and processed by CPU.

Some terms and functions used in DHCP Snooping are explained below:

- 1) DHCP Request: Packets sent from DHCP Client to DHCP Server.
- 2) DHCP Ack: Packets sent from DHCP Server to DHCP Client.
- 3) DHCP Snooping TRUST Port: Because the packets for obtaining IP addresses through DHCP are in the form of broadcast, some illegal servers may prevent users from obtaining IP addresses, or even cheat and steal user information. To solve this problem, DHCP Snooping classifies the ports into two types: TRUST port and UNTRUST port. The device forwards only the DHCP reply packets received through the TRUST port while discarding all the DHCP reply packets from the UNTRUST port. In this way, the illegal DHCP Server can be shielded by setting the port connected to the legal DHCP Server as a TRUST port and other ports as UNTRUST ports.
- 4) DHCP Snooping Binding Database: By snooping the packets between the DHCP Clients and the DHCP Server, DHCP Snooping combines the IP address, MAC address, VID, port and lease time into an entry to form a DHCP Snooping user database.

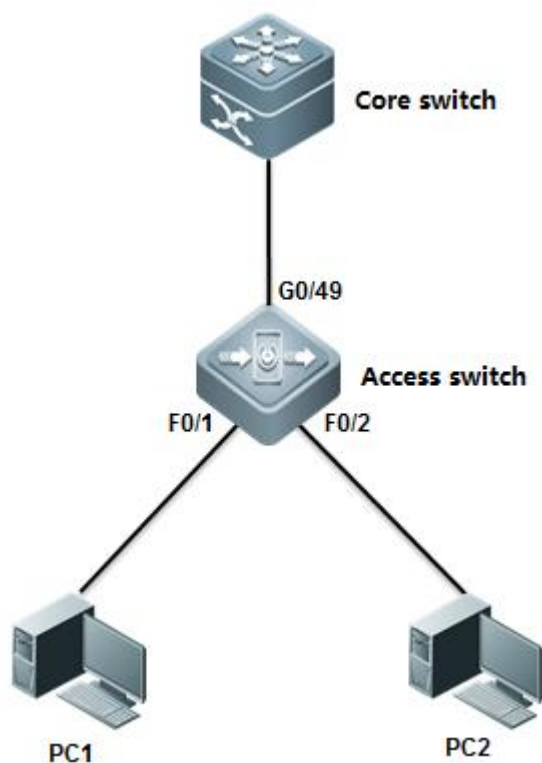


Configuration

I. Requirements

As figure shown below, Core switch acts as DHCP Server and assign IP address to stations. Administrator wants to enable DHCP Snooping in case that some users connect their household router to network and the household router assigns IP address to stations, then stations cannot access to the network once they require the wrong IP address.

II. Network Topology



III. Configuration Tips

1. Enable DHCP Snooping on Access switch and configure the uplink port as DHCP Snooping trust port
2. Configure Core switch as DHCP Server.

IV. Configuration Steps

Configuring Core Switch:

```
Ruijie(config)#service dhcp
```

2. Assign IP address to Vlan 1 which is the user gateway

```
Ruijie(config)#interface vlan 1  
Ruijie(config-if-VLAN 1)#ip address 192.168.1.254 255.255.255.0  
Ruijie(config-if-VLAN 1)#exit
```

3. Create DHCP pool

```
Ruijie(config)#ip dhcp pool vlan1  
Ruijie(dhcp-config)#network 192.168.1.0 255.255.255.0  
Ruijie(dhcp-config)#dns-server 218.85.157.99  
Ruijie(dhcp-config)#default-router 192.168.1.254  
Ruijie(dhcp-config)#end
```

```
Ruijie#wr
```

Configuring Access Switch:

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#ip dhcp snooping
```

3. Configure the port connected to DHCP Server as DHCP Snooping trust port

```
Ruijie(config)#interface gigabitEthernet 0/49
Ruijie(config-GigabitEthernet 0/49)#ip dhcp snooping trust
```

-----By default , all ports are DHCP Snooping untrust port. Only trust port can forward DHCP Offer and Ack packets

.Save configuration

```
Ruijie(config-GigabitEthernet 0/49)#end
Ruijie#write -----> Confirm and save configuration
```

V. Verification

1. How to display DHCP assignment on DHCP Server.

```
Ruijie#show ip dhcp binding
```

| IP address | Client-Identifier/ Hardware address | Lease expiration | Type |
|-------------|--|---------------------------|-----------|
| 192.168.1.1 | 0100.21cc.cf6f.70 | 000 days 23 hours 42 mins | Automatic |
| 192.168.1.2 | 0100.1aa9.c405.f347. 6967.6162.6974.4574. 6865.726e.6574.302f. 31 | 000 days 23 hours 44 mins | Automatic |

↓
allocated IP address

01 indicates ethernet and following 12 bits indicate client MAC address

2. How to display NIC status on station . Start -> Run -> cmd -> ipconfig/all

```
Ethernet adapter :

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : 00-21-CC-CF-6F-70 → MAC address
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::248b:c4f7:acc4:8ec1%13 (Preferred)
IPv4 Address. . . . . : 192.168.1.1 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 2013 . 3 . 8 9:38:56
Lease Expires . . . . . : 2013 . 3 . 9 9:39:40
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 352330188
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-5B-95-3B-60-67-20-AE-75-E4
DNS Servers . . . . . : 218.85.157.99
NetBIOS over Tcpip. . . . . : Enabled
```

3. How to display DHCP Snooping binding table

```
Ruijie#show ip dhcp snooping binding
```

Total number of bindings: 2

| MacAddress | IpAddress | Lease(sec) | Type | VLAN | Interface |
|----------------|-------------|------------|---------------|------|------------------|
| 0021.cccf.6f70 | 192.168.1.1 | 86234 | dhcp-snooping | 1 | FastEthernet 0/1 |
| 001a.a9c4.05f3 | 192.168.1.2 | 86367 | dhcp-snooping | 1 | FastEthernet 0/2 |

4. How to display DHCP Snooping status

```
Ruijie#show ip dhcp snooping
```

Switch DHCP snooping status : ENABLE
 DHCP snooping Verification of hwaddr status : DISABLE
 DHCP snooping database write-delay time : 0 seconds
 DHCP snooping option 82 status : DISABLE
 DHCP snooping Support bootp bind status : DISABLE

| Interface | Trusted | Rate limit (pps) |
|----------------------|------------------|------------------|
| GigabitEthernet 0/49 | YES → trust port | unlimited |

2.9.5.4 IP Source Guard

Overview

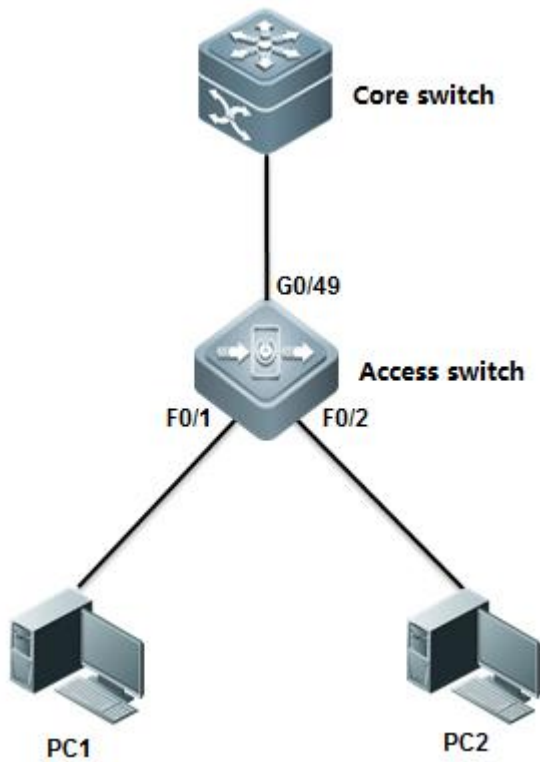
IP Source Guard: IP Source Guard maintains a hardware-based IP packet filtering database to filter packets, guaranteeing that only the users matching the database can access network resources. The hardware-based IP packet filtering database is the key for IP Source Guard to enable efficient security control in DHCP applications. This database is on the basis of DHCP Snooping database. After IP Source Guard is enabled, the DHCP Snooping database is synchronized with the hardware-based IP packet filtering database. In this way, IP Source Guard can strictly filter IP packets from clients on the device with DHCP Snooping enabled.

By default, once IP Source Guard is enabled on a port, all the IP packets traveling through the port (except for DHCP packets) will be checked on the port. Only the users attaining IP addresses through DHCP and the configured static binding users can access the network. IP Source Guard supports source MAC- and source IP-based filtering or source IP-based filtering. In the former case, IP Source Guard will check the source MAC and source IP addresses of all packets and only allow those packets matching the hardware-based IP packet filtering database to pass through. In the latter case, IP Source Guard checks the source IP addresses of IP packets.

I. Requirements

As figure shown below, Core switch acts as DHCP Server. Administrator wants to enable IP Source Guard to enhanced network security and prevent those users who configure illegal static IP address themselves from accessing the network.

II. Network Topology



III. Configuration Tips

1. Core switch acts as DHCP Server
2. Enable DHCP Snooping and IP Source Guard on Access switch to enhance network security

IV. Configuration Example

Configuring Core switch:

1. Enable DHCP Service

```
Ruijie(config)#service dhcp
```

2. Assign IP address to Vlan 1 which is user gateway.

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.1.254 255.255.255.0
Ruijie(config-if-VLAN 1)#exit
```

3. Create DHCP pool .

```
Ruijie(config)#ip dhcp pool vlan1
Ruijie(dhcp-config)#network 192.168.1.0 255.255.255.0
Ruijie(dhcp-config)#dns-server 218.85.157.99
Ruijie(dhcp-config)#default-router 192.168.1.254
```

```
Ruijie(dhcp-config)#end
Ruijie#wr
```

Configuring Access switch:

1. Enable DHCP Snooping

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#ip dhcp snooping ----->enable DHCP Snooping
```

2. Configure the port connected to DHCP Server as DHCP Snooping trust port

```
Ruijie(config)#interface gigabitEthernet 0/49
Ruijie(config-GigabitEthernet 0/49)#ip dhcp snooping trust ----->By default , all ports are untrust port. Only trust
port can forward DHCP Offer and Ack packets
```

3. Enable IP Source Guard on port connected to Users

```
Ruijie(config)#interface range fastEthernet 0/1-2 ----->configure a range of interfaces
Ruijie(config-if-range)#ip verify source port-security ----->enable IP Source Guard in mode
"souce IP + MAC"
```

4. Configure static IP&MAC binding .Stations that matches the binding entry can pass IP Source Guard validation also.

```
Ruijie(config)#ip source binding 001a.a2bc.3a4d vlan 10 192.168.10.5 interface fa0/15
Ruijie(config)#interface fastEthernet 0/15
Ruijie(config-fastethernet 0/15)#ip verify source port-security ----->enable IP Source Guard in
mode "souce IP + MAC"
```

5 . Save Configuration

```
Ruijie(config-if-range)#end
Ruijie#write
```

V. Verification

1. How to display DHCP assigement

```
Ruijie#show ip dhcp binding
```

| IP address | Client-Identifier/ Hardware address | Lease expiration | Type |
|-------------|--|---------------------------|-----------|
| 192.168.1.1 | 0100.21cc.cf6f.70 | 000 days 23 hours 42 mins | Automatic |
| 192.168.1.2 | 0100.1aa9.c405.f347. 6967.6162.6974.4574. 6865.726e.6574.302f. 31 | 000 days 23 hours 44 mins | Automatic |

↑
allocated IP address

↑
01 indicates ethernet and following 12 bits indicate client MAC address

2. How to display NIC status on station . Start -> Run -> cmd -> ipconfig/all

```

Ethernet adapter ...

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : 00-21-CC-CF-6F-70 → MAC address
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::248b:c4f7:acc4:8ec1%13 <Preferred>
IPv4 Address. . . . . : 192.168.1.1<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 2013 . 3 . 8 9:38:56
Lease Expires . . . . . : 2013 . 3 . 9 9:39:40
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 352330188
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-5B-95-3B-60-67-20-AE-75-E4
DNS Servers . . . . . : 218.85.157.99
NetBIOS over Tcpip. . . . . : Enabled
  
```

3. How to display DHCP snooping binding table

```

Ruijie#show ip dhcp snooping binding

Total number of bindings: 2

-----
MacAddress      IpAddress      Lease(sec)    Type           VLAN    Interface
-----
0021.cccf.6f70  192.168.1.1    86155         dhcp-snooping  1       FastEthernet 0/2
001a.a9c4.05f3  192.168.1.2    86189         dhcp-snooping  1       FastEthernet 0/1
  
```

4. How to display IP Source Guard table

```

Ruijie#show ip verify source.
Interface      Filter-type  Filter-mode  Ip-address      Mac-address      VLAN
-----
FastEthernet 0/1  ip+mac      active       192.168.1.2     001a.a9c4.05f3  1
FastEthernet 0/1  ip+mac      active       deny-all       deny-all        1
FastEthernet 0/2  ip+mac      active       192.168.1.1     0021.cccf.6f70  1
FastEthernet 0/2  ip+mac      active       deny-all       deny-all        1
  
```

drop traffic that not in the binding table

5. Use ping to test connectivity when station passes IP source Guard validation.

```
C:\Users\Scott>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

ping gateway successfully

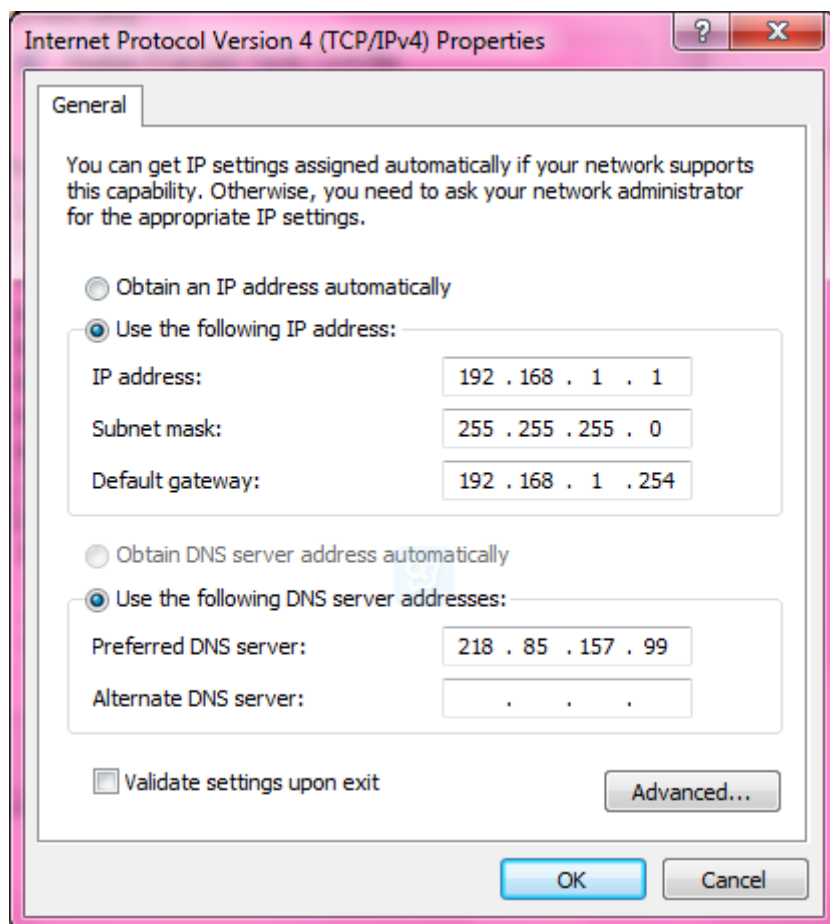
6. How to display ARP table on station.

```
C:\Users\Scott>arp -a

Interface: 192.168.1.1 --- 0x19
    Internet Address      Physical Address      Type
    192.168.1.254         14-14-4b-5b-6e-71    dynamic
    192.168.1.255         ff-ff-ff-ff-ff-ff    static
```

7. Execute "ipconfig/release" to release IP address assigned from DHCP, then configure static IP address

```
C:\Users\Scott>ipconfig/release
```



8. Confirm that we have assigned static IP address to station

```

Ethernet adapter ...

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : 00-21-CC-CF-6F-70
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::248b:c4f7:acc4:8ec1%13 (Preferred)
IPv4 Address. . . . . : 192.168.1.1 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 2013.3.8 9:38:56
Lease Expires . . . . . : 2013.3.9 9:39:40
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 Iaid . . . . . : 352330188
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-5B-95-3B-60-67-20-AE-75-E4
DNS Servers . . . . . : 218.85.157.99
NetBIOS over Tcpip. . . . . : Enabled
  
```

9. There's no binding entry when we display IP source Guard table

```
Ruijie#show ip verify source
```

| Interface | Filter-type | Filter-mode | Ip-address | Mac-address | VLAN |
|------------------|-------------|-------------|-------------|----------------|---------------------|
| FastEthernet 0/1 | ip+mac | active | 192.168.1.2 | 001a.a9c4.05f3 | 1 |
| FastEthernet 0/1 | ip+mac | active | deny-all | deny-all | no binding entry in |
| FastEthernet 0/2 | ip+mac | active | deny-all | deny-all | port 0/2 |

10. Use ping to test the connectivity when station doesn't pass the IP source Guard validation

```
C:\Users\Scott>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Scott>
```

11. ARP entry still exists because IP Source Guard only detects IP packets , not ARP packets.

```
C:\Users\Scott>arp -d clear arp

C:\Users\Scott>arp -a print arp

Interface: 192.168.1.1 --- 0x19
  Internet Address      Physical Address      Type
  192.168.1.254         14-14-4b-5b-6e-71    dynamic
                        can still acquire MAC address of gateway dynamically

C:\Users\Scott>
```

12. Add one static binding entry to IP source guard table

```
Ruijie(config)#ip source binding 0021.cccf.6f70 vlan 1 192.168.1.1 int f0/2
```

13. Confirm that entry has been installed in IP source guard table.

```
Ruijie#show ip verify source
```

| Interface | Filter-type | Filter-mode | Ip-address | Mac-address | VLAN |
|------------------|-------------|-------------|-------------|----------------|------|
| FastEthernet 0/1 | ip+mac | active | 192.168.1.2 | 001a.a9c4.05f3 | 1 |
| FastEthernet 0/1 | ip+mac | active | deny-all | deny-all | |
| FastEthernet 0/2 | ip+mac | active | 192.168.1.1 | 0021.cccf.6f70 | 1 |
| FastEthernet 0/2 | ip+mac | active | deny-all | deny-all | |

14. Finally , use ping to test connectivity successfully.

```
C:\Users\Scott>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64 ping gateway successfully
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2.9.5.5 Port Security

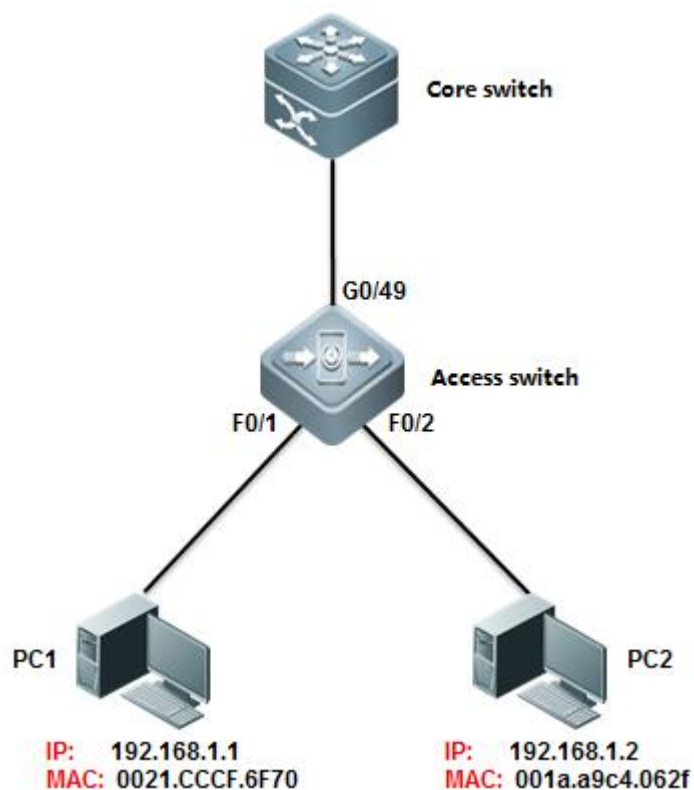
Scenario

Port security: Port security function allows the packets to enter the switch port by the source MAC address, source MAC+IP address or source IP address. You can control the packets by setting the specific MAC address statically, static IP+MAC binding or IP binding, or dynamically learning limited MAC addresses. The port with port security enabled is named as secure port. Only the packets with the source MAC address in the port security address table, or IP+MAC binding configured, or IP binding configured, or the learned MAC address, can join the switch communication, while other packets are dropped.

I. Requirements

1. You can only connect PC1 (IP: 192.168.1.1, MAC: 0021.CCCF.6F70) to port F0/1. If you connect PC1 to other ports, PC1 cannot access the network. If other PCs connect port F0/1, they cannot access the network neither.
2. Port F0/2 can only forward traffic of PC (IP=192.168.1.2, MAC=any) to the network.

II. Network Topology



III. Configuration Tips

Enable Port security on port F0/1 and F0/2, then set port security maximum value to 1.

IV. Configuration Steps

Configuring Core switch:

1. **Assign IP address to Vlan 10 which is user gateway.**

```
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.1.254 255.255.255.0
```

2. **Save configuration**

```
Ruijie(config-if-VLAN 10)#end
Ruijie#wr
```

Configuring Access switch:

1. **Enable port security on interface F0/1 to allow the PC (IP = 192.168.1.1 VLAN=10, MAC=0021.cccf.6f70) to access network.**

```
Ruijie(config-if-VLAN 10)#end
Ruijie#configure terminal
Ruijie(config)#interface fastEthernet 0/1
```

```
Ruijie(config-if-FastEthernet 0/1)#switchport port-security binding 0021.CCCF.6F70 vlan 10 192.168.1.1
Ruijie(config-if-FastEthernet 0/1)#switchport port-security ----->enable Port Security
Ruijie(config-if-FastEthernet 0/1)#exit
```

2. Enable port security on interface F0/2 to allow the PC (IP = 192.168.1.1 VLAN=10, MAC=any) to access network.

