Example for CLI Configuration

（GTP-2871/GTP-5271）

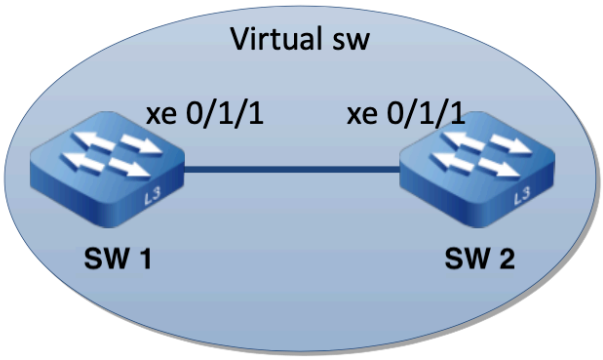
Contents

1. Example for stacked configuration

1.1 Example for configuring basic stacking functions

Networking requirements

According to user requirements, the two switches adopt stacking networking.



Configuration stacking

1. According to the topology, connect the stack cables between the devices. Note: Must optical port, 10G optical module
2. Enable stacking on the two devices and configure stack member IDs and stack ports.
3. Restart both devices at the same time. Check the stacking situation.

Operating steps

Step1 Connect the stack according to the topology.
Step2 Enable stacking on the switch and configure stack member IDs and stack ports respectively.

#Configure for SW1
Console(config)# switch mode virtual
Need to reboot to take effect.
Console(config)# switch virtual member 0
Need to reboot to take effect.
Console(config)#vsl-channel 2 0/1/1
Configs of this port will be lost,are you sure to continue (y/n)?[n]y
Need to reboot to take effect.

Configure for SW2
Console(config)# switch mode virtual

Need to reboot to take effect.
Console(config)# switch virtual member 1
Need to reboot to take effect.
Console(config)#vsl-channel 1 0/1/1
Configs of this port will be lost,are you sure to continue (y/n)?[n]y
Need to reboot to take effect.

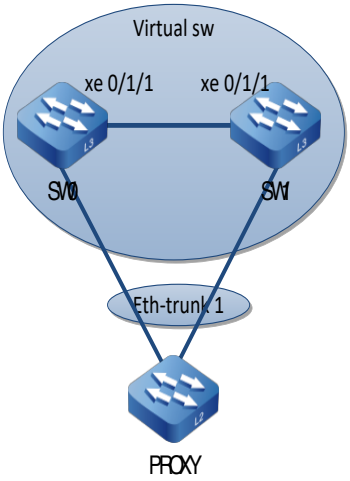
Configuration file

#View the stack after reboot
Console#show switch virtual members
Informations of stack devices:
switch 1 <local>
macaddress 00:fe:fe:fe:00:11 device id 0 priority 0
master device left hops 0 right hops 0
stack identity fe001100517a
it's master device 00:fe:fe:fe:00:11 device id 0
switch 2
macaddress 00:fe:fe:fe:00:22 device id 1 priority 0
slave device left hops infinite right hops 1
stack identity fe001100517a
it's master device 00:fe:fe:fe:00:11 device id 0
Total entries: 2

1.2 Example for ETH-TRUNK MAD function

Networking requirements

Two devices form a stack system and are connected to upstream and downstream devices through an inter-device EthTrunk. Users want to perform stack split detection through the cross-device Eth-Trunk.



Configuration stacking

1. Configure the dual-active detection function of the Eth-Trunk 1 connected to the PROXY in the stack system.
2. Configure the MAD proxy function of Eth-Trunk 1 on the SW.

Operating Steps

Step1 Configure stacking between SW0 and SW1. For details, see Steps for configuring basic stacking functions.

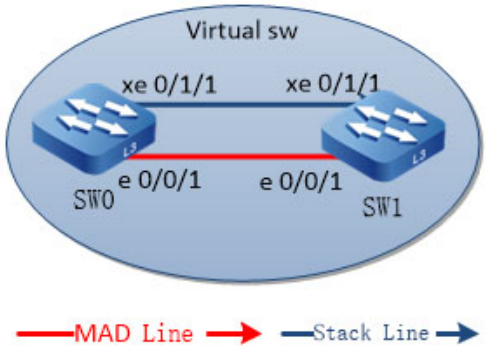
Step2 Configure the functions of the Eth-Trunk connected to the PROXY stack and enable the MAD and MAD proxy functions respectively.
Stacking system configuration
Console(config)# interface eth-trunk 1
Console(config-if-eth-trunk-1)#link-aggregation members ethernet 0/0
/1 ethernet 1/0/1
Console(config-if-eth-trunk-1)#mad lacp

SW Configuration
Console(config)# interface eth-trunk 1
Console(config-if-eth-trunk-1)#link-aggregation members interface ethernet 0/0
/1 ethernet 1/0/1
Console(config-if-eth-trunk-1)#mad lacp-relay-

1.3 Example for BFD MAD function

Networking requirements

Two devices form a stack system and are connected to upstream and downstream devices through an inter-device EthTrunk. Users want to perform stack split detection through the cross-device Eth-Trunk.



Configuration stacking

As shown in above, configure BFD MAD detection in the stack system.

Operating Steps

Step1 Configure stacking between SW0 and SW1. For details, see Steps for configuring basic stacking functions.

Step2 Configure a MAD BFD port: Use the vlan100 interface and 20, 21 of each SW for MAD detection, and configure the BFD port for reserved ports.