```
Ruijie(config)#interfac fastEthernet 0/2
Ruijie(config-if-FastEthernet 0/2)# switchport port-security binding 192.168.1.2 ----->binding ip address
192.168.1.2 to interface f0/2
Ruijie(config-if-FastEthernet 0/2)#switchport port-security ----->enable port security
```

3. Save Configuration

```
Ruijie(config-if-FastEthernet 0/2)#end
Ruijie#write ----->confirm and save
```

Note:

1. You can configure Port security in three modes: **only MAC address**, **IP+MAC** and **only IP address**

Following example shows how to configure Port Security in "**IP+MAC**" mode:

```
Ruijie(config-if-FastEthernet 0/1)#switchport port-security binding 0021.CCCF.6F70 vlan 1 192.168.1.1
```

Following example shows how to configure Port Security in "**only IP address**" mode:

```
Ruijie(config-if-FastEthernet 0/1)#switchport port-security binding 192.168.1.2
```

Following example shows how to configure Port Security in "**only MAC address**" mode:

```
Ruijie(config-if-FastEthernet 0/1)#switchport port-security mac-address 0021.CCCF.6F70
```

2. When you enable port security on port F0/1 in "Only MAC address" mode and bind mac address of PC1 on it, in addition you don't enable port security on other ports, PC1 can access network through port F0/1, but **it cannot access network through other ports**.

3. When you enable port security on port F0/1 in "Only IP address" or "IP + MAC" mode and bind corresponding information of PC1 on it, in addition you don't enable port security on other ports, PC1 can access network through port F0/1 and **it can also access network through other ports**.

V. Verification

How to display Port security table

```

Ruijie#show port-security address
Vlan Mac Address      IP Address      Type      Port      Rem
-----
1      0021.cccf.6f70 192.168.1.1     Configured Fa0/1
      --      192.168.1.2     Configured Fa0/2

```

2.9.5.6 Port Protect

Overview

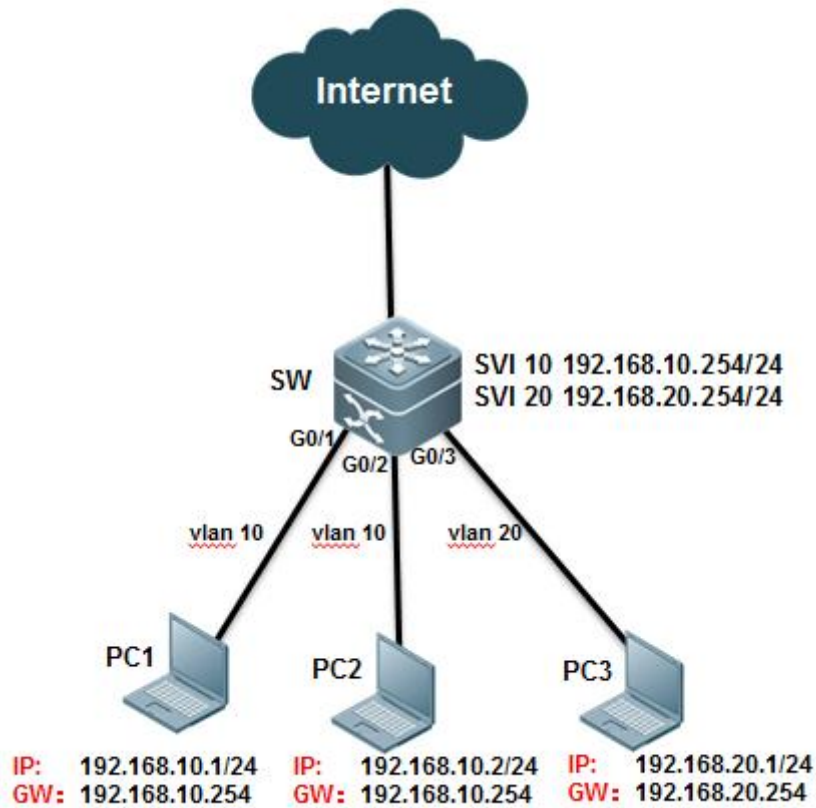
Port Protect: In some application environments, some ports are not required to communicate with each other on a device. In such case, frame forwarding is not allowed between the protected ports, no matter the frames are unicast frames, broadcast frames or multicast frames. To achieve this purpose, you can set some ports as protected ports. Once ports are set as protected ports, **they cannot communicate with each other**. However, protected ports can still communicate with unprotected ports.

There are two protected port modes: one is to block layer 2 forwarding between protected ports but allow layer 3 routing; the other is to block layer 2 forwarding and layer 3 routing between protected ports. The first mode is by default when both modes are supported.

I. Requirements

As figure shown below, PC1 and PC2 belong to VLAN 10. PC3 belongs to VLAN 20. All PC can access to internet, but they cannot communicate with each other.

II. Network Topology



III. Configuration Tips

1. PC1 and PC2 are in the same VLAN 10 and you can enable port protect on ports connected to PC1 and PC2 to prevent PC1 from communicating with PC2.
2. PC3 and PC1, PC2 are in different VLAN and you can enable port protect on ports connected to PC1, PC2 and PC3, then enable "protected-ports route-deny" feature globally to prevent all PCs from communicating from each other.

IV. Configuration Steps

Configuring switch:

```
Ruijie#configure terminal
Ruijie(config)#vlan 10
Ruijie(config-vlan)#vlan 20
Ruijie(config-vlan)#exit
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.10.254 255.255.255.0
Ruijie(config-if-VLAN 10)#interface vlan 20
Ruijie(config-if-VLAN 20)#ip address 192.168.20.254 255.255.255.0
Ruijie(config-if-VLAN 20)#exit
Ruijie(config)#interface GigabitEthernet 0/1
```

```

Ruijie(config-if-GigabitEthernet 0/1)#switchport access vlan 10
Ruijie(config-if-GigabitEthernet 0/1)#switchport protected ----->enable Port protect
Ruijie(config-if-GigabitEthernet 0/1)#interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#switchport access vlan 10
Ruijie(config-if-GigabitEthernet 0/2)#switchport protected ----->enable Port protect
Ruijie(config-if-GigabitEthernet 0/2)#interface GigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#switchport access vlan 20
Ruijie(config-if-GigabitEthernet 0/3)#switchport protected ----->enable Port protect
Ruijie(config-if-GigabitEthernet 0/3)#exit
Ruijie(config)#protected-ports route-deny -----> Configuring the Route-deny
globally to blocks Layer 3 traffic between all protected ports.
Ruijie(config)#end
Ruijie#wr

```

Note:

- 1) When you configure ports as protected ports, they cannot communicate with each other. However, protected ports can still communicate with unprotected ports.
- 2) Only S5750E , S8600 , S12000 series switch support "protected-ports route-deny" feature
- 3) Port protect feature only takes effect on a single Switch .For example, PC1 connects to SWA ,PC2 connects to SWB ,then configure the ports connected to them as protected port , but they can still communicate with each other.

V. Verification

1. How to display port protect status

```

Ruijie#show interfaces switchport

```

| Interface | Switchport | Mode | Access | Native | Protected | VLAN list |
|---------------------|------------|--------|--------|--------|-----------|-----------|
| GigabitEthernet 0/1 | enabled | ACCESS | 10 | 1 | Enabled | ALL |
| GigabitEthernet 0/2 | enabled | ACCESS | 10 | 1 | Enabled | ALL |
| GigabitEthernet 0/3 | enabled | ACCESS | 20 | 1 | Enabled | ALL |
| GigabitEthernet 0/4 | enabled | ACCESS | 1 | 1 | Disabled | ALL |
| GigabitEthernet 0/5 | enabled | ACCESS | 1 | 1 | Disabled | ALL |
| GigabitEthernet 0/6 | enabled | ACCESS | 1 | 1 | Disabled | ALL |

2.9.5.7 AAA**2.9.5.7.1 Authentication****Overview**

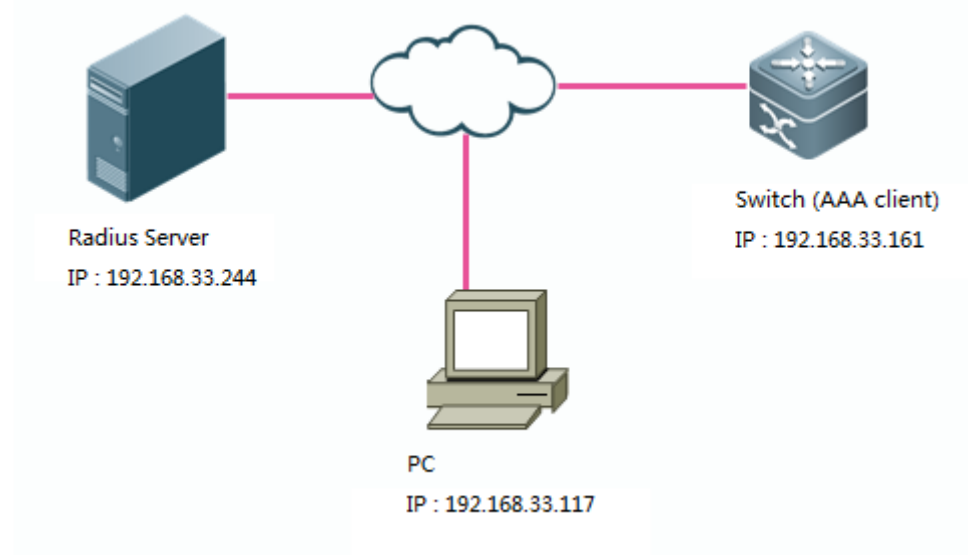
It verifies whether a user can access, where the Radius protocol or Local can be used. The authentication is the method to identify a user before his/her access to the network and network services. The AAA is configured by the definition of a naming list for authentication method and application of it on every interface. The method list defines the authentication type and

execution order. Before a defined authentication is executed, the method list must be applied on a specific interface. The default method list is exceptional. If no other method list is defined, the default method list will automatically apply on all interfaces. The defined method list overwrites the default method list. All authentication methods other than the local, line password and allowing authentication must be defined with AAA.

I. Requirements

1. Administrator wants to setup a Radius server to authenticate users at login. The first method is Radius Server and the fallback is local identity.
2. In case that illegal user breaks in with method of exhaustion ,administrator should set login limits and each account has 3 times to attempts. Otherwise this account will be locked for 1 hour.(by default , limit is 3 attempts and locked time is 15 hours)

II. Network Topology



III. Configuration Tips

1. Enable AAA service, then configure Switch-to-RADIUS-Server Communication.
2. Optimize AAA configuration (AAA lock)
3. Configure Radius Server.

IV. Configuration Steps

Configuring switch:

```
Ruijie#enable
Ruijie#configure terminal
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 192.168.33.244
Server
```

----->enable AAA
----->specify IP address of Radius Server

```

Ruijie(config)#radius-server key ruijie ----->specify key for
Radius Server
Ruijie(config)#aaa authentication login ruijie group radius local ----->define authentication login method list.
first method is Radius Server and fallback is local account.
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication ruijie ----->apply AAA authentication on Line VTY
Ruijie(config-line)#exit
Ruijie(config)#username admin password ruijie ----->define local account
Ruijie(config)#enable password ruijie ----->set enable password
Ruijie(config)#service password-encryption ----->encrypt all password globally
Ruijie(config)#aaa local authentication attempts 3 ----->configure the rule that switch will lock the account
if input the right username but wrong password for three times.
Ruijie(config)#aaa local authentication lockout-time 1 ----->unlock after 1 hour
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip add 192.168.33.161 255.255.255.0
Ruijie(config-if-VLAN 1)#end
Ruijie#write -----> confirm and save configuration

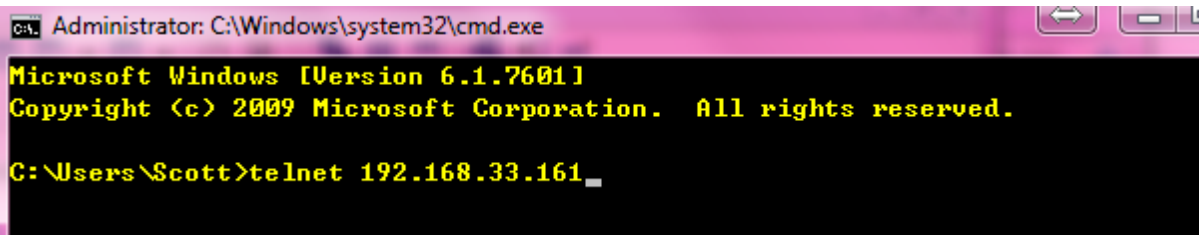
```

Configuring Radius server:

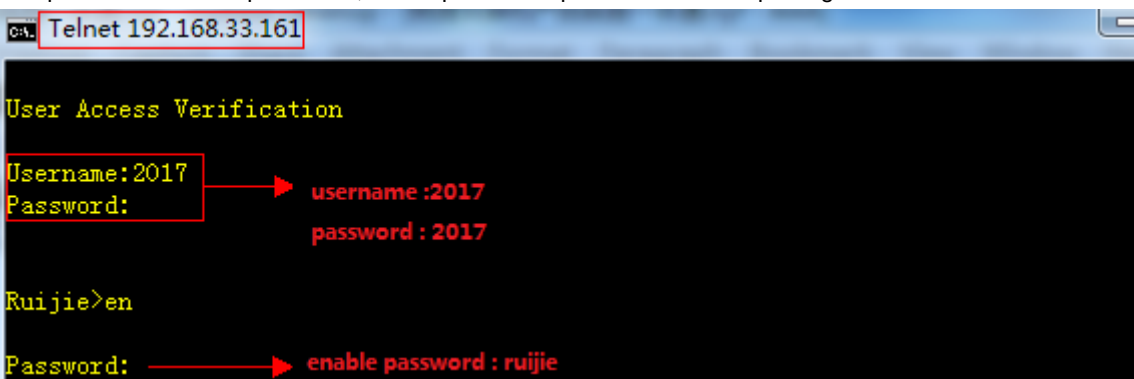
Configuration of different radius servers vary .See relevant configuration guide.

V. Verification

1. Try to telnet a switch



2. Input username and password , then input enable password to enter privilege mode.



3. Show login user status

```
Ruijie#show user
```

| Line | User | Host(s) | Idle | Location |
|-----------|------|---------|----------|----------------|
| 0 con 0 | | idle | 00:00:40 | |
| * 1 vty 0 | 2017 | idle | 00:00:00 | 192.168.33.117 |

Annotations: Red arrows point from '2017' to 'logged on user' and from '192.168.33.117' to 'logged on IP'.

4. If first method (Radius Server) failed ,fallback method takes effect.

Telnet 192.168.33.161

```
User Access Verification
Username:2017
Password:
% Authentication failed

User Access Verification
Username:admin
Password:
local account takes effect now

Ruijie>enable
Password:
Ruijie#show user
```

| Line | User | Host(s) | Idle | Location |
|-----------|-------|---------|----------|----------------|
| 0 con 0 | | idle | 00:01:36 | |
| * 1 vty 0 | admin | idle | 00:00:00 | 192.168.33.117 |

Annotations: Red boxes highlight the failed login with '2017' and the successful login with 'admin'. Red arrows point to explanatory text: 'username 2017 ,password 2017 is invalid now' and 'local account takes effect now'.

5. If you input right username and wrong password three times , your account has been locked.

管理员: C:\Windows\system32\cmd.exe

```
User Access Verification
Username:2017
% Authentication failed

User Access Verification
Username:2017
% Authentication failed

User Access Verification
Username:2017
% Authentication failed
```

Annotation: A red arrow points from the first failure to the text: 'system prompt authentication failed even enter the right username after enter wrong password three times in succession'.

1. Switch enables login authentication on vty line automatically **once you use "Ruijie(config)#aaa new-model" command to enable AAA** , requesting user log in with local account.

This example shows how to create a local account:

```
Ruijie(config)#username admin password Ruijie
```

3. This example shows how to enable aaa login authentication on console line with use local account

```
Ruijie(config)#aaa new-model ----->enable AAA
Ruijie(config)#aaa authentication login ruijie local ----->define authentication login method list named ruijie and
first method is local account.
Ruijie(config)#username admin password ruijie
Ruijie(config)#line console 0
Ruijie(config-line)#login authentication ruijie
Ruijie(config-line)#end
```

4. This example shows how to use local account to be the enable password

```
Ruijie(config)#aaa new-model ----->enable AAA
Ruijie(config)#aaa authentication enable default local ----->define authentication enable method list named ruijie
and first method is local account.
Ruijie(config)#username admin password ruijie
```

5. This example shows how to grant account privilege level 15, so that this account acquire "#" privilege mode **immediately when logs in**

```
Ruijie(config)#username admin password ruijie
Ruijie(config)#username admin privilege 15
```

6. This example shows how to log in a switch through telnet without any authentication:

```
Ruijie(config)#aaa new-model
Ruijie(config)#aaa authentication login default none
Ruijie(config)#line vty 0 4
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#end
```

Note: We don't suggest you to do this kind of non-authentication

2.9.5.7.2 Athorization

Overview

The AAA authorization enables the administrator to control the user's use of the services or the rights. After the AAA authorization service is enabled, the network device configures the user sessions by using the user configuration file stored

locally or in the server. After the authorization is completed, the user can only use the services allowed in the profile or has the allowed rights.

Authorization Types

Ruijie product supports the following AAA authorization methods:

Exec authorization method – the user terminal logs in the NAS CLI and is granted the privilege level (0-15 level).

Command authorization method – after the user terminal logs in the NAS CLI, the specific commands are authorized.

Network authorization method – grant the available service to the user session in the network.

Introduction and limits of privilege 1-15 for Ruijie production explain as below :

Level 0: the lowest level (like Ruijie>), only several commands are granted ----ping , traceroute and enable

Level 1: normal user level (like Ruijie>), "show" command is added compare with level 0.

Level 2-14 : ordinary administrator (like Ruijie#), most operations (like configuring , showing , modifying)are allowed , but a few of High-risk operations (like delete. modify files, reload) are forbidden

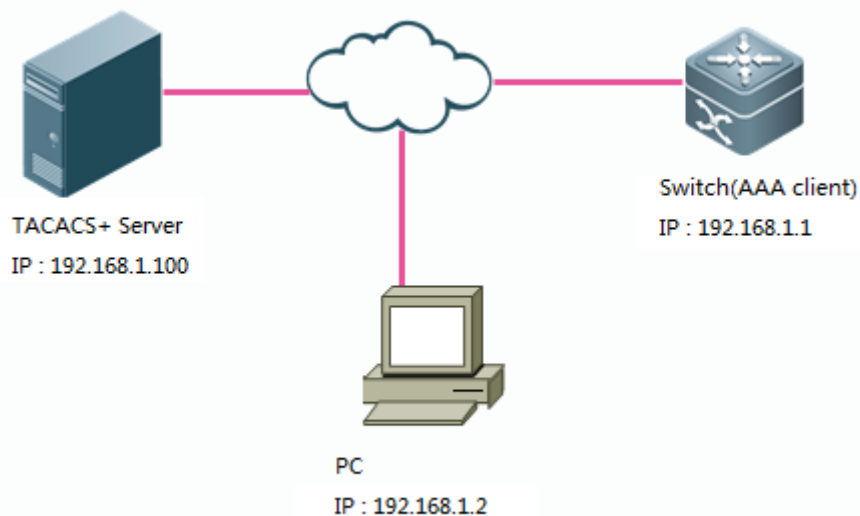
Level 15: Super administrator (Ruijie#) , highest level , unlimite to do anything

Only TACACS+ supports the command authorization method. For the detailed information, please refer to TACACS+ Configuration

I. Requirements

Tacacs+ server authenticate users when user logs in through telnet ,then TACACS+ Server grants user corresponding privilege .

II. Network Topology



III. Configuration Tips

1. Configure basic route to ensure switch , TACACS+ Server and PC can communicate with each other , then configure aaa authentication
2. Define AAA authorization list and apply AAA authorization list on VTY line
3. Create local username and password
4. Configure TACACS+ Server

IV. Configuration Steps

1. Configure basic route to ensure switch , TACACS+ Server and PC can communicate with each other , then configure aaa authentication

See [chapter AAA--->Authentication](#)

2. Define AAA authorization list and apply AAA authorization list on VTY line

```
Ruijie(config)#aaa authorization exec execauth group tacacs+ local ----->define authorization exec method
named "execauth" and first method is tacacs ,fallback method is local.
Ruijie(config)#line vty 0 4
Ruijie(config-line)#authorization exec execauth ----->apply authorization method "execauth" on VTY
```

3. Define local account

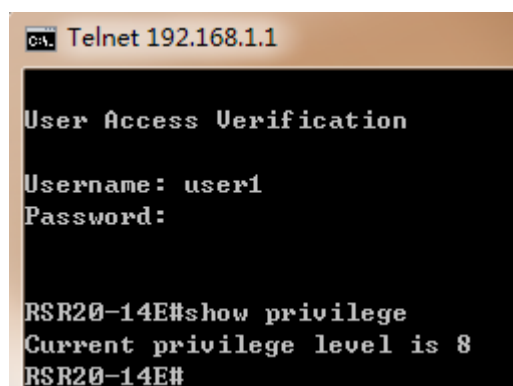
```
Ruijie(config)#username ruijie password ruijie ----->configure local account :username "ruijie" password
"ruijie"
Ruijie(config)#username ruijie privilege 8 ----->grant account "ruijie" privilege level 8
```

4. Configure TACACS+

Configuration of different TACACS+ servers vary, See relevant configuration guide.

V. Verification

Verify that the user requires privilege mode (level 8) immediately log in the switch.



```
C:\> Telnet 192.168.1.1

User Access Verification

Username: user1
Password:

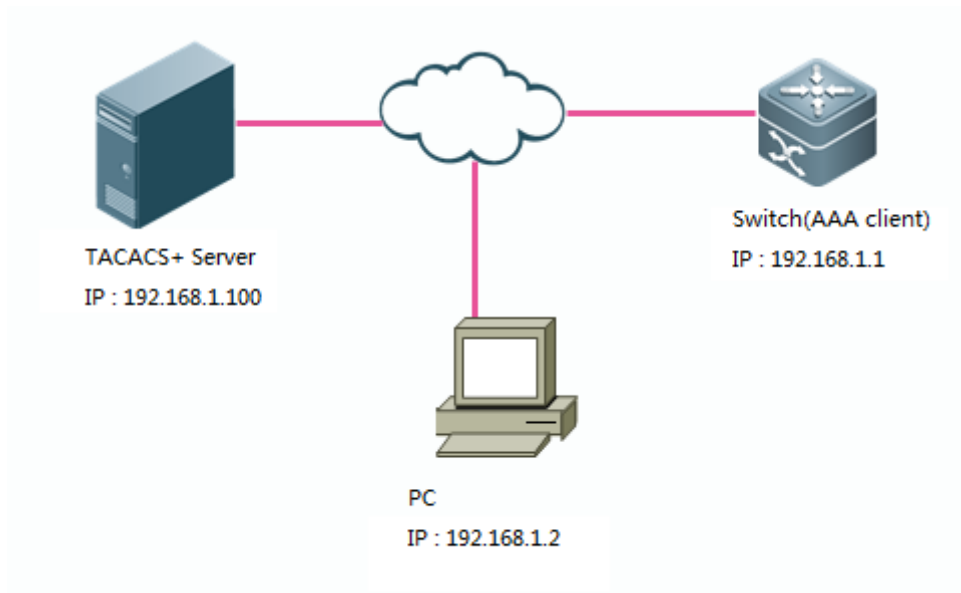
RSR20-14E#show privilege
Current privilege level is 8
RSR20-14E#
```

Configuring command authorization

I. Requirements

Tacacs+ server authenticates user when user logs in through telnet, and user can use "show" and "ping" command only.

II. Network Topology



III. Configuration Tips

1. Configure basic route to ensure switch, TACACS+ Server and PC can communicate with each other , then configure aaa authentication
2. Configure login authorization
3. Define authorization command method
4. Configure TACACS+ Server

IV. Configuration Steps

1. **Configure basic route to ensure switch , TACACS+ Server and PC can communicate with each other , then configure aaa authentication**

See [chapter AAA--->Authentication](#)

2. **Configure login authorization**

Note:

You must assign privilege level 15 to user if user needs to execute "show run" , otherwise system returns an error message "unknown command"

See [Chapter AAA--->Athorization--->Configuring login authorization](#)

3. Define authorization command method

Note:

- 1) You must specify authorization methods for each privilege level from 0 to 15 independently on Ruijie device .
- 2) By default , switch has applied authorization methods "default" on VTY Line , otherwise you must specify authorization methods on VTY line.

This example shows how to specify authorization methods for different privilege level from 0 to 15.

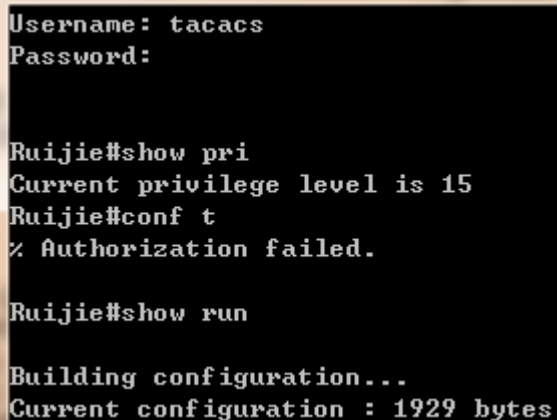
```
Ruijie(config)#aaa authorization commands 0 default group tacacs+ local
Ruijie(config)#aaa authorization commands 1 default group tacacs+ local
Ruijie(config)#aaa authorization commands 2 default group tacacs+ local
Ruijie(config)#aaa authorization commands 3 default group tacacs+ local
Ruijie(config)#aaa authorization commands 4 default group tacacs+ local
Ruijie(config)#aaa authorization commands 5 default group tacacs+ local
Ruijie(config)#aaa authorization commands 6 default group tacacs+ local
Ruijie(config)#aaa authorization commands 7 default group tacacs+ local
Ruijie(config)#aaa authorization commands 8 default group tacacs+ local
Ruijie(config)#aaa authorization commands 9 default group tacacs+ local
Ruijie(config)#aaa authorization commands 10 default group tacacs+ local
Ruijie(config)#aaa authorization commands 11 default group tacacs+ local
Ruijie(config)#aaa authorization commands 12 default group tacacs+ local
Ruijie(config)#aaa authorization commands 13 default group tacacs+ local
Ruijie(config)#aaa authorization commands 14 default group tacacs+ local
Ruijie(config)#aaa authorization commands 15 default group tacacs+ local
```

4. Configure Tacacs server

Configuration of different TACACS+ servers vary .See relevant configuration guide.

V. Verification

When you log in, you can execute "show run" and "ping" command only.



```
Username: tacacs
Password:

Ruijie#show pri
Current privilege level is 15
Ruijie#conf t
% Authorization failed.

Ruijie#show run

Building configuration...
Current configuration : 1929 bytes
```

2.9.5.7.3 Accounting

Overview

The AAA accounting function enables you to trace the services and network resources used by the user. After the accounting function is enabled, the network access server or router sends the user's network accesses to the Radius security server by means of attribute pair. You may use some analysis software to analyze these data to implement the billing, audition and tracing function for the user's activities.

Accounting Types

Our product currently supports the following accounting types:

Exec Accounting -- record the accounting information of entering to and exiting from the CLI of the user terminal logged in the NAS CLI.

Command Accounting – record the specific command execution information after the user terminal logs in the NAS CLI.

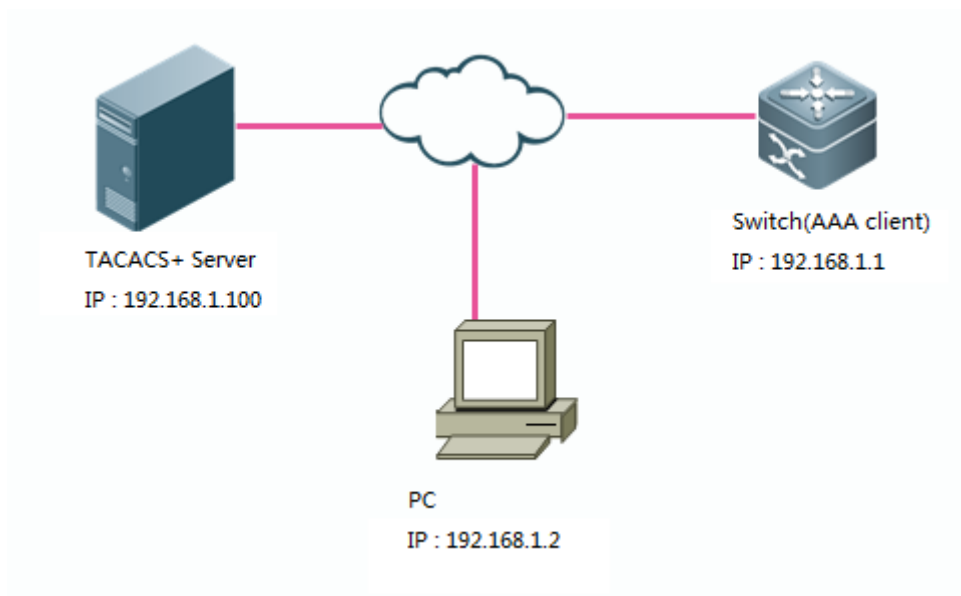
Network Accounting – records the related information on the user session in the network.

Only TACACS+ supports the command accounting function. For the detailed information, please refer to TACACS+ Configuration.

I. Requirements

1. Tacacs+ Server accounts when user logs in and logs out
2. Tacacs+ Server accounts when user enters commands

II. Network Topology



III. Configuration Tips

1. Configure basic route to ensure switch, TACACS+ Server and PC can communicate with each other , then configure aaa login authentication
2. Define AAA accounting method and apply AAA authorization method on VTY line

IV. Configuration Steps

Tacacs+ Server accounts when user logs in and logs out

1. **Configure basic route to ensure switch , TACACS+ Server and PC can communicate with each other , then configure aaa login authentication**

See [Chapter AAA--->Authentication--->Configuring login authentication using Radius](#)

2. **Define AAA accounting method and apply AAA authorization method on VTY line**

```
Ruijie(config)#aaa accounting exec execaccout start-stop group tacacs+ //define accounting method named
"execaccout"
Ruijie(config)#line vty 0 4
Ruijie(config-line)#accounting exec execaccout
```

Tacacs+ Server accounts when user enters commands

1. **Configure basic routing and aaa login parameters**

See [Chapter AAA--->Authentication--->Configuring login authentication using Radius](#)

2. **Define AAA accounting method and apply AAA authorization method on VTY line**

Note:

You must specify accounting methods for each privilege level from 0 to 15 independently on Ruijie device .

This example shows how to spacificy accounting methods for different privilge level from 0 to 15.

```
Ruijie(config)#aaa accounting commands 0 commaccout start-stop group tacacs+ //Define method named
"commaccout"
Ruijie(config)#aaa accounting commands 1 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 2 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 3 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 4 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 5 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 6 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 7 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 8 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 9 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 10 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 11 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 12 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 13 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 14 commaccout start-stop group tacacs+
Ruijie(config)#aaa accounting commands 15 commaccout start-stop group tacacs+

Ruijie(config)#line vty 0 4
Ruijie(config-line)#accounting commands 0 commaccout //apply accounting method "commaccout" on vty line
Ruijie(config-line)#accounting commands 1 commaccout
Ruijie(config-line)#accounting commands 2 commaccout
Ruijie(config-line)#accounting commands 3 commaccout
Ruijie(config-line)#accounting commands 4 commaccout
Ruijie(config-line)#accounting commands 5 commaccout
Ruijie(config-line)#accounting commands 6 commaccout
Ruijie(config-line)#accounting commands 7 commaccout
Ruijie(config-line)#accounting commands 8 commaccout
Ruijie(config-line)#accounting commands 9 commaccout
Ruijie(config-line)#accounting commands 10 commaccout
Ruijie(config-line)#accounting commands 11 commaccout
Ruijie(config-line)#accounting commands 12 commaccout
Ruijie(config-line)#accounting commands 13 commaccout
Ruijie(config-line)#accounting commands 14 commaccout
Ruijie(config-line)#accounting commands 15 commaccout
```

V. Verification

1. Tacacs+ Server accounts when user logs in and logs out

This example shows the entries about logs in and logs out on cisco ACS :

The screenshot shows the Cisco Systems Reports and Activity interface. On the left, a sidebar lists various reports, with 'TACACS+ Accounting' highlighted. The main panel displays 'TACACS+ Accounting' with a table of log entries. The table has columns: Date, Time, User-Name, Group-Name, Caller-Id, Acct-Flags, elapsed time, and service. Two entries are visible for user3 on 03/13/2013.

| Date | Time | User-Name | Group-Name | Caller-Id | Acct-Flags | elapsed time | service |
|------------|----------|-----------|---------------|-------------|------------|--------------|---------|
| 03/13/2013 | 18:39:14 | user3 | Default Group | 192.168.1.2 | stop | 19 | shell |
| 03/13/2013 | 18:38:55 | user3 | Default Group | 192.168.1.2 | start | .. | shell |

2. Tacacs+ Server accounts when user enters commands

This example shows the entries about command accounting on cisco ACS :

The screenshot shows the Cisco Systems Reports and Activity interface. On the left, a sidebar lists various reports, with 'TACACS+ Administration' highlighted. The main panel displays 'Tacacs+ Administration activity' with a table of log entries. The table has columns: Date, Time, User-Name, Group-Name, cmd, priv-lvl, and service. Six entries are visible for user3 on 03/13/2013.

| Date | Time | User-Name | Group-Name | cmd | priv-lvl | service |
|------------|----------|-----------|---------------|---------------------|----------|---------|
| 03/13/2013 | 19:04:05 | user3 | Default Group | show version <cr> | 1 | shell |
| 03/13/2013 | 19:03:59 | user3 | Default Group | show clock <cr> | 1 | shell |
| 03/13/2013 | 19:03:49 | user3 | Default Group | show privilege <cr> | 1 | shell |
| 03/13/2013 | 19:03:39 | user3 | Default Group | exit <cr> | 0 | shell |
| 03/13/2013 | 19:03:36 | user3 | Default Group | exitt <cr> | 0 | shell |
| 03/13/2013 | 19:03:35 | user3 | Default | exit <cr> | 0 | shell |

2.9.5.8 ACL

2.9.5.8.1 Anti-virus ACL

Overview

ACL is the shortened form of Access Control List, or Access List. It is also popularly called firewall, or packet filtering in some documentation. ACL controls the messages on the device interface by defining some rules: Permit or Deny.

According to usage ranges, they can be divided into ACLs and QoS ACLs. By filtering the data streams, you can restrict the communication data types in the network and restrict the users of the network and the device they can use. When data streams pass the switch, ACLs classify and filter them, that is, check the data streams input from the specified interface and determine whether to permit or deny them according to the matching conditions. To sum up, the security ACL is used to control which dataflow is allowed to pass through the network device. The QoS policy performs priority classification and processing for the dataflow.

ACLs consist of a series of entries, known as Access Control Entry (ACE). Each entry specifies its matching condition and behavior. Access list rules can be about the source addresses, destination addresses, upper layer protocols, time-ranges or other information of data flows.

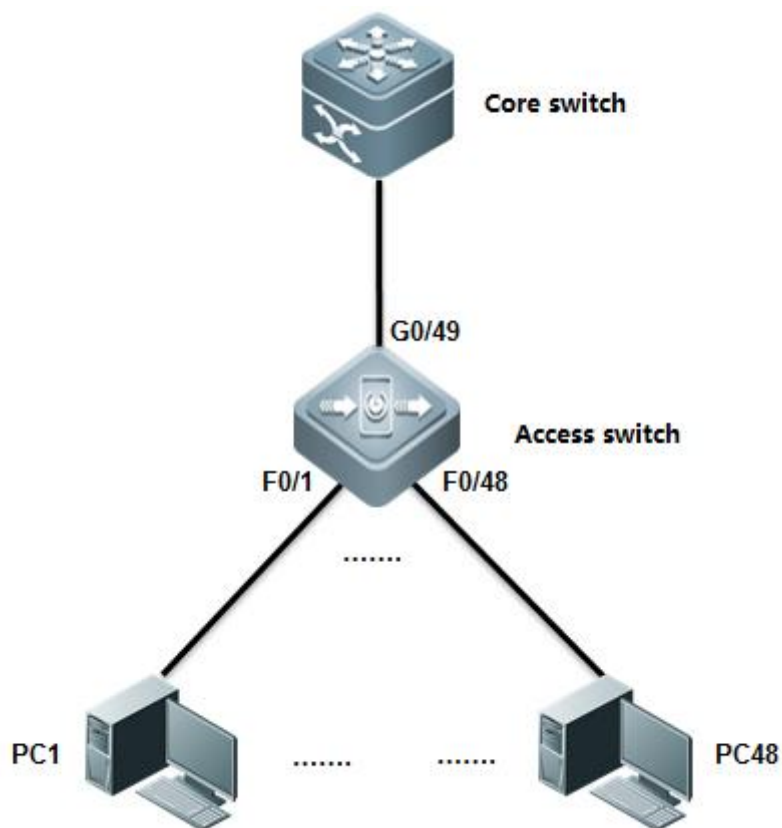
I. Requirements

Administrator wants to deploy anti-virus ACL on Access switch to filter common virus port and enhance network security .

II. Configuration Tips

1. Create extended ACL and define ACE
2. Apply ACL on interfaces
3. Add and delete Access Control Entry(ACE).

III. Network Topology



IV. Configuration Steps

Configuring Access switch:

1. Create extended ACL and define ACE

```
Ruijie# configure terminal
Ruijie(config)# ip access-list extended  defencevirus          ----->create an extended ACL named defencevirus
Ruijie(config-ext-nacl)# 10 deny tcp any any eq 27665        ----->specify virus ports. These information comes from daily practice
Ruijie(config-ext-nacl)# 20 deny tcp any any eq 16660
Ruijie(config-ext-nacl)# 30 deny tcp any any eq 65000
Ruijie(config-ext-nacl)# 40 deny tcp any any eq 33270
Ruijie(config-ext-nacl)# 50 deny tcp any any eq 39168
Ruijie(config-ext-nacl)# 60 deny tcp any any eq 6711
Ruijie(config-ext-nacl)# 70 deny tcp any any eq 6712
Ruijie(config-ext-nacl)# 80 deny tcp any any eq 6776
```

```
Ruijie(config-ext-nacl)# 90 deny tcp any any eq 6669
Ruijie(config-ext-nacl)# 100 deny tcp any any eq 2222
Ruijie(config-ext-nacl)# 110 deny tcp any any eq 7000
Ruijie(config-ext-nacl)# 120 deny tcp any any eq 135
Ruijie(config-ext-nacl)# 130 deny tcp any any eq 136
Ruijie(config-ext-nacl)# 140 deny tcp any any eq 137
Ruijie(config-ext-nacl)# 150 deny tcp any any eq 138
Ruijie(config-ext-nacl)# 160 deny tcp any any eq 139
Ruijie(config-ext-nacl)# 170 deny tcp any any eq 445
Ruijie(config-ext-nacl)# 180 deny tcp any any eq 4444
Ruijie(config-ext-nacl)# 190 deny tcp any any eq 5554
Ruijie(config-ext-nacl)# 200 deny tcp any any eq 9996
Ruijie(config-ext-nacl)# 210 deny tcp any any eq 3332
Ruijie(config-ext-nacl)# 220 deny tcp any any eq 1068
Ruijie(config-ext-nacl)# 230 deny tcp any any eq 455
Ruijie(config-ext-nacl)# 240 deny udp any any eq 31335
Ruijie(config-ext-nacl)# 250 deny udp any any eq 27444
Ruijie(config-ext-nacl)# 260 deny udp any any eq 135
Ruijie(config-ext-nacl)# 270 deny udp any any eq 136
Ruijie(config-ext-nacl)# 280 deny udp any any eq netbios-ns
Ruijie(config-ext-nacl)# 290 deny udp any any eq netbios-dgm
Ruijie(config-ext-nacl)# 300 deny udp any any eq netbios-ss
Ruijie(config-ext-nacl)# 310 deny udp any any eq 445
Ruijie(config-ext-nacl)# 320 deny udp any any eq 4444
Ruijie(config-ext-nacl)# 330 permit ip any any
Ruijie(config-ext-nacl)#exit
```

2. Apply ACL on interfaces

```
Ruijie(config)#interface range fastEthernet 0/1-24
Ruijie(config-if-range)#ip access-group defencevirus in
```

3. ACE Add and delete ACE

```
Ruijie(config-ext-nacl)#15 deny tcp any any eq 707 ----->insert No.15 ACE between No.10 and No.20 .
Ruijie(config-ext-nacl)#no 15 ----->delete No.15
```

Note: ACL enforces in hardware , so ACL is not applied if there are insufficient hardware resource available .

V. Verification

How to display ACL configuration and status

```
Ruijie(config)#show ip access-group ----->where ACL apply
ip access-group defencevirus in
Applied On interface GigabitEthernet 0/1.
Ruijie# show access-lists ----->show ACL configuration
ip access-list extended defencevirus
 10 deny tcp any any eq 27665
 15 deny tcp any any eq 707
 20 deny tcp any any eq 16660
 30 deny tcp any any eq 65000
 40 deny tcp any any eq 33270
 50 deny tcp any any eq 39168
 60 deny tcp any any eq 6711
 70 deny tcp any any eq 6712
 80 deny tcp any any eq 6776
 90 deny tcp any any eq 6669
100 deny tcp any any eq 2222
110 deny tcp any any eq 7000
120 deny tcp any any eq 135
130 deny tcp any any eq 136
140 deny tcp any any eq 137
150 deny tcp any any eq 138
160 deny tcp any any eq 139
170 deny tcp any any eq 445
180 deny tcp any any eq 4444
190 deny tcp any any eq 5554
200 deny tcp any any eq 9996
```

```
210 deny tcp any any eq 3332
220 deny tcp any any eq 1068
230 deny tcp any any eq 455
240 deny udp any any eq 31335
250 deny udp any any eq 27444
260 deny udp any any eq 135
270 deny udp any any eq 136
280 deny udp any any eq netbios-ns
290 deny udp any any eq netbios-dgm
300 deny udp any any eq netbios-ss
310 deny udp any any eq 445
320 deny udp any any eq 4444
330 permit ip any any
```

6. Configuration Script

```
ip access-list extended defencevirus
10 deny tcp any any eq 27665
20 deny tcp any any eq 16660
30 deny tcp any any eq 65000
40 deny tcp any any eq 33270
50 deny tcp any any eq 39168
60 deny tcp any any eq 6711
70 deny tcp any any eq 6712
80 deny tcp any any eq 6776
90 deny tcp any any eq 6669
100 deny tcp any any eq 2222
110 deny tcp any any eq 7000
120 deny tcp any any eq 135
130 deny tcp any any eq 136
140 deny tcp any any eq 137
150 deny tcp any any eq 138
160 deny tcp any any eq 139
```

```
170 deny tcp any any eq 445
180 deny tcp any any eq 4444
190 deny tcp any any eq 5554
200 deny tcp any any eq 9996
210 deny tcp any any eq 3332
220 deny tcp any any eq 1068
230 deny tcp any any eq 455
240 deny udp any any eq 31335
250 deny udp any any eq 27444
260 deny udp any any eq 135
270 deny udp any any eq 136
280 deny udp any any eq netbios-ns
290 deny udp any any eq netbios-dgm
300 deny udp any any eq netbios-ss
310 deny udp any any eq 445
320 deny udp any any eq 4444
330 permit ip any any
```

3.9.5.8.2 TCP Unidirectional control ACL

Overview

By filtering the packets of TCP SYN initialization, you can block the TCP traffic from stations in lower security zone to that in higher security zone. As per the process of TCP connection, the first TCP initialization packet in which the SYN bit is set to 1 and the ACK bit is set to 0. Therefore, you can use ACL to block this kind of packet to filter the subsequence TCP traffic from lower security zone to higher security zone in the one-way direction

This feature is especially suitable for Servers, such as FTP , WEB ,that provides services for internet users . Users from internet is allowed to visit these servers, but servers are forbidden to visit the internet.

This feature of Access Lists don't have any impact on traffic of ICMP and UDP

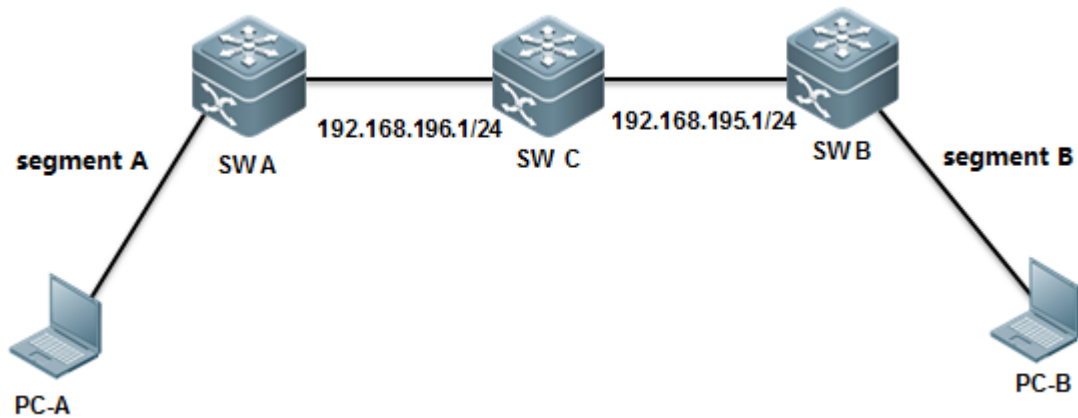
I. Requirements

There're two subnets in the network : subnet A 192.168.200.0/24 and subnet B 192.168.100.0/24.Stations in subnet A can visit stations in subnet B through TCP , but stations in subnet B cannot visit stations in subnet B through TCP.

II. Configuration Tips

ACL can block TCP traffic by filtering the TCP packet in which SYN bit is 1 and ACK bit is 0.

III. Network Topology



IV. Configuration Steps

Scheme 1: Apply ACL on Switch B

Configuring Switch B:

```

Ruijie# configure terminal
Ruijie(config)# ip access-list extended 101 ----->create extended ACL 101
Ruijie(config-ext-nacl)# deny tcp 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255 match-all syn ----->deny TCP
TCP packets in which Syn bit is 1 and other bit is 0(includes ACK bit)
Ruijie(config-ext-nacl)# permit ip any any ----->permit any other traffic
Ruijie(config-ext-nacl)# exit
Ruijie(config)# interface gigabitEthernet 3/2
Ruijie(config-if)# ip access-group 101 in ----->apply ACL 101 on the interface in the
input direction
Ruijie(config-if)#end
Ruijie#wr
  
```

Scheme 2: Apply ACL on Switch A

```

Ruijie# configure terminal
Ruijie(config)# ip access-list extended 101 ----->create extended ACL 101
Ruijie(config-ext-nacl)# deny tcp 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255 match-all syn ----->deny
TCP packets in which Syn bit is 1 and other bit is 0(includes ACK bit)
Ruijie(config-ext-nacl)# permit ip any any ----->permit any other traffic
Ruijie(config-ext-nacl)# exit
Ruijie(config)# interface VLAN 100
  
```

```
Ruijie(config-if-VLAN100)# ip access-group 101 out ----->apply ACL 101 on the SVI in the output
direction
Ruijie(config-if)#end
Ruijie#wr
```

V. Verification

How to display ACL configuration:

```
Ruijie# show access-lists 101
ip access-list extended 101
10 deny tcp 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255 match-all syn
20 permit ip any any
```

Verify that stations in subnet B cannot initialize TCP connection to stations in subnet A ,but they can still communicate with each other on ICMP and UDP

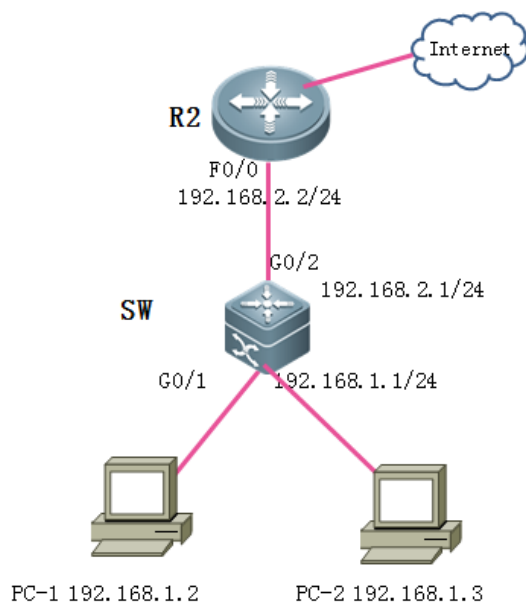
3.9.5.8.3 Time-based ACL

I. Requirements

Filter the traffic from stations in Intranet to Internet during office hour(from 9:00 am to 12:00 am and 14:00 pm to 18:00 pm) and permit this traffic in any other time.

Stations in Intranet can communicate with each other unlimited.

II. Network Topology



III. Configuration Tips

1. Correct switch clock, because time-based ACL refers to switch clock.
2. When define a time-range, you cannot define a time-range that across 00:00. For example, If you want to define a time-range from 10:00 pm to 7:00 am :

```
Ruijie(config)#time-range aaa
Ruijie(config-time-range)#periodic daily 0:00 to 7:00
Ruijie(config-time-range)#periodic daily 22:00 to 23:59
```

3. Both standard and extend ACL support time-range ACL

IV. Configuration Steps

1. Correct switch clock

```
Ruijie>enable
Ruijie(config)#clock timezone beijing 8 -----> set timezone to UTC+8
Ruijie(config)#exit
Ruijie#clock set 10:00:00 12 1 2012 -----> hour:minute:second month day year
```

2. Define time-range

```
Ruijie(config)#time-range work ----->define a time-range named work
Ruijie(config-time-range)#periodic daily 9:00 to 12:30
Ruijie(config-time-range)#periodic daily 14:00 to 18:30
Ruijie(config-time-range)#exit
```

3. Create a ACL and define ACE

```
Ruijie(config)#ip access-list extended 100
Ruijie(config-ext-nacl)#5 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.255.255 ----->permit any traffic between
stations in intranet
Ruijie(config-ext-nacl)#10 deny ip 192.168.1.0 0.0.0.255 any time-range work ----->deny any traffic from
192.168.1.0/24 to Internet during work time
Ruijie(config-ext-nacl)#20 permit ip any any ----->permit any other traffic(you must configure this command ,
because there's an implicit deny any in the end)
Ruijie(config-ext-nacl)#exit
```

4. Apply ACL on interface

```
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip access-group 100 in ----->apply ACL 100 on interface connected to
intranet
```

5. Save configuration

```
Ruijie(config-if-GigabitEthernet 0/1)#end
Ruijie#write
```

V. Verification

1) How to display system clock

```
Ruijie#show clock
10:14:01 beijing Sat, Dec 1, 2012
```

2) How to display ACL configuration

```
Ruijie#show access-lists
ip access-list extended 100
  5 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.255.255
  10 deny ip 192.168.1.0 0.0.0.255 any time-range work (active)
  20 permit ip any any
```

----->red mark "active" indicates that it is office time now

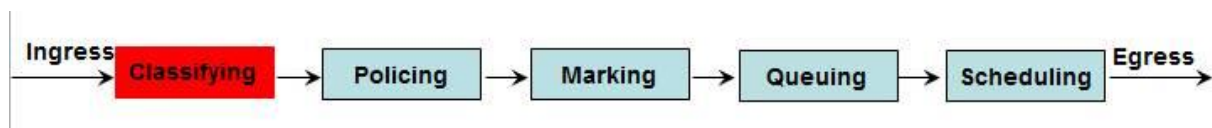
3) How to display ACL status

```
Ruijie#show ip access-group
ip access-group 100 in
Applied On interface GigabitEthernet 0/1.
```

3.9.6 QoS

3.9.6.1 Working Principles and Basic Configuration

QoS on Switches



Note: The preceding figure shows the QoS data processing process. The following describes the functions of each step.

1. Classifying

Classify the incoming data traffic into non-IP data traffic and IP data traffic and labels the two data traffic types with different differentiated services code point (DSCP) values.

DSCP labeling for non-IP data traffic

Method 1: On the ingress interface, configure the policy mapping.

```
Mac access-list extended mac_acl
  permit ...
  class-map mac_class
  match access-group mac_acl
```

```
policy-map mac_policy
  class mac_class
    set cos 6

interface Gi0/1
  service-policy input mac_policy
```

The obtained CoS information is mapped based on the CoS-to-DSCP MAP table.

In this way, the data traffic is labeled with DSCP values.

Method 2: Enable the port trust mode CoS on the ingress port. If the L2 header of the packet

```
interface Gi0/1
  mls qos trust cos
```

Contains CoS, the CoS value (contained in the VLAN Tag field) is obtained from the packet.

The obtained coS information is mapped based on the CoS-to-DSCP MAP table.

In this way, the data traffic is labeled with SDGP values.

Method 3: Enable the port trust mode CoS on the ingress port. If the L2 header of the packet

```
interface Gi0/1
  mls qos trust cos
  mls qos cos 6
```

Does not contain CoS, obtain the CoS value of the packet according to the default CoS value of the ingress interface.

The obtained CoS information is mapped based on the CoS-to-DSCP MAP table.

In this way, the data traffic is labeled with DSCP values.

Note

1. The above criteria 2, 3 take effect only when the QoS trust mode of the port is enabled. Enabling the QoS trust mode of a port does not mean getting the QoS information directly from the message or the input port of the message without analyzing the message contents.
2. The above three criteria may apply simultaneously on the same port. In this case, they will take effect according to the sequence 1, then 2 and then 3. In other words, the ACLs work first for the classifying operation. When it fails, the criteria 2 will be used, and so on. Here, if the QoS trust mode of the port is enabled, criteria 2 and 3 will be used to get the QoS information directly from the message or the port; otherwise, default DSCP value 0 will be assigned for the messages failing the classifying operation.

DSCP labeling for IP data traffic

Method 1: On the ingress interface, use the mapping table based on the applied policy.

Method 2: Enable the port trust mode IP precedence on the ingress port. Obtain the IP precedence information from the IP packet header.

The obtained IP precedence information is mapped based on the ip-prec-dscp MAP table.

In this way, the data traffic is labeled with DSCP values.

Method 3: Enable the port trust mode COS on the ingress interface to obtain the COS information of the packet.

There are two situations as follows:

1. The L2 header does not contain COS. In this case, the COS information of the packet is obtained based on the default COS of the ingress interface.
2. The L2 header contains COS. In this case, the COS information of the packet is directly obtained from the L2 header.

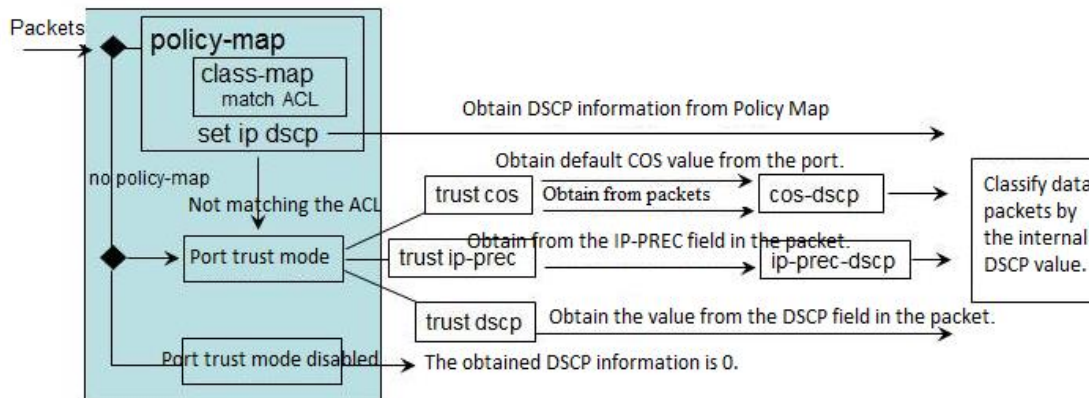
The obtained CoS information is mapped based on the CoS-DSCP MAP table.

In this way, the data traffic is labeled with DSCP values.

Method 4: Enable the port trust mode DSCP on the ingress port. Obtain the DSCP information from the IP packet header.

2. Summary

The incoming data traffic is classified into non-IP data traffic and IP data traffic.



```
Ruijie(config)# policy-map policy-map-name
Ruijie(config-pmap)#class class-map-name
Ruijie(config-pmap-c)#police rate-bps burst-byte [exceed-action {drop | dscp dscp-value}]
```

rate-bps is the second (kbps)

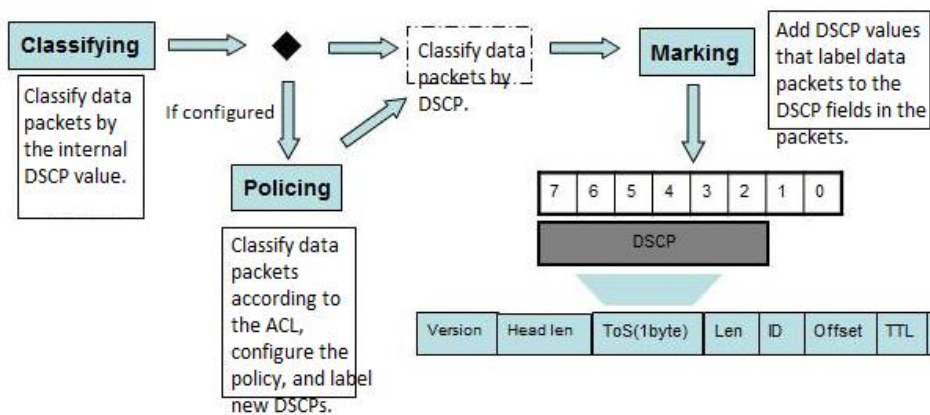
burst-byte is the bandwidth (Kbyte)

Apply police-map into interface

```
Ruijie(config-if)#service-policy input policy-map-name
```

Note: When one mapping policy is applied on multiple ports, the rate restriction bandwidth of each port is independent from each other.

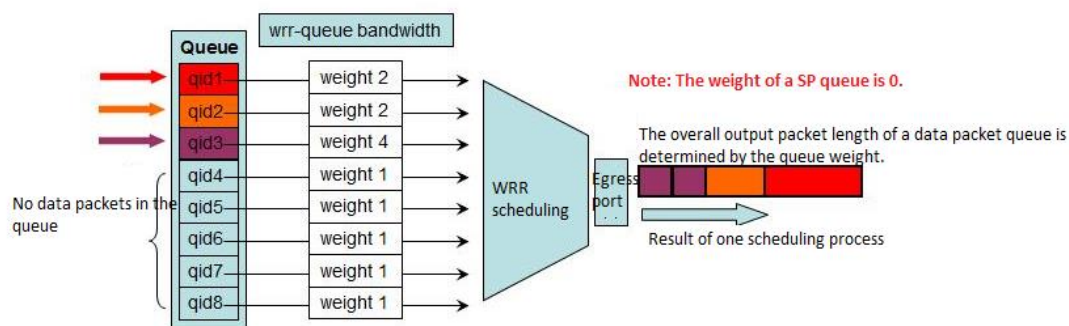
3. Marking:

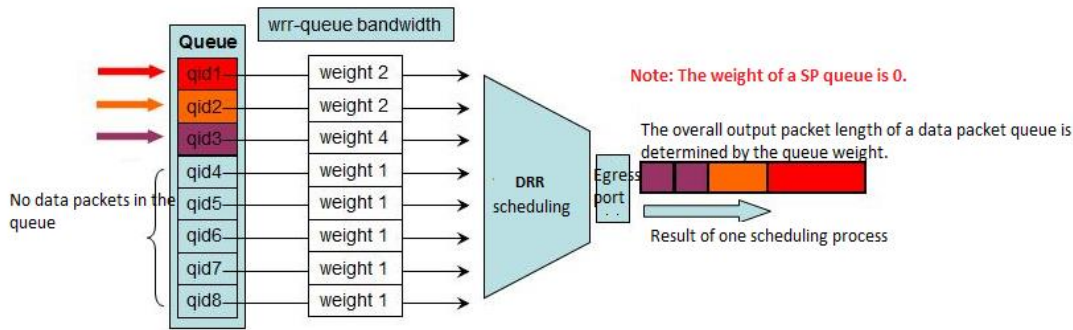


The DSCP-to-CoS Map table and CoS-to-Queue Map table are the default ones on the device.

The CoS-Map table is a default mapping table of CoS values and queues.

| CoS 值 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|-------|---|---|---|---|---|---|---|---|
| 队列 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |





Configuration method:

1. Select the output queue scheduling algorithm.
2. Configure the scheduling weight for the output queue.

Weight of queue 1 Weight of queue 8

```
Ruijie(config)# {wrr-queue | drr-queue} bandwidth weight1 ... weight8
```

When the weight (WRR/DRR) is set to **0**, SP scheduling is used for the queue. The following is an example describing how to configure the SP+DRR or SP+WRR scheduling algorithm.

SP+DRR/SP+WRR Scheduling Configuration on Switch 11x

The SP group queue features the top priority. The DRR group queue is scheduled only when the SP queue is empty.

| Group type | SP0 | SP0 | DRR0 | DRR0 | DRR0 | SP1 | DRR1 | DRR1 |
|------------|-----|-----|------|------|------|-----|------|------|
| Queue | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Weight | 0 | 0 | 1 | 2 | 3 | 0 | 1 | 1 |

Different from that on type-A switches, the scheduling sequence is SP1, SP0, and other DRR queues in weight sequence.

3.9.6.2 Rate Limit on Ports

Scenario

The QoS Policy Map table can be correlated to the ACL for rate limit on certain types of traffic (for example, HTTP traffic and traffic of users on the xx network segment). As the ACL can be configured flexibly, different traffic types can be set with different rate limits. Regardless of the configuration complexity, you can take the method into consideration if necessary.

The rate limit feature supports only unitary rate limit on a port. The function does not differentiate the rate limit by traffic type. It is similar to fixed bandwidth allocation to the port. The method features simple configuration and unitary control.

Function Overview

There are two methods of implementing rate limit on a port of a switch.

1. Create a QoS Policy Map table. Apply the Policy Maps table on the in/out direction of the port to implement rate limit in the in/out direction.
2. Apply the rate limit input/output policy on the port for rate limit in the in/out direction.

Both the QoS rate limit method and the rate limit policy are realized in the hardware level with the two rate three color leaky bucket scheduling (CIR average rate + CBS burst length). The rate limit granule is 64 Kbps and the precision approximately equals packet length / (packet length + interframe spacing + CRC), and the Ethernet interframe spacing and CRC cost is 20 bytes.

The test proves that the shorter a packet is, the lower the precision is. For example, the rate limit precision for packets in the length of 64 bytes is lower than that of 1518 bytes.

Generally, rate limit using the policy map method is carried out based on the leaky bucket algorithm and the rate limit policy is carried out by the register on the port. However, on Ruijie products, both methods are carried out based on the leaky bucket algorithm and feature equal effect.

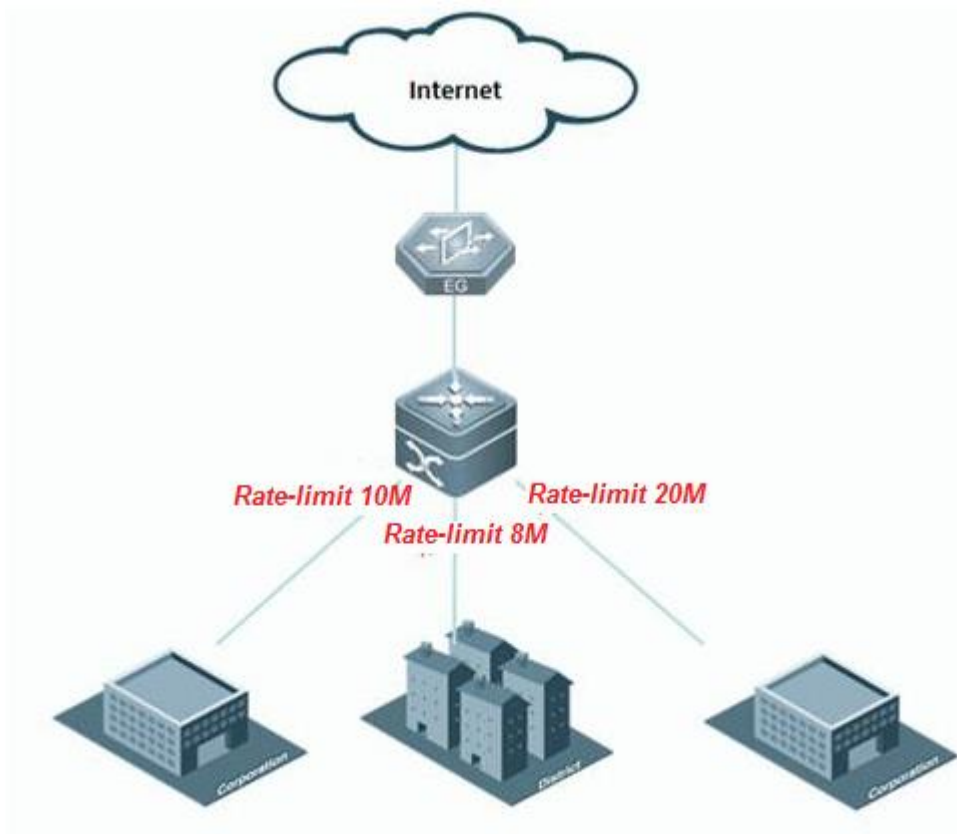
The major difference between the two methods are that the policy map method supports correlation with the ACL and can implement rate limit for packets of certain traffic types (for example, HTTP traffic and traffic of users on the xx network segment), featuring flexible control. The rate limit policy supports only unitary rate limit on a port. The function does not differentiate the rate limit by traffic type, featuring unitary control.

The N18000 series, S8600E, and S7800E support the bi-directional rate limit policy and bi-directional policy map method for rate limit.

I. Networking Requirements

The branches of an organization connect to the core switch through MSTP links and share unified Internet access egresses. As the branches vary in sizes and scales, the network administrator wants to specify uplink and downlink rates for the port of each branch.

II. Network Topology



III. Configuration Tips

1. Use the policy map method to limit the rate.
 - 1) Use the ACL to classify the traffic.
 - 2). Configure a class map table to correlate to the ACL.
 3. Configure a policy map table to correlate to the class map table and set the traffic policy.
 4. Invoke the policy map table on the port.
2. Use the rate limit policy for rate control.
 1. Apply the rate limit policy on the port.

IV. Configuration Steps

1. Use the ACL to classify the traffic.

----->Note:

1. The rate limit command configures not only the rate limits but also the burst rate. The burst rate can be configured in the following way:
 - 1) The value range of the burst rate is (2, 4, 8, 16, 32, 6...1024, 2*1024, 4*1024, 16*1024).
 - 2) A minimum of 200 ms buffering capacity is recommended for the leaky bucket. That is, that minimal recommended value is $(CIR/8)*200ms$, or $Rate\ limit/40$.

3) The burst rate can increase the leaky bucket size for unexpected services, such as video and file transmission, and thereby enhance QoS burst tolerance.

Considering the above three principles, a 2^x most proximate to the value of Rate limit/10 is selected.

2. Configure the rate limit policy for rate control on the port.

1. The rate limit command configures not only the rate limits but also the burst rate. The burst rate can be configured in the following way:

1). The value range of the burst rate is (2, 4, 8, 16, 32, 6...1024, $2*1024$, $4*1024$, $16*1024$).

2). A minimum of 200 ms buffering capacity is recommended for the leaky bucket. That is, that minimal recommended value is $(CIR/8)*200ms$, or Rate limit/40.

3) The burst rate can increase the leaky bucket size for unexpected services, such as video and file transmission, and thereby enhance QoS burst tolerance.

Considering the above three principles, a 2^x most proximate to the value of Rate limit/10 is selected.

Command description:

Input/output: indicates whether the input or output traffic rate is to be limited.

kbps: indicates the upper rate limit in the unit of kbps.

burst-bytes: indicates the burst traffic size (leaky bucket size) in the unit of Kbyte.

V. Verification

1. Run the **Ruijie#show policy-map interface gigabitEthernet 1/1** command to check the QoS policy invoked by the port.
2. Run the **Ruijie#show mls qos rate-limit** command to view the rate limit policy of the port.

3.9.7 Reliability

3.9.7.1 BFD

Overview

BFD can detect linkstatus in micro second and would be suitable for the scenario that requires sensitive delay, less packet loss, like financial industry, ISP, medical industry.

For example, OSPF converge time would be at lease 40s to 50s which is intolerable for intolerability, but if cooperate OSPF with BFD, the converge time would be less than 1s.

BFD can also operate with many other protocol like static route, VRRP, PBR etc.

BFD: (Bidirectional Forwarding Detection)provides low-overhead, short-duration detection ofthe connectivity in the forwarding path between adjacent routers.The fast detection of failures in the forwarding path speeds up enabling the backup forwarding path and improves the network performance. The BFD detection mechanism is independent from the applied interface media type, the encapsulation format mad the associated upper-layer protocols such as OSPF, BGP, RIP.The BFD establishes a session between adjacent routers enables the route protocols to re-calculate the route table by rapidly sending

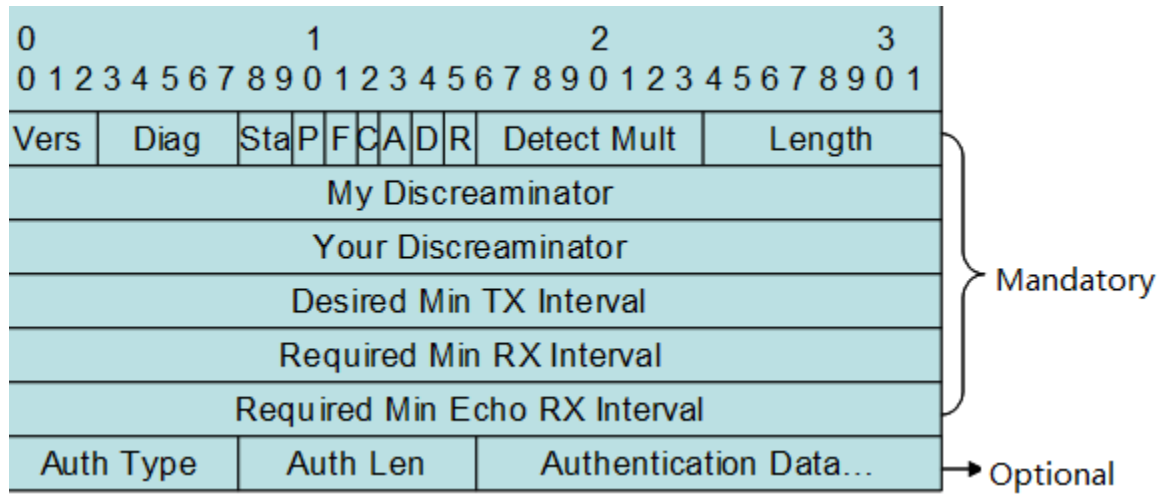
the detection fault to the running route protocols and decreases the network convergence time sharply. The BFD itself cannot discover the neighbors, so it needs the upper-layer protocols to notify the neighbors of which the session is established.

BFD Packet format

BFD uses UDP packets and there're 2 types packets---control and echo.

If one end receives the version 0 control packets from the peer, the default version 1 will automatically switch to version 0 to establish the BFD session. You can use the `show bfd neighbors` command to view the version member.

Format of BFP control packets(version 1) is shown as below:



Vers: BFD protocol version. Currently, the value is 1

Diag: the cause of latest switchover

Sta: Local status of the BFD

P: When a parameter changes, the sender places this flag in a BFD packet, to which the receiver must immediately respond.

F: The packet must have the F flag set for responding to the packet with the P flag set.

C: Forward/control separation flag. Once this flag is set, the change of the control plane does not affect the BFD. For example, if the control plane deploys OSPF, the BFD continues with link status detection when OSPF restarts or performs a graceful restart (GR).

A: Authentication flag. If this flag is set, sessions need to be authenticated.

D: Query demand flag. If this flag is set, the sender expects to detect links in the query mode.

R: Reserved Flag

Detect Mult: Detection timeout multiples. This flag is used by the detector to compute the timeout duration.

Length: Packet length

My Discriminator: Discriminator used by the BFD session to connect to the local end

Your Discriminator: Discriminator used by the BFD session to connect to the remote end

Desired Min Tx Interval: Minimum BFD packet sending interval supported by the local end

Required Min RX Interval: Minimum BFD packet receiving interval supported by the local end

Required Min Echo RX Interval: Minimum echo packet receiving interval supported by the local end. If the local end does not

support the echo function, set the value to 0.

Auth Type: Authentication types, including

Simple Password

Keyed MD5

Meticulous Keyed MD5

Keyed SHA1

Meticulous Keyed SHA1

Auth Length : Authentication data length

Authentication Data: Authentication data area

The UDP port number for control packet is 3784.

The difference between DLDLP and BFD:

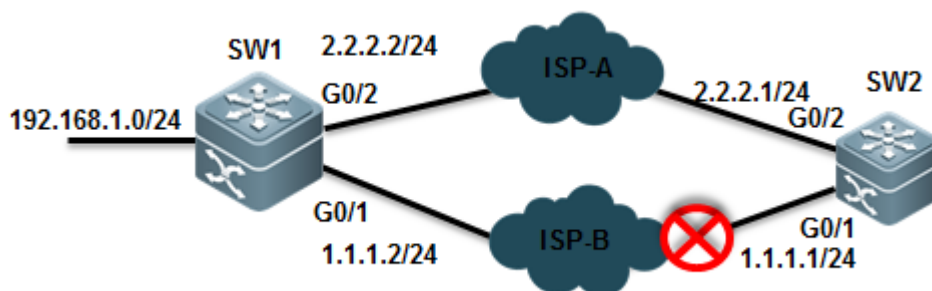
1. You must apply DLDLP on ethernet port , and you can apply BFD between any two hosts regardless port type.
2. DLDLP utilizes ICMP ,and BFD utilizes BFD mechanism.
3. You can apply DLDLP on one end because DLDLP is a unidirection detection , but you must apply BFD on both ends because BFD is a bidirection detection
4. DLDLP bases on port ,and when DLDLP detection failed , DLDLP shuts the port down (for example , SVI , Layer 3 port) and remove all the routes that is related to the port. BFD bases on pairs , when BFD detection failed , BFD controls only the specific route.

BFD with static route

I. Requirements

As figure shown below, SW1 connects to SW2 with two equal access to two different service providers so there're two static routes to the same detination. The static route to ISP-B is a floating route and it is the backup path. Use BFD to detect link availability.

II. Network Topology



III. Configuration Tips

Associate static route with BFD

IV. Configuration Steps

Configuring SW1

1. Assign IP address and configure floating static route

```
SWA(config)#interface gigabitEthernet 0/1
SWA(config-GigabitEthernet 0/1)#no switchport
SWA(config-GigabitEthernet 0/1)#ip address 1.1.1.2 255.255.255.0
SWA(config)#interface gigabitEthernet 0/2
SWA(config-GigabitEthernet 0/2)#no switchport
SWA(config-GigabitEthernet 0/2)#ip address 2.2.2.2 255.255.255.0
SWA(config)#ip route 0.0.0.0 0.0.0.0 g0/1 1.1.1.1 ----->when associate static route with BFD , you
must configure outgoing interface and next hop at the same time . The next hop ip address must be the source ip
address of the BFD peer.
SWA(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1 200 ----->floating static route
```

2. Associate BFD with static route

```
SWA(config)#interface gigabitEthernet 0/1
SWA(config-GigabitEthernet 0/1)#bfd interval 500 min_rx 500 multiplier 3 ----->set BFD time parameter and
enable BFD on the interface. We suggest you to use 500/500/3 value . BFD sends a detection packet every 500ms
and is timeout when BFD doesn't receive replies three times.
SWA(config-GigabitEthernet 0/1)#no bfd echo ----->by default BFD echo mode is on .when a FW or devices
of other vendors connect between two BFD peers , the devices can possible filter BFD packets ,then BFD will fail to
build connections . We suggest you to disable BFD echo.
SWA(config)#ip route static bfd GigabitEthernet 0/1 1.1.1.1 source 1.1.1.2 -----> associate BFD with
static route
```

Configuring SW2:

1. Assign IP address and configure floating static route

```
SWB(config)#interface gigabitEthernet 0/1
SWB(config-GigabitEthernet 0/1)#ip address 1.1.1.1 255.255.255.0
SWB(config)#interface gigabitEthernet 0/2
SWB(config-GigabitEthernet 0/2)#ip address 2.2.2.1 255.255.255.0
SWB(config)#ip route 192.168.1.0 255.255.255.0 1.1.1.2
SWB(config)#ip route 192.168.1.0 255.255.255.0 2.2.2.2 200
```

2. Associate BFD with static route

```
SWB(config)#interface gigabitEthernet 0/1
SWB(config-GigabitEthernet 0/1)#bfd interval 500 min_rx 500 multiplier 3
SWB(config-GigabitEthernet 0/1)#no bfd echo
SWB(config)#ip route static bfd GigabitEthernet 0/1 1.1.1.2 source 1.1.1.1
```

V. Verification

1. How to display BFD neighbor status

```
R1#sh bfd nei
OurAddr          NeighAddr          LD/RD RH/RS      Holdown(mult)  State  Int
1.1.1.2          1.1.1.1            2/1   Up              0(5 ) Up
GigabitEthernet 0/1
```

2. Use "show ip route" EXEC command to display IP route table

3. Use "traceroute" to confirm that SW1 selects ISP-A

4. Shutdown port G0/1 on SW2 to simulate the scenario ISP-A is down, then use "traceroute" to confirm that SW1 selects ISP-B

5. How to display detail BFD neighbor information

```
Ruijie# show bfd neighbors details
OurAddr      NeighAddr    LD/RD  RH/RS  Holdown(mult)  State  Int
1.1.1.2      1.1.1.1      1/2    Up      532 (3 ) Up    GigabitEthernet 0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: route
Uptime: 02:18:49
Last packet: Version: 1      - Diagnostic: 0
I Hear You bit: 1           - Demand bit: 0
Poll bit: 0                  - Final bit: 0
Multiplier: 3                - Length: 24
My Discr.: 2                  - Your Discr.: 1
Min tx interval: 50000        - Min rx interval: 50000
```

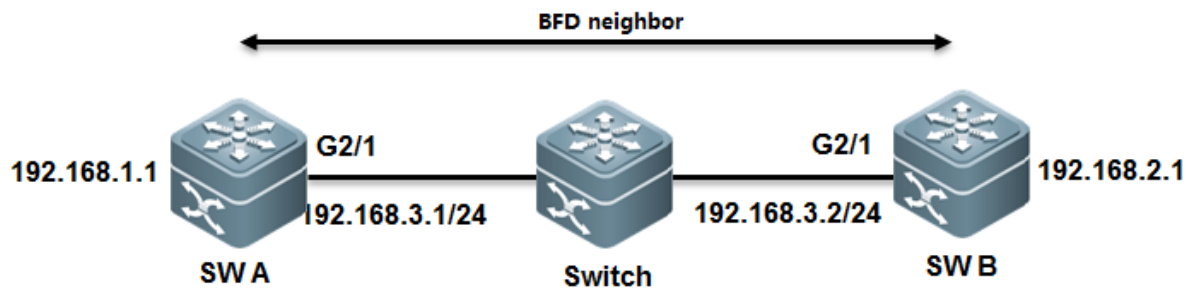
Relevant information

| Field | Description |
|---|---|
| OurAddr | IP address for the session on the local end |
| NeighAddr | IP address for the adjacent session |
| LD/RD | Session discriminator on the local and peer end |
| RH/RS | Current status of the session peer end |
| Holdown(mult) | Time of not receiving the Hello packets on the local end and the detected timeout time of the session |
| State | Current session state |
| Int | Interface number for the session |
| Session state is UP and using echo function with 50 ms interval | Whether the session is in echo mode and the interval of sending frames. This information is shown only in the echo mode |
| Local Diag | Diagnostic information of the session |
| Demand mode | Whether the demand mode is enabled or not |
| Poll bit | Whether the session configuration is modified |
| MinTxInt | Minimum sending interval of the session on the local End |
| MinRxInt | Minimum receiving interval of the session on the local end |
| Multiplier | Timeout times detected on the local end |
| Received MinRxInt | Minimum sending interval of the session on the peer end |
| Received Multiplier | Timeout times detected on the peer end |
| Holdown (hits) | Session detection time and the detected timeout times |
| Hello (hits) | Minimum interval of receiving the Hello packet after the session negotiation |
| Rx Count | Count of BFD packets received on the local end |
| Rx Interval (ms) min/max/avg | Minimum/maximum/average interval of receiving the session on the local end |
| Tx Count | Count of BFD packets sent on the local end |
| Tx Interval (ms) min/max/avg | Minimum/maximum/average interval of sending the session on the local end |
| Registered protocols | Type of protocol registered to the session |
| Uptime | Time of keeping the session UP |
| Last packet | Last BFD packet received on the local end |

BFD with OSPF**I. Requirements**

Administrator connects a L2 Switch between Switch A and Switch B and both SW1 and SWB are running OSPF. Administrator wants to associate OSPF with BFD to ensure a fast OSPF convergence when the link between SWB and switch is down.

II. Network Topology



III. Configuration Tips

1. Assign IP address and configure OSPF
2. Associate BFD with OSPF

IV. Configuration Steps

Configuring SWA:

1. Assign IP address and configure OSPF

```

SWA(config)#interface gigabitEthernet 2/1
SWA(config-GigabitEthernet 2/1)#ip address 192.168.3.1 255.255.255.0
SWA(config)#interface gigabitEthernet 1/1
SWA(config-GigabitEthernet 1/1)#ip address 192.168.1.1 255.255.255.0
SWA(config-router)#router ospf 123
SWA(config-router)#network 192.168.3.0 0.0.0.255 area 0
SWA(config-router)#network 192.168.1.0 0.0.0.255 area 0
  
```

2. Associate BFD with OSPF

```

SWA(config)#interface gigabitEthernet 2/1
SWA(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
  
```

----->set BFD time parameter and enable BFD on the interface. We suggest you to use 500/500/3 value . BFD sends a detection packet every 500ms and is timeout when BFD doesn't receive replies three times.

```
SWA(config-GigabitEthernet 2/1)#no bfd echo
```

----->by default BFD echo mode is on .when a FW or devices of other vendors connect between two BFD peers , the devices can possible filter BFD packets ,then BFD will fail to build connections . We suggest you to disable BFD echo.

```
SWA(config-router)# router ospf 123
```

```
SWA(config-router)# bfd all-interfaces
```

----->associate BFD with OSPF

Configuring SWB:

1. Assign IP address and configure OSPF

```
SWB(config)#interface gigabitEthernet 2/1
SWB(config-GigabitEthernet 2/1)#ip address 192.168.3.2 255.255.255.0
SWB(config)#interface gigabitEthernet 1/1
SWB(config-GigabitEthernet 1/1)#ip address 192.168.2.1 255.255.255.0
SWB(config-router)# router ospf 123
SWB(config-router)#network 192.168.3.0 0.0.0.255 area 0
SWB(config-router)#network 192.168.2.0 0.0.0.255 area 0
```

2. Associate BFD with OSPF

```
SWB(config)#interface gigabitEthernet 2/1
SWB(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
SWB(config-GigabitEthernet 2/1)#no bfd echo
SWB(config-router)#router ospf 123
SWB(config-router)#bfd all-interfaces
```

V. Verification

1. How to display BFD neighbor status

```
Ruijie# show bfd neighbors
```

| OurAddr | NeighAddr | LD/RD | RH/RS | Holdown(mult) | State | Int |
|-------------|-------------|-------|-------|---------------|-------|------|
| 192.168.3.1 | 192.168.3.2 | 1/2 | Up | 532 (3) | Up | G2/1 |

2. How to display detail BFD neighbor information

```
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 |

```

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5

Received MinRxInt: 50000, Received Multiplier: 3

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332

Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196

Registered protocols: OSPF

Uptime: 02:18:49

Last packet: Version: 1      - Diagnostic: 0

I Hear You bit: 1            - Demand bit: 0

Poll bit: 0                  - Final bit: 0

Multiplier: 3                - Length: 24

My Discr.: 2                  - Your Discr.: 1

Min tx interval: 50000        - Min rx interval: 50000

```

Relevant information

| Field | Description |
|---|---|
| OurAddr | IP address for the session on the local end |
| NeighAddr | IP address for the adjacent session |
| LD/RD | Session discriminator on the local and peer end |
| RH/RS | Current status of the session peer end |
| Holdown(mult) | Time of not receiving the Hello packets on the local end and the detected timeout time of the session |
| State | Current session state |
| Int | Interface number for the session |
| Session state is UP and using echo function with 50 ms interval | Whether the session is in echo mode and the interval of sending frames. This information is shown only in the echo mode |
| Local Diag | Diagnostic information of the session |
| Demand mode | Whether the demand mode is enabled or not |
| Poll bit | Whether the session configuration is modified |
| MinTxInt | Minimum sending interval of the session on the local End |
| MinRxInt | Minimum receiving interval of the session on the local end |
| Multiplier | Timeout times detected on the local end |
| Received MinRxInt | Minimum sending interval of the session on the peer end |

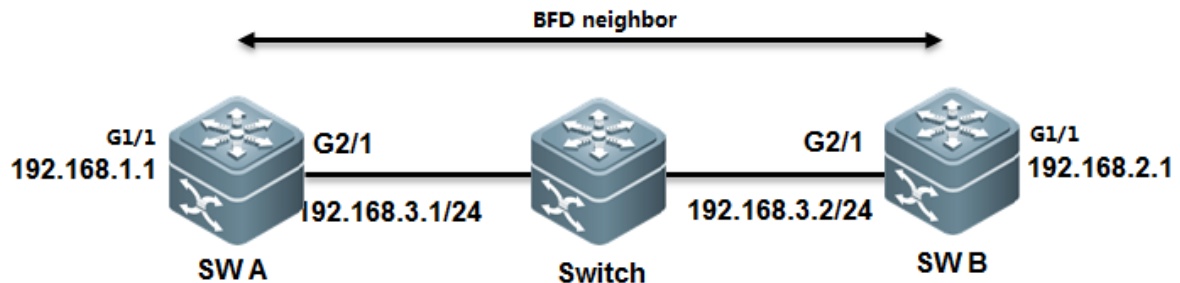
| | |
|------------------------------|--|
| Received Multiplier | Timeout times detected on the peer end |
| Holdown (hits) | Session detection time and the detected timeout times |
| Hello (hits) | Minimum interval of receiving the Hello packet after the session negotiation |
| Rx Count | Count of BFD packets received on the local end |
| Rx Interval (ms) min/max/avg | Minimum/maximum/average interval of receiving the session on the local end |
| Tx Count | Count of BFD packets sent on the local end |
| Tx Interval (ms) min/max/avg | Minimum/maximum/average interval of sending the session on the local end |
| Registered protocols | Type of protocol registered to the session |
| Uptime | Time of keeping the session UP |
| Last packet | Last BFD packet received on the local end |

BFD with PBR

I. Requirements

Administrator connects a L2 Switch between Switch A and Switch B and enable PBR on both SW1 and SWB. Administrator wants to associate PBR with BFD, BFD will fast switchover to fallback PBR when the link between SWB and switch is down.

II. Network Topology



III. Configuration Tips

1. Assign IP address
2. Associate PBF with BFD

IV. Configuration Steps

Configuring SWA

1. Assign IP address to G2/1 on SWA and configure BFD

```
SWA# configure terminal
```

```
SWA(config)# interface GigabitEthernet2/1
SWA(config-if)# no switchport
SWA(config-if)# ip address 192.168.3.1 255.255.255.0
SWA(config-if)# bfd interval 500 min_rx 500 multiplier 3 ----->set BFD time parameter and enable BFD on the
interface. We suggest you to use 500/500/3 value . BFD sends a detection packet every 500ms and is timeout
when BFD doesn't receive replies three times.
SWA(config-if)# no bfd echo ----->by default BFD echo mode is on .when a FW or devices of other vendors
connect between two BFD peers , the devices can possible filter BFD packets ,then BFD will fail to build
connections . We suggest you to disable BFD echo
```

2. Assign IP address to G1/1 on SWA

```
SWA(config-if)# exit
SWA(config)# interface GigabitEthernet1/1
SWA(config-if)# no switchport
SWA(config)# ip address 192.168.1.1 255.255.255.0
```

3. Associate PBR with BFD

```
SWA(config)# ip access-list extended 100
SWA(config-ext-nacl)# permit ip any 192.168.2.0 0.0.0.255
SWA(config-ext-nacl)# deny ip any any
SWA(config-ext-nacl)# exit
SWA(config)# route-map Example1 permit 10
SWA(config-route-map)# match ip address 100
SWA(config-route-map)# set ip precedence priority
SWA(config-route-map)#set ip next-hop verify-availability 192.168.3.2 bfd GigabitEthernet 0/1 192.168.3.2
SWA(config)# end
SWA#wr
```

Configuring SWB

1. Assign IP address to G2/1 on SWB and configure BFD

```
SWB# configure terminal
SWB(config)# interface GigabitEthernet 2/1
SWB(config-if)# no switchport
SWB(config-if)# ip address 192.168.3.2 255.255.255.0
```

```
SWB(config-if)# bfd interval 500 min_rx 500 multiplier 3 ----->set BFD time parameter and enable BFD on the interface. We suggest you to use 500/500/3 value . BFD sends a detection packet every 500ms and is timeout when BFD doesn't receive replies three times.
```

```
SWB(config-if)# no bfd echo ----->by default BFD echo mode is on .when a FW or devices of other vendors connect between two BFD peers , the devices can possible filter BFD packets ,then BFD will fail to build connections . We suggest you to disable BFD echo
```

2. Assign IP address to G1/1 on SWB

```
SWB(config-if)# exit
SWB(config)# interface GigabitEthernet1/1
SWB(config-if)# no switchport
SWB(config)# ip address 192.168.2.1 255.255.255.0
```

3. Associate PBR with BFD

```
SWB(config)# ip access-list extended 100
SWB(config-ext-nacl)# permit ip any 192.168.1.0 0.0.0.255
SWB(config-ext-nacl)# deny ip any any
SWB(config-ext-nacl)# exit
SWB(config)# route-map Example1 permit 10
SWB(config-route-map)# match ip address 100
SWB(config-route-map)# set ip precedence priority
SWB(config-route-map)#set ip next-hop verify-availability 192.168.3.1 bfd GigabitEthernet 2/1 192.168.3.1
SWB(config)# end
SWB#
```

V. Verification

1. How to display BFD neighbor status

```
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 |

```
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
```

```

Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: PBR
Uptime: 02:18:49
Last packet: Version: 1      - Diagnostic: 0
I Hear You bit: 1            - Demand bit: 0
Poll bit: 0                  - Final bit: 0
Multiplier: 3                - Length: 24
My Discr.: 2                  - Your Discr.: 1
Min tx interval: 50000        - Min rx interval: 50000
Min Echo interval: 0

```

2. How to display detail BFD neighbor information

```

Ruijie# show bfd neighbors details

```

| OurAddr | NeighAddr | LD/RD | RH/RS | Holdown(mult) | State | Int |
|-------------|-------------|-------|-------|---------------|-------|-------|
| 192.168.3.2 | 192.168.3.1 | 2/1 | Up | 532 (5) | Up | Ge2/1 |

```

Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 500000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago
Registered protocols: PBR
Uptime: 02:18:49
Last packet: Version: 1      - Diagnostic: 0
I Hear You bit: 1            - Demand bit: 0
Poll bit: 0                  - Final bit: 0
Multiplier: 5                - Length: 24
My Discr.: 1                  - Your Discr.: 2
Min tx interval: 500000        - Min rx interval: 500000
Min Echo interval: 0

```

Relevant info as below:

| Field | Description |
|---|---|
| OurAddr | IP address for the session on the local end |
| NeighAddr | IP address for the adjacent session |
| LD/RD | Session discriminator on the local and peer end |
| RH/RS | Current status of the session peer end |
| Holdown(mult) | Time of not receiving the Hello packets on the local end and the detected timeout time of the session |
| State | Current session state |
| Int | Interface number for the session |
| Session state is UP and using echo function with 50 ms interval | Whether the session is in echo mode and the interval of sending frames. This information is shown only in the echo mode |
| Local Diag | Diagnostic information of the session |
| Demand mode | Whether the demand mode is enabled or not |
| Poll bit | Whether the session configuration is modified |
| MinTxInt | Minimum sending interval of the session on the local End |
| MinRxInt | Minimum receiving interval of the session on the local end |
| Multiplier | Timeout times detected on the local end |
| Received MinRxInt | Minimum sending interval of the session on the peer end |
| Received Multiplier | Timeout times detected on the peer end |
| Holdown (hits) | Session detection time and the detected timeout times |
| Hello (hits) | Minimum interval of receiving the Hello packet after the session negotiation |
| Rx Count | Count of BFD packets received on the local end |
| Rx Interval (ms) min/max/avg | Minimum/maximum/average interval of receiving the session on the local end |
| Tx Count | Count of BFD packets sent on the local end |
| Tx Interval (ms) min/max/avg | Minimum/maximum/average interval of sending the session on the local end |
| Registered protocols | Type of protocol registered to the session |
| Uptime | Time of keeping the session UP |
| Last packet | Last BFD packet received on the local end |

3.9.7.2 DLDP

Overview

DLDP: Data Link Detection Protocol (DLDP) is a protocol designed to detect Ethernet link fault quickly.

Based on the SDH platform, the MSTP supports access, processing, and transmission of multiple services, such as TDM, ATM, and Ethernet, providing a multi-service node for the unified network management system. Because Ethernet lacks in the link keep-alive protocol, Ethernet access is always used at user access points. As a result, link protocol status is still normal even if lines for Ethernet to access the MSTP network are disconnected. In this case, route convergence slows down and the difficulty in locating a fault is increased.

The major procedure for device link detection can be divided into the following stages:

Initialization stage

When DLDP is enabled on the interface, DLDP is changed into initialization status, and then an ARP request is sent to obtain the MAC address of the peer device. If DLDP cannot obtain the peer MAC address, DLDP is in the initialization stage unless users prohibit this function and DLDP status is changed into deleted. After the peer MAC address is obtained, DLDP status is changed into link succeeded.

Link succeeded status

In this state, DLDP can send a link detection request to detect line connectivity. After DLDP responses are received, the interface is marked UP. If responses are not received, requests are sent until the number of requests exceed the maximum number. In this case, the link is marked failed and DLDP status is changed into initialization. If users delete this function during this process, DLDP status is changed into deleted.

Deleted status

In deleted state, the interface status is not analyzed by the link detection function. In this case, the interface status is consistent with the physical channel status.

The devices on both sides detected by DLDP can be set to work in active/passive mode. In the passive mode, DLDP detection packets are not sent actively and only the DLDP detection packets from the peer end are detected and replied to for link detection. When multi-channel DLDP detection is configured on a convergence router, the passive mode can greatly reduce processing load of the convergence device and traffic load of lines. In the passive mode, the peer end must be set to active mode so that the devices on both sides can normally work with each other.

The difference between DLDP and BFD:

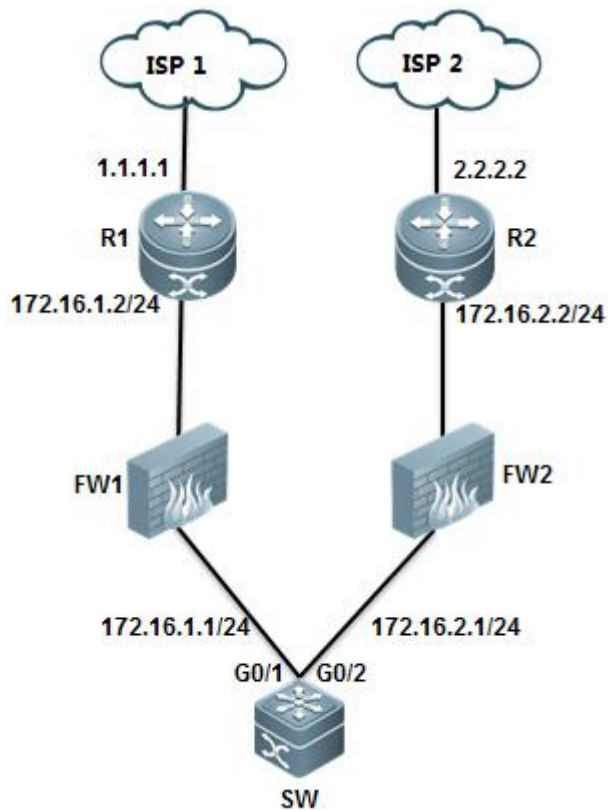
1. You must apply DLDP on ethernet port, and you can apply BFD between any two hosts regardless port type.
2. DLDP utilizes ICMP, and BFD utilizes BFD mechanism.
3. You can apply DLDP on one end because DLDP is a unidirectional detection, but you must apply BFD on both ends because BFD is a bidirectional detection.
4. DLDP bases on port, and when DLDP detection failed, DLDP shuts the port down (for example, SVI, Layer 3 port) and remove all the routes that are related to the port. BFD bases on pairs, when BFD detection failed, BFD controls only the specific route.

I. Requirements

The following figure provides two equal access to two different service providers, and there are two static routes. Route of ISP 1 is main path and route of ISP2 is a floating route, and it is the "backup" or redundant path.

The issue is when FW1 connects between R1 and SW, even if ISP 1 is down, SW cannot detect the issue and will still forward traffic to R1. Administrator can enable DLDP to solve this problem.

II. Network Topology



III. Configuration Tips

1. Configure two default routes on SW, one route points to ISP1 at 172.16.1.2, the other route is floating route and points to ISP2 at 172.16.2.2
2. Configure DLDP on SW to detects ISP 1 at 1.1.1.1 with next-hop 172.16.1.2

IV. Configuration Steps

Configuring SW

1. Assign IP address and configure basic IP routing

```

Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#no switchport
Ruijie(config-if-GigabitEthernet 0/1)#ip address 172.16.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#no switchport

```

```
Ruijie(config-if-GigabitEthernet 0/2)#ip address 172.16.2.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/2)#exit
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 ----->configure default route
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 20 -----> configure floating static route with metric 20
```

2. Configure DLDP on SW

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#dldp 1.1.1.1 next-hop 172.16.1.2 ----->detect ISP 1 at 1.1.1.1 with next-hop 172.16.1.2
```

By default ,DLDP sends a detection packet every 1000 ms and sends 4 detection packet in all , if all detection packets are failed , DLDP is timeout and can resume when receiveing 3 continuous replies

```
Ruijie(config)#show dldp interface gigabitEthernet 0/1
```

| Interface | Type | Ip | Next-hop | Interval | Retry | Resume | State |
|-----------|--------|---------|------------|----------|-------|--------|-------|
| Gi0/4 | Active | 1.1.1.1 | 172.16.1.2 | 100 | 4 | 3 | |

DLDP command format:

```
Ruijie(config-if)# dldp ip-address [ next-hop ip-address ] [ interval tick ] [ retry retry-num ] [ resume resume-num ]
```

Use this command to enable the DLDP detection function

next-hop ip-address: The nexthop IP address

Interval tick: The detection interval time. The valid range is 1 to 3600, in ticket, 1 ticket approximately equals to 10ms. By default it is **100** ticket (1 second).

retry retry-num: The retransmission times. The valid range is 1 to 3600, **4** by default. System change port state from up to down if no reply after sending 4 icmp echo

resume resume-num: The resume times of the link of the peer device detected. Before changing the link state from DOWN to UP, the continuous DLDP detection packets shall be received. The valid range is 1-200. **3** by default.

3. DLDP Optimization

Modify parameters based on the following rules:

Note:

- 1) DLDP allows to configure multiple ICMP detection on the same layer 3 port. Port changes to down when all ICMP detection fails and to recovers when one ICMP detection resumes.
- 2) DLDP uses the interface primary IP address as the communication source.
- 3) Pay attention to CPP and NFPP setting when require many ICMP detections (e.g more than 100 IP detection and 20pps for each IP) Suggest to turn off ICMP-Guard:

```
Ruijie#configure terminal
```

```
Ruijie(config)#nfpp
Ruijie(config-nfpp)#no icmp-guard enable
Ruijie(config-nfpp)#end
Ruijie#wr
and tune CPP parameters :
Ruijie(config)#cpu-protect type icmp bandwidth 4096
```

V. Verification

1. Display IP route table when DLDLP doesn't time out

```
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 172.16.1.2 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 172.16.1.2
C    172.16.1.0/24 is directly connected, GigabitEthernet 0/1
C    172.16.1.1/32 is local host.
C    172.16.2.0/24 is directly connected, GigabitEthernet 0/2
C    172.16.2.1/32 is local host.
```

2. Display DLDLP status

```
Ruijie#show dldp int g0/1
Interface  Type      Ip      Next-hop  Interval  Retry  Resume
-----
Gi0/1     Active   1.1.1.1  172.16.1.2  100      4      3
```

3. Show debug to describe how DLDLP works

```
Ruijie#debug ip icmp ----->enable debug ip icmp then shutdown loopback 0

*Mar 29 14:21:26: %7: ICMP: echo reply rcvd, src 1.1.1.1, dst 172.16.1.1
*Mar 29 14:21:27: %7: ICMP: echo reply rcvd, src 1.1.1.1, dst 172.16.1.1
*Mar 29 14:21:28: %7: ICMP: echo reply rcvd, src 1.1.1.1, dst 172.16.1.1
*Mar 29 14:21:29: %7: ICMP:sending redirect host to 172.16.1.1,gw 172.16.1.2
*Mar 29 14:21:29: %7: ICMP:sending ttl(time to live) exceeded to 172.16.1.1
*Mar 29 14:21:29: %7: ICMP:redirect rcvd from 172.16.1.1 --for dst 1.1.1.1 use gw 172.16.1.2
```

```

*Mar 29 14:21:29: %7: ICMP: time exceeded rcvd from 172.16.1.1----->1st timeout
*Mar 29 14:21:30: %7: ICMP:sending redirect host to 172.16.1.1,gw 172.16.1.2
*Mar 29 14:21:30: %7: ICMP:sending ttl(time to live) exceeded to 172.16.1.1
*Mar 29 14:21:30: %7: ICMP:redirect rcvd from 172.16.1.1 --for dst 1.1.1.1 use gw 172.16.1.2
*Mar 29 14:21:30: %7: ICMP: time exceeded rcvd from 172.16.1.1----->2nd timeout
*Mar 29 14:21:31: %7: ICMP:sending redirect host to 172.16.1.1,gw 172.16.1.2
*Mar 29 14:21:31: %7: ICMP:sending ttl(time to live) exceeded to 172.16.1.1
*Mar 29 14:21:31: %7: ICMP:redirect rcvd from 172.16.1.1 --for dst 1.1.1.1 use gw 172.16.1.2
*Mar 29 14:21:31: %7: ICMP: time exceeded rcvd from 172.16.1.1----->3rd timeout
*Mar 29 14:21:32: %7: ICMP:sending redirect host to 172.16.1.1,gw 172.16.1.2
*Mar 29 14:21:32: %7: ICMP:sending ttl(time to live) exceeded to 172.16.1.1
*Mar 29 14:21:32: %7: ICMP:redirect rcvd from 172.16.1.1 --for dst 1.1.1.1 use gw 172.16.1.2
*Mar 29 14:21:32: %7: ICMP: time exceeded rcvd from 172.16.1.1----->shutdown port after 4th timeout
*Mar 29 14:21:33: %DLDP-5-STATECHANGE: Interface GigabitEthernet 0/1 - Dldp 1.1.1.1 state changed to down.
*Mar 29 14:21:33: %7: ICMP:sending redirect host to 172.16.1.1,gw 172.16.1.2
*Mar 29 14:21:33: %7: ICMP:sending ttl(time to live) exceeded to 172.16.1.1
*Mar 29 14:21:33: %7: ICMP:redirect rcvd from 172.16.1.1 --for dst 1.1.1.1 use gw 172.16.1.2
*Mar 29 14:21:33: %7: ICMP: time exceeded rcvd from 172.16.1.1
*Mar 29 14:21:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to
down.

```

4. When DLDLP detection fails , DLDLP shutdowns the port , then floating static route is installed in IP route table.

```

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

Gateway of last resort is 172.16.2.2 to network 0.0.0.0
S* 0.0.0.0/0 [20/0] via 172.16.2.2 —> flexible route takes effect
C   172.16.2.0/24 is directly connected, GigabitEthernet 0/2
C   172.16.2.1/32 is local host.

```

3.9.7.3 RLDP

Overview

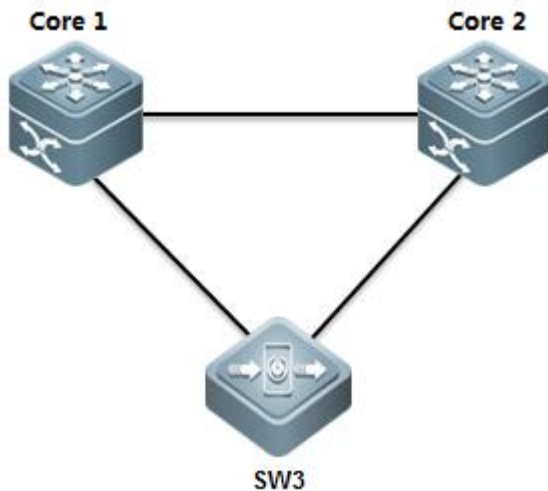
RLDP: Rapid Link Detection Protocol is one of Ruijie's proprietary link protocol designed to detect Ethernet link fault quickly. General Ethernet link detection mechanism only makes use of the status of the physical connections and detects the connectivity of the link via the auto-negotiation of the physical layer. This detection mechanism has restrictions and sometimes cannot provide reliable link detection information for the user. For example, if the optical fiber receiving line pair on the optical interface is misconnected, due to the existence of the optical converter, the related port of the device is "linkup" physically but actually the corresponding layer-2 link cannot work for communications.

The RLDP enables easy detection of Ethernet device link fault, including the one-way link fault, two-way link fault and loop link fault.

BPDUGuard: BPDUGuard put ports in err-disable status if ports receive BPDU packets

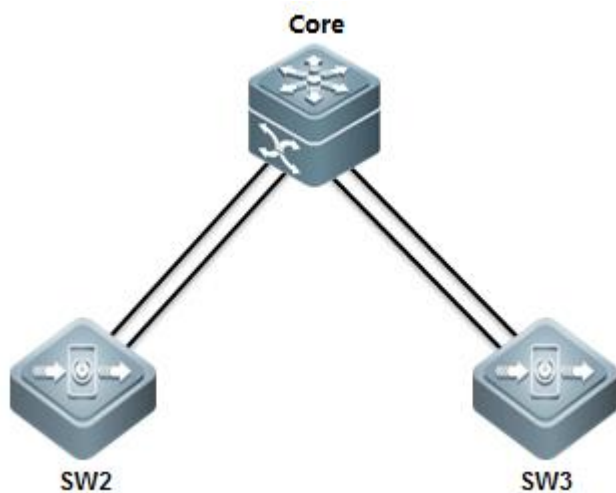
Common layer 2 loops occurs in following scenarios

1. Both core switches connect to a same access switch



In this scenario, you can enable MSTP to prevent loop and ensure network redundancy.

2. Both access switches connect double links to core switch



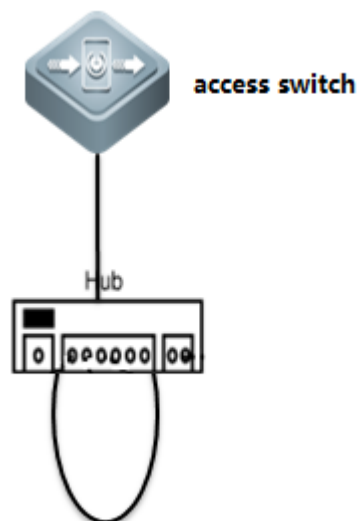
In this scenario, you can enable **Aggregate port (AP)** to prevent loop and ensure network redundancy

3. One cable connects to two ports on a same switch



In this scenario, you can enable **RLDP or BPDU Guard** to prevent loop

4. Access switch connects to a hub and a loop occurs in the hub



In this scenario , we suggest you to enable **RLDP rather than BPDU Guard** to prevent loop because BPDU Guard is a standard protocol and utilizes multicast packets at MAC 01-80-C2-00-00-00 to communicate. Some hubs can probably filter packets sent to this MAC ,so even when a loop occurs , BPDU Guard doesn't put the port in err-disable status. Compare with BPDU Guard , RLDP is Ruijie private protocol that utilizes mutlicast packets at MAC 01-d0-f8-00-00-02 to communicate which doesn't be filtered.

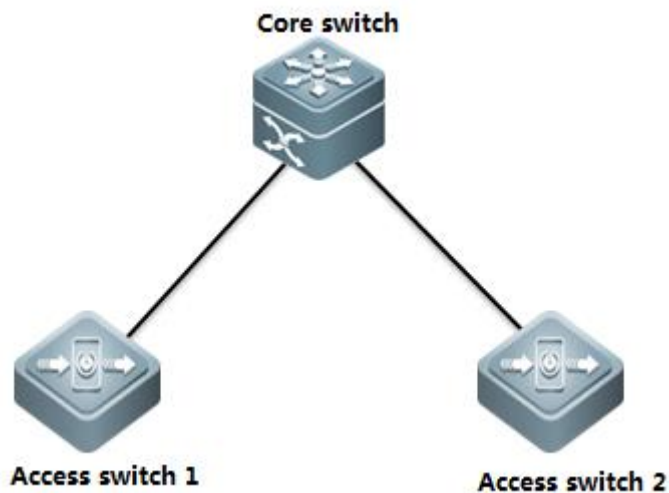
I. Requirements

Administrator wants to enable RLDP on edge ports on access switch to prevent loop

II. Configuration Tips

1. Enable RLDP globally
2. Configure RLDP on interfaces
3. Configure error recovery interval

III. Network Topology



IV. Configuration Steps

Configuring access switch :

```
Ruijie#configure terminal
```

```
Ruijie(config)#rldp enable ----->enable RLDP globally
```

```
Ruijie(config)#interface range g0/1-24 -----> configure a range interfaces
```

```
Ruijie(config-if-range)#rldp port loop-detect shutdown-port ----->If RLDP detects a loop , RLDP shutdown this port
```

```
Ruijie(config-if-range)#exit
```

```
Ruijie(config)#errdisable recovery interval 300 -----> those ports recover after 300s
```

```
Ruijie(config)#end
```

```
Ruijie#wr
```

Note:

- 1) We suggest you to enable BPDU Guard and Portfast at the same time (you must enable STP first)

```
Ruijie#configure terminal
```

```
Ruijie(config)#spanning-tree
```

```
Ruijie(config)#interface range g0/1-24
```

```
Ruijie(config-if-range)#spanning-tree bpduguard enable
```

```
Ruijie(config-if-range)#spanning-tree portfast
```

```
Ruijie(config)#interface gigabitEthernet 0/25
```

```
Ruijie(config-if-GigabitEthernet 0/25)#spanning-tree bpdufilter enable
```

```
Ruijie(config-if-GigabitEthernet 0/25)#exit
```

```
Rujijie(config)#errdisable recovery interval 300
Rujijie(config)#end
Rujijie#wr
```

V. Verification

1. How to display RLDP status

```
Rujijie#show rldp
rldp state      : enable
rldp hello interval: 3
rldp max hello   : 2
rldp local bridge : 001a.a9c4.062e
-----
GigabitEthernet 0/24
port state      : normal
neighbor bridge : 0000.0000.0000
neighbor port   :
loop detect information :
    action: shutdown-port
    state : normal
```

3. System returns following messages when a loop occurs between ports G0/5 and G0/7

```
Rujijie#
*Mar 19 20:16:00: %RLDP-3-LINK_DETECT_ERROR: loop detection error detect on interface GigabitEthernet 0/7.set
this interface errordisable!
*Mar 19 20:16:00: %RLDP-3-LINK_DETECT_ERROR: loop detection error detect on interface GigabitEthernet 0/5.set
this interface errordisable!
Mar 19 20:16:01: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 1, changed state to down.
*Mar 19 20:16:02: %LINK-3-UPDOWN: Interface GigabitEthernet 0/5, changed state to down.
*Mar 19 20:16:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/5, changed state to down.
*Mar 19 20:16:02: %LINK-3-UPDOWN: Interface GigabitEthernet 0/7, changed state to down.
*Mar 19 20:16:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/7, changed state to down.
```

3. RLDP shutdown both ports G0/5 and G0/7

```
Rujijie#show interfaces status
```

| Interface | Status | Vlan | Duplex | Speed | Type |
|---------------------|----------|------|---------|---------|--------|
| GigabitEthernet 0/1 | down | 1 | Unknown | Unknown | copper |
| GigabitEthernet 0/2 | down | 1 | Unknown | Unknown | copper |
| GigabitEthernet 0/3 | down | 1 | Unknown | Unknown | copper |
| GigabitEthernet 0/4 | down | 1 | Unknown | Unknown | copper |
| GigabitEthernet 0/5 | disabled | 1 | Unknown | Unknown | copper |
| GigabitEthernet 0/6 | down | 1 | Unknown | Unknown | copper |
| GigabitEthernet 0/7 | disabled | 1 | Unknown | Unknown | copper |

4. Both ports recover after 300s:

```
*Mar 19 20:21:01: %PORT_SECURITY-4-ERR_RECOVER: Interface GigabitEthernet 0/5 recover from an error.
*Mar 19 20:21:01: %PORT_SECURITY-4-ERR_RECOVER: Interface GigabitEthernet 0/7 recover from an error.
*Mar 19 20:21:01: %RLDP-3-LINK_DETECT_RECOVER: rldp recover interface GigabitEthernet 0/7 from loop error
*Mar 19 20:21:01: %RLDP-3-LINK_DETECT_RECOVER: rldp recover interface GigabitEthernet 0/5 from loop error
*Mar 19 20:21:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 1, changed state to up.
*Mar 19 20:21:06: %LINK-3-UPDOWN: Interface GigabitEthernet 0/5, changed state to up.
*Mar 19 20:21:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/5, changed state to up.
*Mar 19 20:21:06: %LINK-3-UPDOWN: Interface GigabitEthernet 0/7, changed state to up.
*Mar 19 20:21:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/7, changed state to up.
```

5. Execute "rldp reset" EXEC command to rest all ports in disabled status immediately

```
Rujijie#rldp reset
Rujijie#
*Mar 19 20:34:32: %PORT_SECURITY-4-ERR_RECOVER: Interface GigabitEthernet 0/7 recover from an error.
*Mar 19 20:34:32: %RLDP-3-LINK_DETECT_RECOVER: rldp recover interface GigabitEthernet 0/7 from loop error
*Mar 19 20:34:32: %PORT_SECURITY-4-ERR_RECOVER: Interface GigabitEthernet 0/5 recover from an error.
*Mar 19 20:34:32: %RLDP-3-LINK_DETECT_RECOVER: rldp recover interface GigabitEthernet 0/5 from loop error
```

3.9.8 Multicast

3.9.8.1 IGMP Snooping

Overview

IGMP Snooping: Internet Group Management Protocol, abbreviated as IGMP Snooping, is an IP multicast flow mechanism running in the VLAN, and used to manage and control the IP multicast flow forwarding in the VLAN and belongs to the Layer2 multicast function. The IGMP Snooping function described below is in the VLAN, and the related ports are the member ports in the VLAN.

The device running IGMP Snooping sets up the mapping for the port and the multicast address by analyzing the received IGMP packets, and forwards the IP multicast packets based on the mapping. With IGMP Snooping enabled, the IP multicast packets are broadcasted in the VLAN; while with IGMP Snooping enabled, the known IP multicast packets are not broadcasted in the VLAN but sent to the specified recipient.

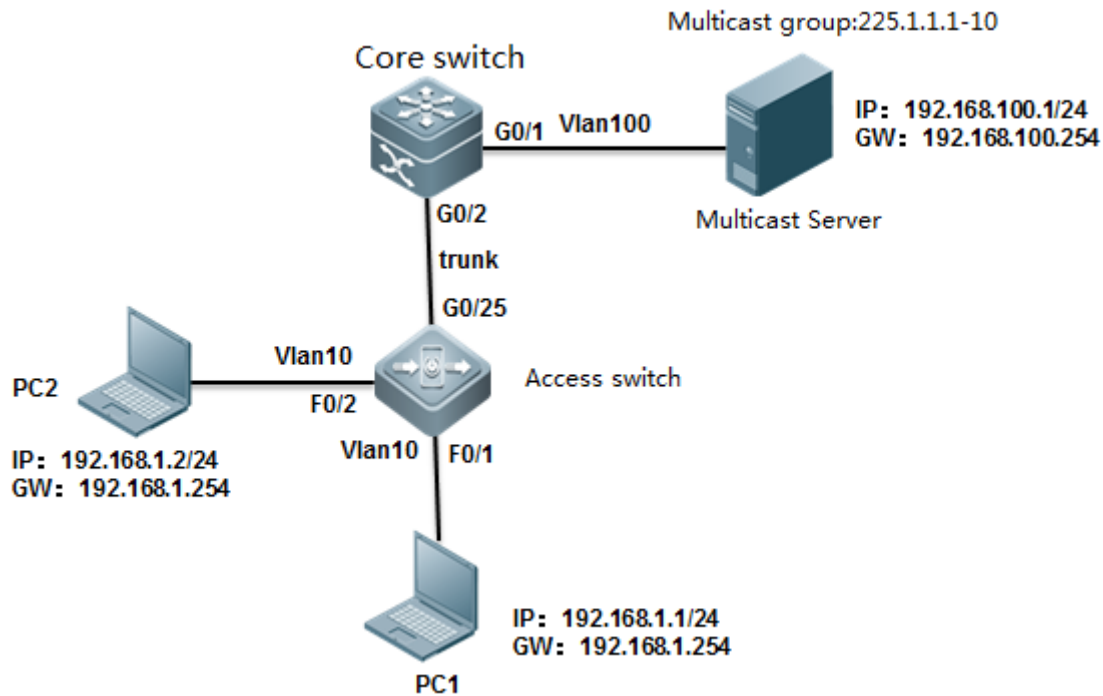
I. Requirements

- 1) As the figure shown, core switch connects to multicast source and runs multicast routing. Access switch connects to users (for example, PC1 and PC2) in Vlan 10
- 2) Enable multicast routing protocol in PIM-DM mode on Core switch. Enable IGMP Snooping in IVGL mode on access switch.
- 3) Users can only join legal multicast group from 225.1.1.1 to 225.1.1.10.
- 4) Enable fast leave on all ports connected to users on access switch.
- 5) On access switch, suppress response packets from IGMP member to core switch to decrease the burden of core switch.

II. Configuration Tips

- 1) Enable multicast routing protocol in PIM-DM mode on every corresponding Layer 3 port on Core switch . Enable IGMP Snooping in IVGL mode on access switch and specify the uplink interface as IGMP Snooping route port.
- 2) Configure IGMP Filter on access switch to prevent user from joining the illegal multicast group
- 3) Enable fast-leave on access switch
- 4) Enable IGMP Snooping suppression on access switch

III. Network Topology



IV. Configuration Steps

Configuring core switch:

- 1) Create vlans and enable multicast routing

```
Ruijie#configure terminal
Ruijie(config)#vlan 10
Ruijie(config-vlan)#vlan 100
Ruijie(config-vlan)#exit
Ruijie(config)#ip multicast-routing
```

- 2) Assign G0/1 connected to multicast source to vlan 100 and enable multicast protocol in PIM-DM mode on SVI 100

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport access vlan 100
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#interface vlan 100
Ruijie(config-if-VLAN 100)#ip address 192.168.100.254 255.255.255.0
Ruijie(config-if-VLAN 100)#ip pim dense-mode
```

- 3) Assign IP address to VLAN 10 and enable multicast protocol in PIM-DM mode on SVI 10

```
Ruijie(config)#interface vlan 10
Ruijie(config-if-VLAN 10)#ip address 192.168.10.254 255.255.255.0
Ruijie(config-if-VLAN 10)#ip pim dense-mode
Ruijie(config-if-VLAN 10)#exit
```

- 3) Configure G0/2 connected to access switch as trunk port

```
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/2)#exit
```

- 4) Save configuration

```
Ruijie(config)#end
Ruijie#wr
```

Configuring access switch:

- 1) Create vlan , assign ports conncted to users to vlan 10 and configure G0/25 connected to core switch as trunk port

```
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exit
Ruijie(config)#interface gigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/25)#exit
Ruijie(config)#interface range fastEthernet 0/1-2
Ruijie(config-if-range)#switchport access vlan 10
Ruijie(config-if-range)#exit
```

- 2) Enable IGMP Snooping in IVGL mode and specify G0/25 as IGMP Snooping route port for vlan 10.

```
Ruijie(config)#ip igmp snooping ivgl
Ruijie(config)#ip igmp snooping vlan 10 mrouter interface g0/25
Ruijie(config)#end
```

- 3) Enable IGMP Filter to allow user join legal multicast group from 225.1.1.1 to 226.1.1.1 only

```
Ruijie(config)#ip igmp profile 1
Ruijie<config-profile>#permit
Ruijie<config-profile>#range 225.1.1.1 226.1.1.10
Ruijie<config-profile>#exit
Ruijie(config)#interface range fastEthernet 0/1-2
Ruijie(config-if-range)#ip igmp snooping filter 1
Ruijie(config-if-range)#exit
```

4) Enable fast-leave

```
Ruijie(config)#ip igmp snooping fast-leave enable
```

5) Enable IGMP Snooping suppression

```
Ruijie(config)#ip igmp snooping suppression enable
Ruijie(config)#end
Ruijie#wr
```

V. Verification

1) How to display IGMP Snooping table on access switch

```
Ruijie# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 229.255.255.250, 10):      ----->illegal igmp snooping entry ,you can enter "ip igmp snooping filter 1" interface
configuration command to filter it
  VLAN(10) 2 OPORTS:
    GigabitEthernet 0/25(M)
    FastEthernet 0/2(D)
(*, 239.255.255.250, 10):      ----->illegal igmp snooping entry ,you can enter "ip igmp snooping filter 1"
interface configuration command to filter it

  VLAN(10) 2 OPORTS:
    GigabitEthernet 0/25(M)
    FastEthernet 0/2(D)
(*, 225.1.1.1, 10):            ----->legal igmp snooping entry
  VLAN(10) 2 OPORTS:
    GigabitEthernet 0/25(M)      ----->M indicates the route port
    FastEthernet 0/2(D)         ----->D indicates the user port
```

2) How to display IGMP Snooping statistics

```
Ruijie#show ip igmp snooping statistics
Current number of Gda-table entries: 1          ----->number of igmp snooping entries
Configured Statistics database limit: 1024      ----->max number of entries
Current number of IGMP Query packet received : 0
Current number of IGMPv1/v2 Report packet received: 0
Current number of IGMPv3 Report packet received: 0
Current number of Leave packet received: 0
Current number of PIM packet received: 0
```

Current number of DVMRP packet received: 0

| GROUP | Interface | Last report time | Last leave time | Last reporter | Report pkts |
|------------|------------|------------------|-----------------|---------------|-------------|
| Leave pkts | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| 225.1.1.1 | VL10:Fa0/2 | ---- | ---- | | ---- |
| 0 | 0 | | | | |

3) How to display igmp snooping route port

```
Ruijie#show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 10):
  VLAN(10)  1 MROUTES:
    GigabitEthernet 0/25(S)
```

3.9.8.2 Multicast optimization

Optimization on access switch:

Enable IGMP Filter on access switch to filter illegal multicast group

Optimization on core switch:

- 1) Enable IGMP Snooping in IVGL mode on core switch which is user gateway
- 2) Apply ACL on the trunk port connected to access switch in input direction to prevent illegal multicast source
- 3) Apply IGMP filter on SVI port which is user gateway
- 4) Prune trunk port
- 5) Filter illegal register packets on RP
- 6) Filter illegal BSR (Dynamic RP)
- 7) Filter C-RP on BSR

1. Optimization on access switch:

- 1) This example enables IGMP Filter on ports connected to users to allow users join legal multicast group from 225.1.1.1 to 225.1.1.10 (**highly recommend**)

```
S86E(config)#ip igmp profile 1
S86E(config-profile)#permit
S86E(config-profile)#range 225.1.1.1 225.1.1.10 ----->specify legal mulitcast IP range
S86E(config-profile)#exit
S86E(config)#interface range fastEthernet 0/1-2
S86E(config-if-range)#ip igmp snooping filter 1 ----->apply filter on the interface
S86E(config-if-range)#exit
```

This example displays the IGMP Snooping table before applying IGMP Snooping filter ,and illegal entries exists

```
Ruijie# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 229.255.255.250, 10):      ----->illegal ip igmp snooping entry
  VLAN(10) 2 OPORTS:
    GigabitEthernet 0/25(M)
    FastEthernet 0/2(D)
(*, 239.255.255.250, 10):      ----->illegal ip igmp snooping entry
  VLAN(10) 2 OPORTS:
    GigabitEthernet 0/25(M)
    FastEthernet 0/2(D)
(*, 225.1.1.1, 10):            ----->legal ip igmp snooping entry
  VLAN(10) 2 OPORTS:
    GigabitEthernet 0/25(M)
    FastEthernet 0/2(D)
```

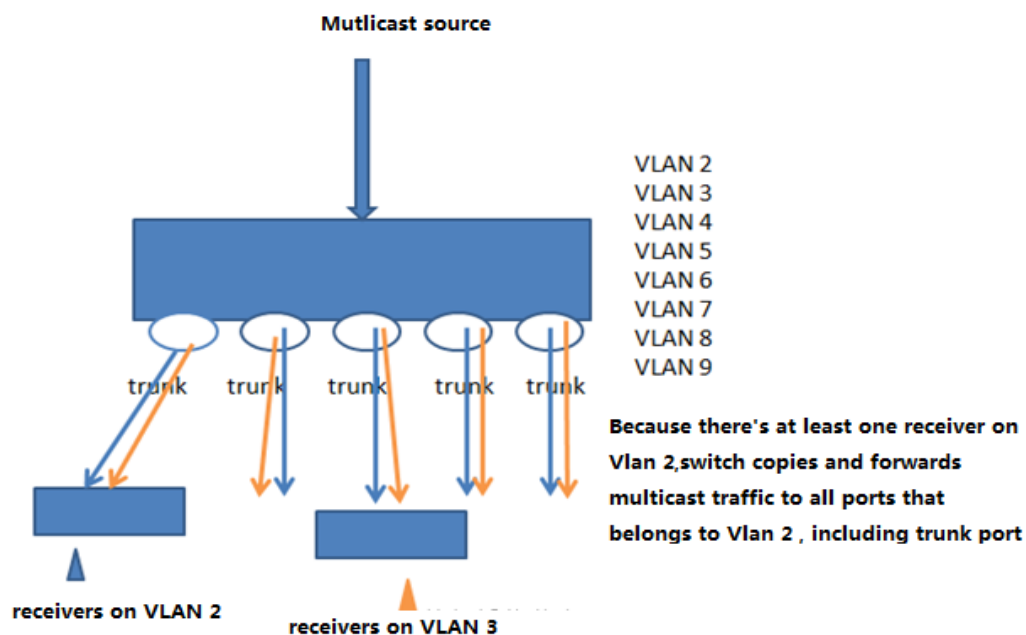
When you finish applying IGMP Snooping filter , enter "clear ip igmp snooping gda-table" EXEC command to clear IGMP Snooping table , then display IGMP Snooping table again.

```
Ruijie#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 225.1.1.1, 10):            ----->only legal ip igmp snooping entry exists
  VLAN(10) 2 OPORTS:
    GigabitEthernet 0/25(M)
    FastEthernet 0/2(D)
```

2. Optimization on core switch

- 1) Enable IGMP Snooping in IVGL mode on core switch which is user gateway (Regardless of multicast routing protocol in PIM-DM or PIM-SM , highly recommend)

Why we should enable IGMP Snooping on a Layer 3 switch that have multicast routing protocol enabled and the switch is also the user gateway.



As above figure shown, switch copies and forward multicast traffic to a port even if there's no receiver on that port.

This example shows how to configure IGMP Snooping in IVGL mode to optimize switch performance.

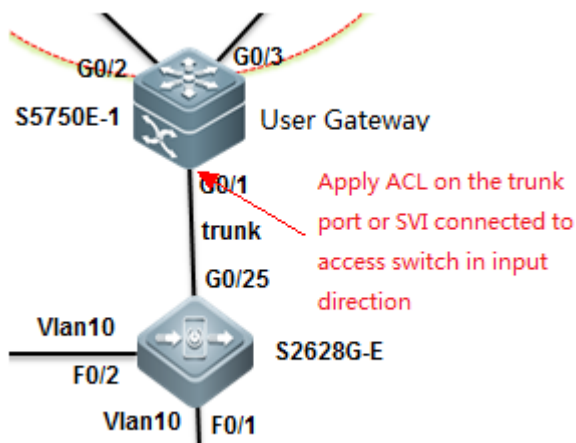
S5750E-1(config)#ip igmp snooping ivgl

2) Apply ACL on the trunk port connected to access switch in input direction to prevent illegal multicast source **(If you've enable IGMP Snooping filter on access switch, this step is a option.)**

This example shows a illegal multicast groups can take up plenty room in IGMP table

```
Ruijie#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface      Uptime    Expires    Last Reporter
225.1.1.1           VLAN 100      00:00:30  00:03:50  192.168.100.1
225.1.1.1           VLAN 10       00:06:36  00:02:20  0.0.0.0
229.255.255.250    VLAN 10       00:08:46  00:02:24  0.0.0.0
239.255.255.250    VLAN 10       00:08:45  00:02:21  0.0.0.0
```

As figure shown, this example configures ACL on the trunk port or SVI in input direction to filter illegal multicast groups



```

S86E(config)#ip access-list extended deny_mc_source
S86E(config-ext-nacl)#10 permit igmp any 225.1.1.0 0.0.0.255 ----->permit legal igmp control packets
S86E(config-ext-nacl)#20 deny igmp any any ----->deny any other illegal control packets
S86E(config-ext-nacl)#30 permit ip any 225.1.1.0 0.0.0.255 ----->legal multicast data packets
S86E(config-ext-nacl)#40 permit ip any 224.0.0.0 0.0.0.255 ----->IGMP packets , need to guarantee
S86E(config-ext-nacl)#50 deny ip any 224.0.0.0 15.255.255.255 ----->deny any other multicast data packets
S86E(config-ext-nacl)#60 permit ip any any

```

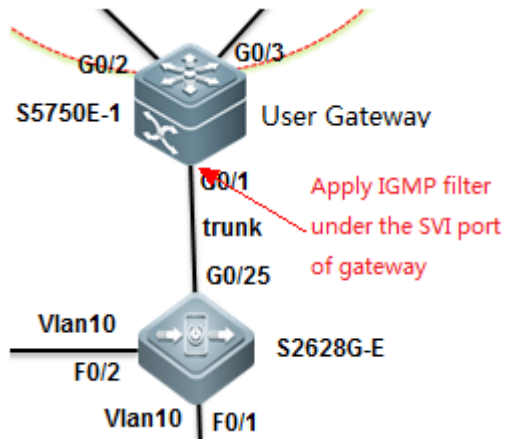
3) Apply ACL on the SVI connected to access switch in input direction to prevent illegal multicast source (If you've enable IGMP Snooping filter on access switch, this step is an option. You can choose method 2 or method 3, and we suggest you to use method 3)

This example shows that illegal multicast groups can take up plenty of room in the IGMP table

```

Ruijie#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface      Uptime    Expires    Last Reporter
225.1.1.1          VLAN 100      00:00:30  00:03:50  192.168.100.1
225.1.1.1          VLAN 10       00:06:36  00:02:20  0.0.0.0
229.255.255.250    VLAN 10       00:08:46  00:02:24  0.0.0.0
239.255.255.250    VLAN 10       00:08:45  00:02:21  0.0.0.0

```



```
S86E(config)#ip access-list standard 10
S86E(config-std-nacl)#10 permit 225.1.1.0 0.0.0.255 ----->legal IGMP multicast source
S86E(config-std-nacl)#20 deny any
S86E(config-std-nacl)#exit
```

Apply ACL on SVI

```
S86E(config)#interface VLAN 10
S86E(config-VLAN 10)#ip igmp access-group 10
S86E(config-VLAN 10)#exit
```

4) Prune trunk port (highly recommend)

```
S86E(config)#interface VLAN 10
S86E(config)#interface gigabitEthernet 0/1
S86E(config-if-GigabitEthernet 0/1)#switchport trunk allowed vlan remove 1-9,11-4094
S86E(config-if-GigabitEthernet 0/1)#exit
```

5) Filter illegal register packets on RP (for PIM-SM , not for PIM-DM)

```
Ruijie(config)# ip access-list extended acl_3500
Ruijie(config-ext-nacl)# permit ip 219.229.134.0 0.0.0.255 239.202.0.0 0.0.255.255
Ruijie(config-ext-nacl)# exit
Ruijie(config)#ip pim accept-register list acl_3500
```

6) Filter illegal BSR(Dynamic RP) (for PIM-SM , not for PIM-DM)

```
Ruijie(config)#ip access-list standard bsr_accept
Ruijie(config-std-nacl)# 10 permit host 10.10.10.1
Ruijie(config-std-nacl)# 20 permit host 10.10.10.2
Ruijie(config-std-nacl)#exit
Ruijie ( config ) #ip pim accept-bsr list bsr_accept
```

7) Filter C-RP on BSR (for PIM-SM , not for PIM-DM)

```
ip pim accept-crp list crp_list
```

3.9.8.3 PIM-DM

Scenario

The Protocol Independent Multicast-Dense Mode (PIM-DM) is the PIM in dense mode, suitable for a small-scale network with dense multicast group members. Its working principle is as follows:

1. The PIM-DM assumes that each subnet of the network has at least one multicast group member and thereby the multicast data are dispersed to all nodes on the network. The PIM-DM prunes branches to which multicast data are to be forwarded and retains only branches of multicast data receivers. The dispersing-pruning process occurs periodically. The pruned branches can be periodically restored to the forwarding status.
2. When a multicast group member appears on the node of the pruned branch, the node sends a graft packet to its downstream device to turn its pruned state into a forwarding state. In this way, the node recovers its multicast data forwarding capability.

Configuration Example

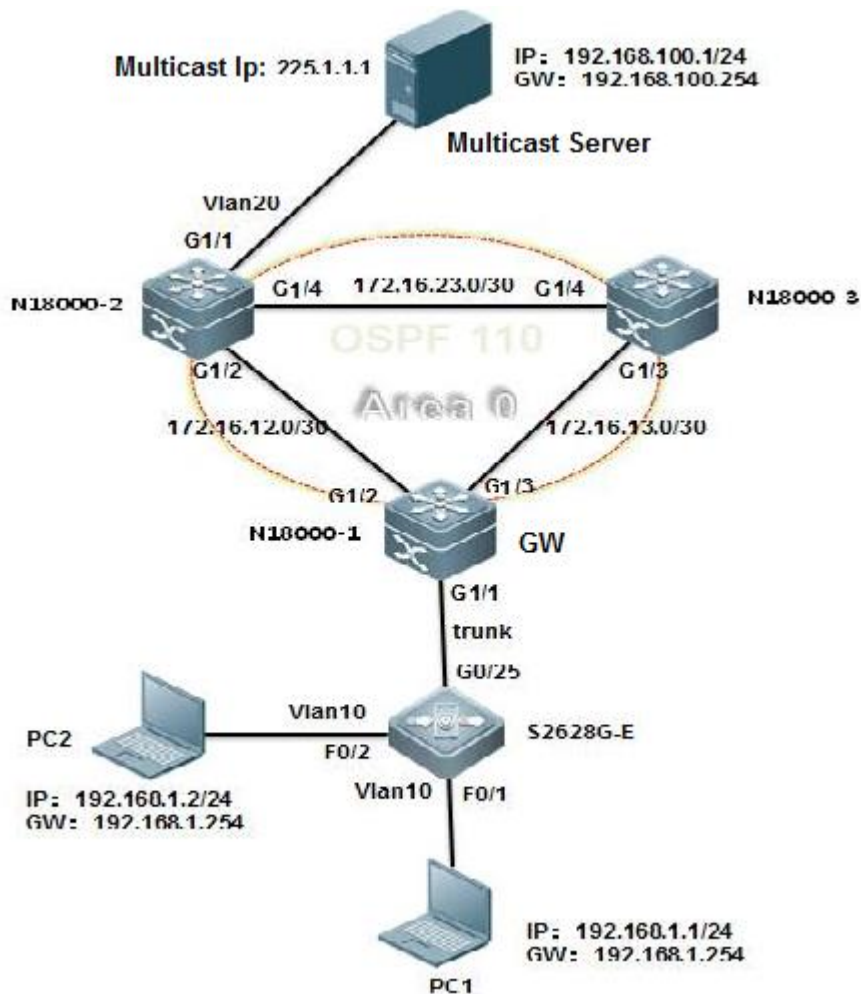
I. Networking Requirements

1. The N18000-1, N18000-2, and N18000-3 are three core devices on the network. They are interconnected to each other through L3 ports and run the OSPF on the process 110. They belong to area 0.
2. The gateway of user PCs is on the N18000-1 and the multicast server is connected to the N18000-2 directly. They are redistributed to the OSPF process.
3. On the N18000-1, N18000-2, and N18000-3, the L3 multicast routing protocol PIM-DM is enabled.
4. On the SS2628G-E switch, the L2 multicast routing protocol IVGL is enabled.
5. The PCs connected to the S26E can access the video on the multicast server on demand.
6. Network optimization is carried out on the multicast network to reduce traffic congestion and multicast spoofing.

II. Configuration Tips

1. On the three core switch, configure the IP addresses and enable the OSPF routing protocol. Ensure that the server and the switch can ping through to each other.
2. On the three switches, enable the multicast routing function PIM-DM.
3. On the access server, set the IGMP Snooping mode to IVGL.

II. Network Topology



IV. Configuration Steps

Step 1. Configure the basic IP addresses, routing, and the multicast function.

On the core servers, perform the following steps:

1. On the N18000-1,

Create VLAN 10, set the SVI address of the user gateway, configure the Trunk port that connects the access switch, and configure the IP addresses for the L3 interconnection with other core servers.

2. On the N18000-2,

Create VLAN 10, set the SVI address of the multicast server gateway, configure the interface that connects the multicast server to Access VLAN 20, and configure the IP addresses for the L3 interconnection with other core servers.

Note:

3. On the N18000-3,

Configure the IP addresses for the L3 interconnection with other core servers.

On the access switch, perform the following steps:

- 1) Create the VLAN and partition the VLAN. Set the port that connects users to an Access port and the uplink port to a Trunk port.
- 2) Set the IGMP Snooping mode to IVGL and set the g0/25 port as the route connection port of VLAN 10.

V. Verification

1. On the switch, check the IGMP groups.
2. Check the PIM-DM information of the port.
3. Check the next hop information of the PIM-DM.

3.9.8.4 PIM-SM

Scenario

Protocol Independent Multicast - Sparse Mode (PIM-SM) transmits multicast data in pull mode, suitable for a large- and medium-scale network with scattered multicast group members. Its working principle is as follows:

1. The PIM-SM assumes all hosts do not require multicast data. Multicast data are sent only if they are explicitly requested. The PIM-SM develops and maintains a rendezvous point tree (RPT) as its core task. The RPT chooses a router in the PIM domain as the public rendezvous point (RP). The multicast data are transmitted to receivers through RPs along the RPT.
2. The router that connects receivers sends join packets to the RP of the multicast group. The packet is delivered to the RP hop by hop and its path forms a branch of the RPT.
3. When the multicast source sends multicast data to a multicast group, the designated router (DR) on the multicast source side registers to the RP and sends the register packet to the RP in unicast mode. The arrival of the packet on the RP triggers the establishment of the shortest path tree (SPT). Then the multicast source forwards the multicast data to the RP on the SPT. After reaching the RP, the multicast data are replicated and forwarded to the receivers along the RPT.

Configuration Example

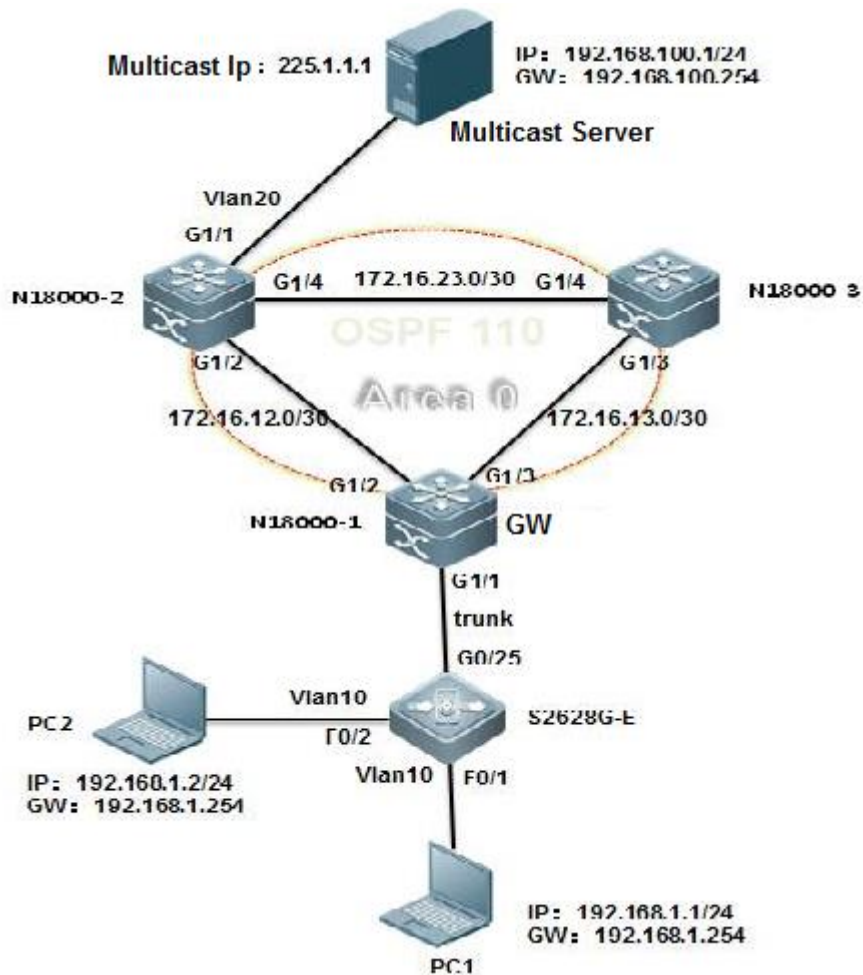
I. Networking Requirements

1. The N18000-1, N18000-2, and N18000-3 are three core devices on the network. They are interconnected to each other through L3 ports and run the OSPF and the process 110. They belong to area 0.
2. The gateway of user PCs is on the N18000-1 and the multicast server is connected to the N18000-2 directly. They are redistributed to the OSPF process.
3. On the N18000-1, N18000-2, and N18000-3, the L3 multicast routing protocol PIM-SM is enabled. The static RP is used. The N18000-2 is configured as an RP.
4. On the SS2628G-E switch, the L2 multicast routing protocol IVGL is enabled.
5. The PCs connected to the S26E can play the video on the multicast server on demand.
6. Network optimization is carried out on the multicast network to reduce traffic congestion and multicast spoofing.

II. Configuration Tips

1. On the three core switch, configure the IP addresses and enable the OSPF routing protocol. Ensure that the server and the switch can ping through to each other.
2. On the three switches, enable the multicast routing function PIM-SM.
3. On the access server, configure the IGMP Snooping function to IVGL mode.

II. Network Topology



IV. Configuration Steps

Step 1. Configure the basic IP addresses, routing, and the multicast function.

On the core servers, perform the following steps:

1. On the N18000-1,

Create VLAN 10, set the SVI address of the user gateway, configure the Trunk port that connects the access switch, and configure the IP addresses for the L3 interconnection with other core servers.

2. On the N18000-2,

Create VLAN 10, set the SVI address of the multicast server gateway, configure the interface that connects the multicast server to Access VLAN 20, and configure the IP addresses for the L3 interconnection with other core servers.

3. On the N18000-3,

- 1) Configure the IP addresses for the L3 interconnection with other core servers.
- 2) Configure the OSPF routing on the N18000-3.

On the access switch, perform the following steps:

- 1) Create the VLAN and partition the VLAN. Set the port that connects users to an Access port and the uplink port to a Trunk port.
- 2) Set the IGMP Snooping mode to IVGL and set the g0/25 port as the route connection port of VLAN 10.

V. Verification

1. On the switch, check the IGMP groups.
2. Check all the RPs and the groups they serve on the switch.
3. Check the BSR information.
4. Check the PIM-SM interface information.
5. Check the PIM-SM routing information.

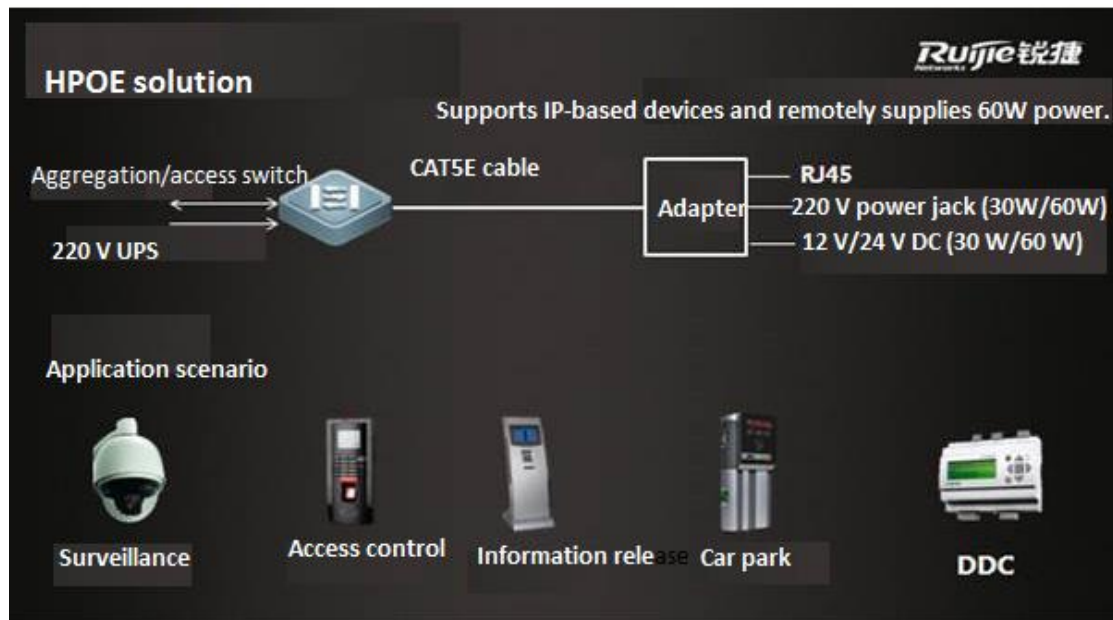
3.9.9 HPOE Function

Product Introduction

POE is short for Power on Ethernet. Currently, the universal standards include IEEE 802.3af (POE) and IEEE 802.3at (POE+). The former provides 15.4W port power output and the latter provides 30W port power output. POE involves Power Sourcing Equipment (PSE) and Powered Device (PD). Generally, a PSE is a switch and a PD is a terminal. The technology uses two pairs of cable in one Ethernet cable to supply power. Currently, the two pairs of cable can provide a maximum power output of 30W.

Based on the current situations, this HPOE solution enables you to supply power to a greater number of terminals through POE, which facilitates deployment, simplifies engineering, and reduces costs. Currently, the solution mainly is applied to weak-current intelligent systems (video surveillance systems) where POE is more widely used. It will be applied to more fields in the future.

Figure 1 HPOE solution



As shown in the preceding figure, the HPOE solution leverages the HPOE core technology to supply power through Ethernet cables to IP-based devices (power < 90W) in the weak-current system. Two products support HPOE, including an HPOE switch. It is connected using the common POE connection method to a PBOX, which then provides a power output and one Ethernet connection to the camera. In this way, highly power-demanding terminals are powered through POE.

Typical Deployment Scenario

2.1. Network Topology

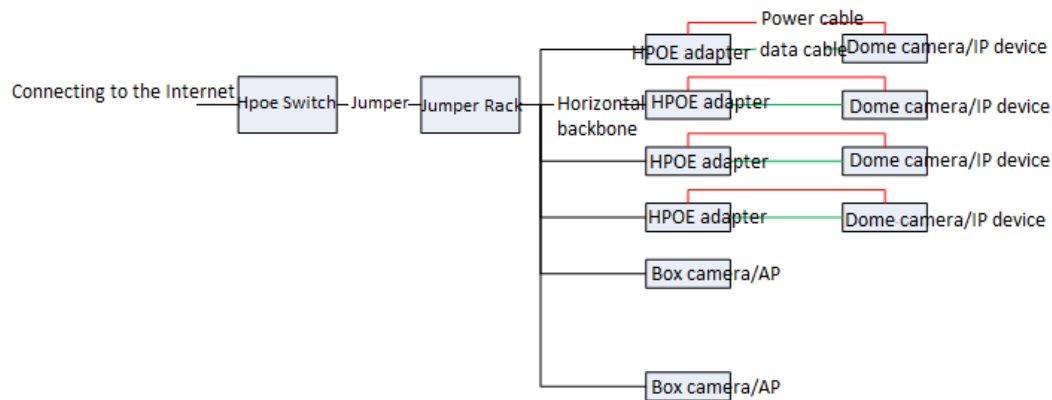
A single HPOE switch or VSU is allowed. Each device has four front electrical ports that support HPOE/POE/POE+ power output, and the other electrical ports support POE/POE+ power output. HPOE ports can be connected in the following ways:

- (1) HPOE port of the switch -> PBOX -> PD (device that does not support POE)
- (2) HPOE port of the switch -> PD (device that supports POE)

2.2 Typical Networking Model

Scenario 1: Four HPOE ports work under full load to supply power to highly power-demanding devices.

Figure 2 Networking model for scenario 1



Scenario description: In this scenario, the HPOE switch supplies power to four highly power-demanding devices at the same time. The remaining power can be supplied using the non-HPOE ports to PDs.

Configuration requirement: All the cameras can be pinged by the switch and the POE functions of the connected ports are enabled.

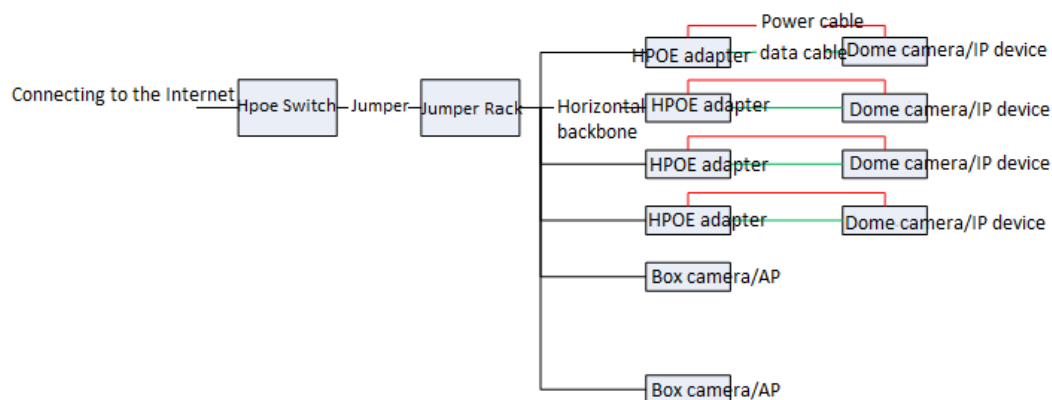
Acceptance:

On the switch, use **Show POE Interfaces Status / Show POE Power Supply** to view power supply information.

(2) Use a web browser to access the addresses of the cameras, enter your user names and passwords, install plug-ins, and verify that video surveillance is normal.

Scenario 2: Power is supplied through HPOE, POE, and POE+ at the same time.

Figure 3 Networking model for scenario 2



Scenario description: In this scenario, the HPOE switch supplies power to several highly power-demanding devices and less power-demanding devices at the same time through HPOE, POE, and POE+.

Configuration requirement: All the cameras can be pinged by the switch and the POE functions of the connected ports are enabled.

Acceptance: same as those for scenario 1

3 Highlight Functions

3.1 Highlight Service Functions

Function: Switch port trunk allowed VLAN only x-x

Original problem: By default, a port of our switch allows transmission of data for all VLANs after being configured as a trunk port. Therefore, frontline engineers have to configure a command to remove all VLANs before project implementation. This increases the workload and may easily cause the loop problem.

Implementation: This function allows transmission of data for only specified VLANs. Therefore, VLAN removal is not required before project implementation.

Effect:

3.2 Highlight Management Function

Function: show this

Original problem: A live network has many configurations. Frontline engineers have to use **show run** or **show run included/begin** to view the configurations of ports or in the OSPF view. This is inconvenient.

Implementation: This function allows engineers in a view to query the configuration commands for the view directly.

Effect:

Function: A version upgrade file name is not limited and **show upgrade history** can be used to view the upgrade history.

Original problem: The 10.X version upgrade file must be renamed **rgos.bin** and the version upgrade history is inaccessible.

Implementation: An version upgrade file can have any name. This facilitates frontline planning. A command is provided for viewing the upgrade history.

Effect:

Function: **debug syslog limit** command

Original problem: After the debug function of a device is enabled, debug log generation may affect the device. In some cases, it results in a device fault.

Implementation: Before the debug function is enabled, the command **debug syslog limit time seconds numbers numbers** can be run to limit the printing time and content of debug logs.

Function: one-key fault information collection

Original problem: To locate a problem that occurs in a product developed a long time ago, engineers must collect information two to three times and on-site engineers have to repeatedly trigger the problem. This is not allowed on a live network.

Implementation: The version 11.x supports one-key fault information collection. A single command is used to collect all related device operation information, including feature-related table entries and underlying component information. The following shows how it is implemented.

In the debug support view:

The tech-support package saves all operation information from the engine and line card to a file. By default, the file is stored in a USB flash drive. If no USB flash drive is available, the file is stored in the **flash** or **tmp** directory. (Recommended)

The tech-support console prints engine operation-related information on the console.

4 Best Practice Solution Guide

4.1 Preparation

4.1.1 Preparation before Installation

Preparation before installation

To ensure the installation successfully, make sure the installation site meets the requirements including ventilation, temperature, humidity, sanitary, power, fiber, cable .etc

For Detail information ,see 《hardware installation and reference guide》 of corresponding products , such as 《RG-S8600E Series Switch Hardware Installation and Reference Guide,V1.10》

On the other hand, double confirm following important information ahead of schedule:

1. The network topology, configuration, IP routing information, user scale, traffic information and running status of current production network.
2. Equipment list and pre-sale solution.
3. Customer's requirements and corresponding features
4. The compatibility with current devices, like STP, AP with switches of other vendors
5. Current link and interface status including optical connector, fiber etc.
6. Design the Network and acquire customer's agreement
7. Customer's network verification requirements
8. Customer's cut over plan requirements
9. Customer's acceptance inspection requirements

4.1.2 Check Switch Software/Hardware

Check software

This figure shows how to display soft and hardware version

```
Ruijie# show version
```

Software selection rules::

1. We suggest you to update the new switch to the latest firmware
2. We suggest you to update the existing switch to the latest firmware also if they're running steady
3. For detail technical specification , see corresponding product configuration guide ,or visit our service portal <http://case.ruijienetworks.com/>

Note:

Confirm whether the project is a "expansion network" or "new network"

- 1) If the project is a expansion network ,focus on the compatibility as following :

Expansion module/line card

For detail information , see "**Hardware Supported**" in corresponding product 《release notes》

Expansion switch

Focus on the compatibility of different protocols (especially MSTP) between Ruijie and other vendor. Do a full validation before implementation

- 2) If the project is a new network

Determine whether the current/latest firmware supports customer's requirement , see configuration guide of corresponding product

- 3) Read 《release notes》 and double confirm the matters need attention

Check hardware:

Take S8600E series switches as example (see 《RG-S8600E Series Switch Hardware Installation and Reference Guide》)

1. M8600E-CM:

| LED | Identification on the panel | Status | Meaning |
|---------------------------------------|-----------------------------|----------------|--|
| System LED | Status | Off | The module is NOT receiving power. |
| | | Solid red | The module is faulty. |
| | | Blinking green | Initialization is in progress. Continuous blinking indicates errors. |
| | | Solid green | The module is operational. |
| Primary/standby supervisor module LED | Primary | Off | The module acts as the standby supervisor module. |
| | | Solid green | The module acts as the primary supervisor module. |
| Fault alarm LED | Alarm | Off | No fault |
| | | Solid red | The system fails, interrupting functioning of the whole system or a module; the device may be damaged if it continues operating. |
| | | Solid yellow | The device overheats, which will affect the system performance. The system may continue operating. |
| SD card slot status LED | None | Off | SD card is not installed, or the is not connected. |
| | | Solid green | An SD card is loaded. |
| | | Blinking green | Data is being accessed from and written into an SD card |
| FE module status LED | FE | Off | The module is NOT receiving power or is NOT in the position. |
| | | Solid green | The module is operational. |
| | | Solid red | The module is faulty. |
| | | Blinking green | Initialization is in progress. Continuous blinking indicates errors. |
| Fan status LED | FAN | Solid green | The fan is operational. |
| | | Solid yellow | The fan is NOT in the position. |
| | | Solid red | The fan is faulty. |
| Power status LED | PWR | Off | The power supply module is NOT in the position. |
| | | Solid green | The power supply module is operational. |
| | | Solid red | The power supply module is faulty. |
| MGMT port status LED | None | Off | The MGMT port is NOT connected. |
| | | Green | The MGMT port is connected at 1000Mbps. |
| | | Yellow | The MGMT port is connected at 10/100Mbps. |
| | | Blinking | The MGMT port is transmitting or receiving data. |

2. M8600E-24GT20SFP4XS-ED LED

| LED | Identification on the panel | Status | Meaning |
|-------------|-----------------------------|----------------|---|
| System LED | Status | Off | The module is NOT receiving power. |
| | | Solid red | The module is faulty. |
| | | Blinking green | Initialization is in progress. Continuous blinking indicates errors. |
| | | Solid green | The module is operational |
| | | Solid yellow | System temperature exceeds the alarm temperature, affecting system performance. But the system continues running. |
| GT port LED | Link/ACT | Off | The port link is NOT connected. |

| | | | |
|---------------|----------|--------------|--|
| | | Solid green | The port is connected at 1000Mbps. |
| | | Solid yellow | The port is connected at 10/100Mbps. |
| | | Blinking | The port is transmitting and receiving data. |
| SFP port LED | Link/ACT | Off | The port link is NOT connected. |
| | | Solid green | The port is connected at 1000Mbps. |
| | | Solid yellow | The port is connected at 100Mbps. |
| | | Blinking | The port is transmitting and receiving data. |
| SFP+ port LED | Link/ACT | Off | The port link is NOT connected. |
| | | Solid green | The port is connected. |
| | | Blinking | The port is transmitting and receiving data. |

3. M8600E-48GT-ED LED

| LED | Identification on the panel | Status | Meaning |
|---------------|-----------------------------|----------------|---|
| System LED | Status | Off | The module is NOT receiving power. |
| | | Solid red | The module is faulty. |
| | | Solid yellow | High temperature alarm. The system keeps operating but the performance is affected. |
| | | Blinking green | Initialization is in progress. Continuous blinking indicates errors. |
| | | Solid green | The module is operational |
| RJ45 port LED | Link/ACT | Off | The port link is NOT connected. |
| | | Solid green | The device is connected to the 1000M port. |
| | | Solid yellow | The device is connected to the 10M or 100M port. |
| | | Blinking | The port is sending and receiving data. |

4. M8600E-48GT-EF LED

| LED | Identification on the panel | Status | Meaning |
|---------------|-----------------------------|----------------|---|
| System LED | Status | Off | The module is NOT receiving power. |
| | | Solid red | The module is faulty. |
| | | Solid yellow | High temperature alarm. The system keeps operating but the performance is affected. |
| | | Blinking green | Initialization is in progress. Continuous blinking indicates errors. |
| | | Solid green | The module is operational |
| RJ45 port LED | Link/ACT | Off | The port link is NOT connected. |
| | | Solid green | The device is connected to the 1000M port. |
| | | Solid yellow | The device is connected to the 10M or 100M port. |
| | | Blinking | The port is sending and receiving data. |

4.2 Best Practic Scenario

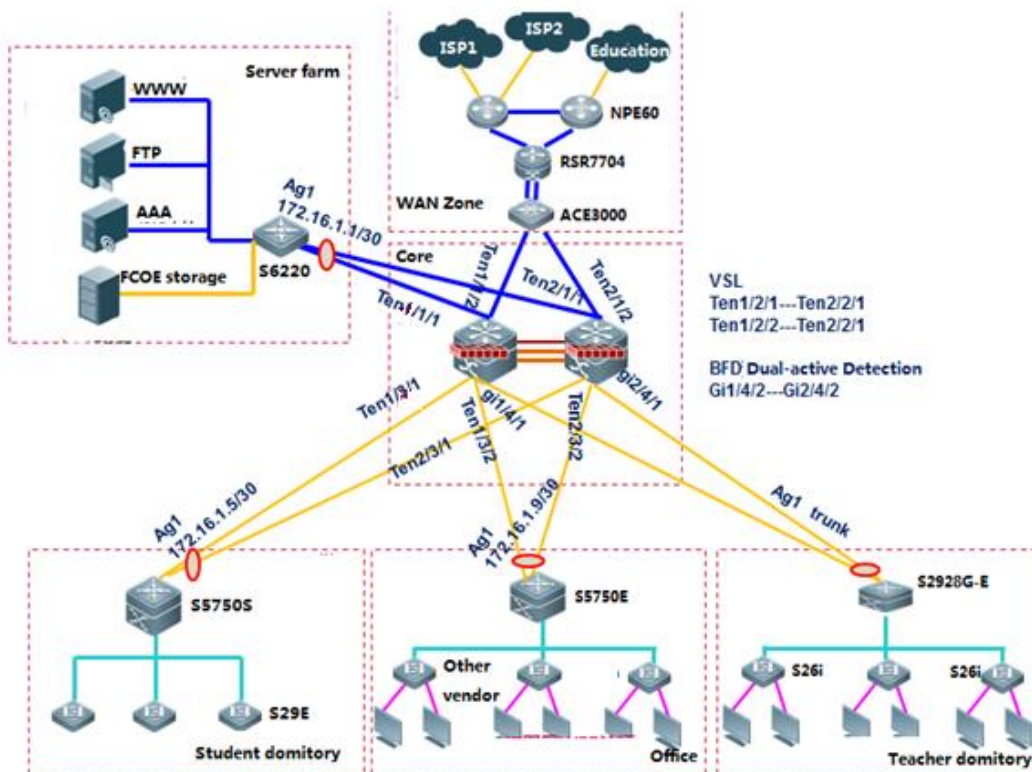
4.2.1 Education

Dual core using VSU

I. Requirement

1. Core switch: Configure two S8600E chassis swithes as VSU , and connect VSU to WAN zone with double uplinks
2. Server farm: Connect some Servers and storage to data center switch S6220 and S6220 is also gateway for servers and storage .You can also connect other servers that have equiped with double NICs to VSU with double links
3. Aggregation switch: For Layer 3 Aggregation switches , they are user gateway and run OSPF .Connect a aggregation switch to two VSU members independently . For Layer 2 aggregation switch , connect them to two VSU members independently ,and VSU is the user gateway.

II. Network Topology



III. Common requirements and features

Select features below base on requirements:

| Num | Customer requirement | Feature | Description | Reference |
|-----|--|---|---|---|
| 1 | Core supports reliability when one chassis fails | OSPF , MSTP+VRRP- 【Core and distribution switches】 | Support ECMP routing loadbalance by OSPF multiple links or tuning OSPF cost | Common Feature --->IP Routing --->OSPF Typical Feature --->MSTP+VRRP |
| 2 | Dual redundant uplinks from distribution to core | OSPF , MSTP+VRRP- 【Core and distribution switches】 | Support ECMP routing loadbalance by OSPF multiple links or tuning OSPF cost | Common Feature --->IP Routing --->OSPF Typical Feature --->MSTP+VRRP |
| 3 | Dynamic routing protocol , link switchover when links down | OSPF- 【Core , distribution and WAN zone】 | OSPF switch over to redundancy links automatically when main link down | Common Feature --->IP Routing --->OSPF |
| 4 | System management | Initialization- 【all switches】 | Hostname , port description , syslog , clock , SNMP etc. | Initialization |
| 5 | IPv4 and IPv6 | IPv6 address , OSPFV3- 【Core , distribution switches】 | Build IPv6 network | Common Feature --->IPv6 |
| 6 | IPv4 and IPv6 multicast | PIM-SM- 【all switches】 | Build multicast network | Common Feature --->Multicast |

IV. Optional optimization

Select optional optimization below base on requirements:

| Num | Technology | Description | Reference |
|-----|---|---|--|
| 1 | DHCP Snooping(Mandatory when using DHCP Server) | Prevent illegal DHCP server --- 【access switch】 | Common Feature --->Security --->DHCP Snooping |
| 2 | IP Source Guard(Mandatory when using DHCP Server) | Prevent user from setting static IP address --- 【access switch】 | Common Feature --->Security --->IP Source Guard |
| 3 | ARP-check | Defend against ARP spoofing --- 【access switch】 | Typical Feature --->Defending against ARP spoofing |
| 4 | NFPP | Tune up port rate limite/attack threshold , 100/200 PPS per port by default , which may drop normal user packets when attack happens or a trunk port carries more than 100 users.Also protect switch itself --- 【distribution or core switch】 | Common Feature --->Security --->NFPP |
| 5 | RLDP,STP Portfast+Bpduguard | Prevent LOOP --- 【access switch】 | Common Feature --->Reliability --->RLDP |

V. Verification

1. For single feature verification, see verification method in each corresponding chapter
2. For total network running status, see Appendix

4.3 Appendix: Common Verification Command

4.3.1 Show version

The example shows the firmware version on a box switch:

This example shows the firmware version on a chassis switch:

```
Ruijie#show version slot
```

Examples

| Dev Slot | Configured Module | Online Module | User Status | Software Status | --- | --- | ----- | --- | ----- |
|----------|-------------------|------------------|-------------|-----------------|-----|-----|-------|-----|-------|
| 1 1 | none | none | | | | | | | |
| 1 2 | M8606-24SFP/12GT | M8606-24SFP/12GT | installed | none | | | | | |
| 1 3 | M8606-2XFP | M8606-2XFP | uninstalled | cannot startup | | | | | |
| 1 4 | M8606-24GT/12SFP | M8606-24GT/12SFP | installed | ok | | | | | |
| 1 M1 | M8606-CM | M8606-CM | master | | | | | | |
| 1 | M2 | | | | | | | | |

Dev: Device ID, equal to 1 by default, and maybe 2 or more if it is a VSU.

Slot: Slot ID slots number of different model vary, but all model has 2 engine slots --M1 and M2 and can plug in either M1 or M2 if there's only one engine.

Port: Port number of the line card. Combo port calculates as one port only.

Configured Module : Installed module, and must be the same to Online Module

Online Module: Whether the module powers on and recognized

User Status: Line card status, installed or uninstalled

Software Status: "OK" indicates working properly, Master indicates primary engine, backup indicates backup engine.

4.3.2 Show run

This example shows how to display switch configuration

```
Ruijie# show run
```

Examples

```
Ruijie# show run
```

```
Building configuration...
```

```
Current configuration : 1366 bytes
```

```

version 11.0(1B2)

!

cwmpp

!

install 3 M8600E-24XS4QXS-DB

!

sysmac 1414.4b34.5624

!

nfpp

```

4.3.3 Show CPU

View cpu utilization every 5s, 1m or 5m by command "show cpu"

```
Ruijie# show cpu
```

Examples

```
Ruijie# show cpu
```

```
=====
```

CPU Using Rate Information

CPU utilization in five seconds: 4.80%

CPU utilization in one minute: 4.10%

CPU utilization in five minutes: 4.00%

| NO | 5Sec | 1Min | 5Min Process |
|----|-------|-------|-------------------|
| 1 | 0.00% | 0.00% | 0.00% init |
| 2 | 0.00% | 0.00% | 0.00% kthreadd |
| 3 | 0.00% | 0.00% | 0.00% ksoftirqd/0 |
| 4 | 0.00% | 0.00% | 0.00% events/0 |

--More--

Usually, "CPU utilization in five minutes" shall be kept below 30% ; Pay attention if it exceeds 60%.

4.3.4 Show memory

This example shows current memory status

Configurations

```
Ruijie# show memory
```

Usually, "Used Rate" shall be kept below 75%; Pay attention if it exceeds 80%.

4.3.5 Show power

This example shows the power status on a chassis switch

```
Ruijie# show power
```

Examples

```
Ruijie# show power
```

```
Chassis-type: RG_S8605E
```

```
Power-redun: no
```

```
Energy-saving: off
```

| power-id | power-type | supply(W) | status | vol-in/out(V) | cur-out(mA) | supply-out(W) |
|----------|------------|-----------|--------|---------------|-------------|---------------|
|----------|------------|-----------|--------|---------------|-------------|---------------|

| | | | | | | |
|---|--------|-----|----|---------|------|----|
| 1 | PA600I | 600 | ok | 231 /12 | 3500 | 42 |
|---|--------|-----|----|---------|------|----|

| | | | | | | |
|---|--------|-----|----|---------|------|----|
| 2 | PA600I | 600 | ok | 232 /12 | 1000 | 12 |
|---|--------|-----|----|---------|------|----|

| | | | | | | |
|---|-----------|------|----|---------|---|---|
| 3 | PA1600I_P | 1600 | ok | N/A /55 | 0 | 0 |
|---|-----------|------|----|---------|---|---|

4.3.6 Show fan

This example shows the fan status on a chassis switch

```
Ruijie# show fan
```

Examples

```
Ruijie# show fan
```

```
Chassis-type: RG_S8605E
```

```
Fan-id: 1
```

```
Fan-type: M05_FAN
```

```
Serial Number: 1234567890123
```

```
Energy-saving: off
```

| fan-id | status | mode | speed-level |
|--------|--------|------|-------------|
|--------|--------|------|-------------|

| | | | |
|---|----|--------|-----|
| 1 | ok | normal | N/A |
|---|----|--------|-----|

4.3.7 Show temperature

This example shows the temperature status on a chassis switch

```
Ruijie# show temperature
```

Examples

```
Ruijie#show temperature
```

```
Chassis-type: RG_S8605E
```

| slot | card_type | warning(C) | shutdown(C) | current(C) |
|------|-----------|------------|-------------|------------|
|------|-----------|------------|-------------|------------|

| | | | | |
|---|-----|-----|-----|-----|
| 1 | N/A | N/A | N/A | N/A |
|---|-----|-----|-----|-----|

4.3.8 Show clock

Configurations

```
Ruijie# show clock
```

Examples

```
Ruijie#show clock
```

```
18:01:03 beijing Tue, Dec 3, 2013
```

4.3.9 Show log

This example shows logs in buffer

Configurations

```
Ruijie# show log
```

Examples

```
Ruijie#show log
```

```
Syslog logging: enabled
Console logging: level debugging, 15495 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 15496 messages logged
Standard format: false
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence-number log messages: enable
Sysname log messages: enable
Count log messages: enable
Trap logging: level informational, 15242 message lines logged,0 fail
```

This example shows how to read logs in flash

Configuration

```
Ruijie# more flash:syslog.txt
```

Examples

```
Ruijie# more flash:syslog.txt
*Dec 24 10:47:38: %SYS-5-CONFIG_I: Configured from console by console
*Dec 24 10:50:00: %SYS-5-CONFIG_I: Configured from console by console
*Dec 24 11:07:50: %SYS-5-CONFIG_I: Configured from console by console
*Dec 24 11:08:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 1, changed st
*Dec 24 11:08:14: %LLDP-4-CREATEREM: Port GigabitEthernet 0/2 created one new neighb
*Dec 24 11:08:16: %LINK-3-UPDOWN: Interface GigabitEthernet 0/2, changed state to up
*Dec 24 11:08:16: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/
*Dec 24 11:09:35: %SYS-5-CONFIG_I: Configured from console by console
```

4.3.10 Verify flash

This example shows how to display file list in flash

Configurations

```
Ruijie# dir
```

Examples

```
s8600E-VSU#dir
Directory of flash:/
Number  Properties      Size           Time                               Name
-----  -
1      -rw-             43.5k      Mon Jun 6 10:01:12 2016  g
2      drw-             560B      Thu Jun 2 10:05:30 2016  at
3      drwx             160B      Fri Apr 1 03:15:46 2016  dev
4      drwx             160B      Fri Apr 1 03:15:35 2016  rep
5      drwx             224B      Fri Apr 1 03:15:36 2016  var
6      drwx             304B      Mon Jun 6 11:39:18 2016  yws
7      drwx             224B      Mon Jun 6 11:47:45 2016  yyy
8      -rw-             32.3k      Thu Sep 8 14:01:59 2016  config.text.0908
9      -rw-             2.0k      Sun Sep 18 10:09:12 2016  split.db
10     drwx             160B      Fri Apr 1 03:15:46 2016  addr
11     drwx             304B      Mon Jun 6 10:01:42 2016  data
12     -rw-             2.4k      Thu May 5 01:06:26 2016  vsd_standalone.text.1
13     -rw-             0B        Fri Apr 8 01:08:00 2016  ssc_fp_appmng_debug.txt
14     -rw-             27.5k      Wed May 11 12:02:41 2016  virtual_switch.text
```

4.3.11 Verify local MAC address

You can enter "show arp" EXEC command to display Layer 3 MAC address.

This example shows the Layer 3 MAC address on S8600 switch. "--" indicates that this arp entry is a local one.

Configuration

```
Ruijie# show arp
```

Examples

```
Ruijie#show arp

Total Numbers of Arp: 7

Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 0 0013.20a5.7a5f arpa VLAN 1
Internet 192.168.195.67 0 001a.a0b5.378d arpa VLAN 1
Internet 192.168.195.65 0 0018.8b7b.713e arpa VLAN 1
```

4.3.12 Verify MAC table

This example displays mac address table

Configuration

```
Ruijie# show mac-address-table
```

Examples

```
Ruijie#show mac-address-table
```

| Vlan | MAC Address | Type | Interface |
|------|----------------|---------|---------------------|
| 1 | 1414.4b19.ecc0 | DYNAMIC | GigabitEthernet 0/2 |

This example displays mac address statistics

```
Ruijie#show mac-address-table count
```

```
Dynamic Address Count : 51
```

```
Static Address Count : 0
```

```
Filter Address Count : 0
```

```
Total Mac Addresses : 51
```

4.3.13 Verify ARP table

Configuration

```
Ruijie# show arp
```

Examples

```
Ruijie#show arp
```

```
Total Numbers of Arp: 7
```

```
Protocol Address Age(min) Hardware Type Interface
```

```
Internet 192.168.195.68 0 0013.20a5.7a5f arpa VLAN 1
```

```
Internet 192.168.195.67 0 001a.a0b5.378d arpa VLAN 1
```

This example displays detail arp information including port, vlan etc

Configurations

```
Ruijie# show arp detail
```

Examples

```
Ruijie#show arp detail
```

```
IP Address MAC Address Type Age(min) Interface Port
20.1.1.1 000f.e200.0001 Static -- -- --
20.1.1.1 000f.e200.0001 Static -- VI3 --
20.1.1.1 000f.e200.0001 Static -- VI3 Gi2/0/1
```

This example displays arp statistics

Configuration

```
Ruijie# show arp count
```

Examples

```
Ruijie#show arp count
The Arp Entry counter:0
The Unresolve Arp Entry:0
```

4.3.14 Verify route table

This example displays IP route table

Configuration

```
Ruijie# show ip route
```

Examples

```
Ruijie# show ip route
```

Codes: C - Connected, L - Local, S - Static

R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

This example displays IP route statistic

Configuration

```
Ruijie# show ip route count
```

Examples

```
Ruijie# show ip route count
```

```
----- route info -----
```

```
the num of active route: 5
```

4.3.15 Verify interface IP address

This example displays IP address on Layer 3 port or SVI

Configuration

```
Ruijie# show ip interface brief
```

Examples

```
Ruijie# show ip interface brief
```

```
Interface IP-Address(Pri) IP-Address(Sec) Status Protocol GigabitEthernet 0/10 2.2.2.2/24 3.3.3.3/24 down down
GigabitEthernet 0/11 no address no address down down
```

```
VLAN 1 1.1.1.1/24 no address down down
```

4.3.16 Verify interface status and description

This example displays port status of all ports including link status, vlan, duplex, speed, medium type

Configuration

```
Ruijie# show interface status
```

Examples

```
Ruijie# Ruijie#show interfaces GigabitEthernet 0/1 status
```

| Interface | Status | Vlan | Duplex | Speed | Type |
|-----------|--------|------|--------|-------|---------------------|
| ----- | ----- | ---- | ----- | ----- | GigabitEthernet 0/1 |
| up | 1 | Full | | | |
| 1000M | copper | | | | |

This example displays interface description

Configuration

```
Ruijie# show interface description
```

This example displays port status of port G0/1

```
Ruijie#show interfaces gigabitEthernet 0/1

Index(dec):1 (hex):1

GigabitEthernet 0/1 is DOWN , line protocol is DOWN

Hardware is marvell GigabitEthernet
Description: TO-ZGE-S8610-2_GE2/1
Interface address is: no ip address

MTU 1500 bytes, BW 1000000 Kbit

Encapsulation protocol is Bridge, loopback not set

Keepalive interval is 10 sec , set

Carrier delay is 2 sec

RXload is 1 ,Txload is 1

Queueing strategy: WFQ

Switchport attributes:

  interface's description:"TO-ZGE-S8610-2_GE2/1"

  medium-type is copper

  lastchange time:0 Day: 0 Hour:45 Minute:26 Second

  Priority is 0

  admin duplex mode is AUTO, oper duplex is Unknown

  admin speed is AUTO, oper speed is Unknown

  flow control admin status is OFF,flow control oper status is Unknown

  broadcast Storm Control is ON,multicast Storm Control is OFF,unicast Storm Control is ON

  5 minutes input rate 0 bits/sec, 0 packets/sec

  5 minutes output rate 0 bits/sec, 0 packets/sec

  37167599 packets input, 2566418459 bytes, 45 no buffer, 45 dropped ----->input direction dropping
  Received 58764 broadcasts, 0 runts, 0 giants

  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
```

```
37210638 packets output, 2565322398 bytes, 0 underruns , 0 dropped ----->output direction dropping
```

```
0 output errors, 0 collisions, 0 interface resets
```

4.3.17 Verify interface packets statistics

This example displays traffic counters on port F0/1

Configuration

```
Ruijie# show interface counters
```

Examples

```
Ruijie#show int fastEthernet 0/1 counters

Interface : Fa0/1

5 minute input rate : 0 bits/sec, 0 packets/sec
5 minute output rate : 0 bits/sec, 0 packets/sec

InOctets          : 68023600
InUcastPkts       : 92842
InMulticastPkts   : 36700
InBroadcastPkts   : 75636

OutOctets         : 3630373
OutUcastPkts      : 32053
OutMulticastPkts  : 1059
OutBroadcastPkts  : 13231

[1] Undersize packets : 0
[2] Oversize packets  : 0
[3] collisions        : 0
[4] Fragments         : 0
[5] Jabbers           : 0
[6] CRC alignment errors : 0
[7] AlignmentErrors   : 0
[8] FCSErrors         : 0
[9] dropped packet events (due to lack of resources): 0
[10] packets received of length (in octets):
```

```
64:119136, 65-127: 75769, 128-255: 12663,
256-511: 3149, 512-1023: 1955, 1024-1518: 38849
```

- [1] A packet which is shorter than Ethernet's minimum packet size of 64 bytes, but has correct checksum.
- [2] A packet which is longer than Ethernet's maximum packet size of 1518 bytes, but has correct checksum.
- [3] Collisions: multiple sites try to send traffic at the same time, leading to a collision, usually it's the duplex problem
- [4] A packet which is shorter than Ethernet's minimum packet size of 64 bytes, but has wrong checksum.
- [5] A packet which is shorter than Ethernet's minimum packet size of 1518 bytes, but has wrong checksum.
- [6] CRC alignment errors: The same to FCS, CRC is the local checksum .Peer recalculates and compares with FCS

after receiving the packet

- [7] Alignment error: Alignment errors are caused by misaligned reads and writes
- [8] Modified or missing fram: FCS checksum error
- [9] Statistics for Dropped packets
- [10] Statistics for received packets based on packet length (in octets)

This example displays traffic summary of all ports

```
Ruijie#show interfaces counters summary
```

| Interface | InOctets | InUcastPkts | InMulticastPkts | InBroadcastPkts |
|-----------|-----------|-------------|-----------------|-----------------|
| ----- | ----- | ----- | ----- | ----- |
| Gi0/1 | 162238880 | 112646 | 16345 | 2 |
| Gi0/2 | 36514 | 6 | 157 | 1 |
| Gi0/3 | 0 | 0 | 0 | 0 |
| Gi0/4 | 99540 | 0 | 420 | 0 |
| Gi0/5 | 0 | 0 | 0 | 0 |
| Gi0/6 | 0 | 0 | 0 | 0 |

This example displays traffic rate of all ports

```
Ruijie#show interfaces counters rate
```

| Interface | Sampling Time | Input Rate (bits/sec) | Input Rate (packets/sec) | Output Rate (bits/sec) |
|-----------|---------------|-----------------------|--------------------------|------------------------|
| ----- | ----- | ----- | ----- | ----- |
| Gi0/1 | 5 seconds | 0 | 0 | 0 |
| Gi0/2 | 5 seconds | 60 | 0 | 60 |
| Gi0/3 | 5 seconds | 0 | 0 | 0 |
| Gi0/4 | 5 seconds | 0 | 0 | 0 |
| Gi0/5 | 5 seconds | 0 | 0 | 0 |