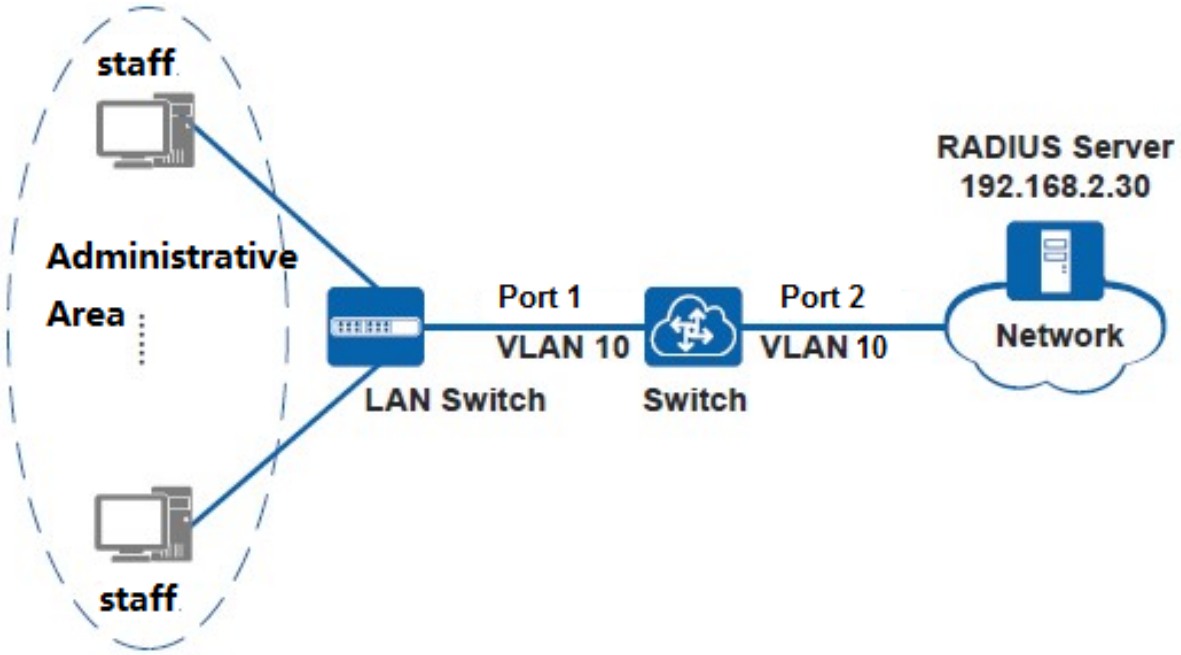
```
Console(config)#vlan 100
Console(config-if-vlan)#switchport ethernet 0/0/1 ethernet 1/0/1
Console(config-if-vlan)#interface range eth 0/0/1 ethernet 1/0/1
Console(config-if-range)#switchport pvid 100
Console(config-if-range)#virtual mad exclude
Step3 MAD BFD configuration
Console(config)#bfd enable
Console(config)#interface vlan-interface 100
Console(config-if-vlanInterface-100)#mad bfd enable
Console(config-if-vlanInterface-100)#mad device-id 0 ip address 20.20.20.20 255.255.255.0
Console(config-if-vlanInterface-100)#mad device-id 1 ip address 20.20.20.21 255.255.255.0
```

2. Example for 802.1x configuration

Configure the 802.1x Authentication Control Enterprise user access Network example

Networking requirements

As the following figure shows, Terminal in a company office area through switch access to the company's internal network. If the company is in the condition of illegal access and unauthorized access, it will lead to the destruction of enterprise business systems and the disclosure of critical information assets, Therefore, the administrator hopes that switch can control the user's network access rights to ensure the security of the company's intranet.



configuration thinking

The following ideas are used on the Switch configuration:
1.Create and configure RADIUS server group.
2.Enable the 802.1x authentication function to achieve strict control of the network access rights of employees in the office area.

operating steps

Step 1 Create VLAN and configure the interface allowed to pass the VLAN to ensure that the network is unobstructed.

```
Console(config)#vlan 10
Console(config-if-vlan)#exit
Console(config)#interface range ethernet 0/0/1 ethernet 0/0/2
Console(config-if-range)#switchport pvid 10
Console(config-if-range)#exit
```

Step 2 Create and configure the radius server and associate it with the domain.

```
# Create and configure radius servers
Console(config)#aaa

# Create AAA dot1x authentication as radius
Console(config-aaa)#radius host Test-Dot1x
Console(config-aaa-radius-test-dot1x)#primary-auth-ip 192.168.2.30 1812
Console(config-aaa-radius-test-dot1x)#primary-acct-ip 192.168.2.30 1813
Console(config-aaa-radius-test-dot1x)#auth-secret-key 1234
Console(config-aaa-radius-test-dot1x)#acct-secret-key 1234
Console(config-aaa-radius-test-dot1x)#username-format without-domain
Console(config-aaa-radius-test-dot1x)#exit

# Create an authentication domain and configure the dot1x authentication application domain
Console(config-aaa)#domain test_dot1x
Console(config-aaa-domain-test_dot1x)#radius host binding test-dot1x
Console(config-aaa-domain-test_dot1x)#state active
Console(config-aaa-domain-test_dot1x)#exit
Console(config-aaa)#exit
```

Step 3 Configuring 802.1x authentication

```
# 802.1x authentication on port 1.
Console(config)#dot1x method macbased interface ethernet 0/0/1
```

Step 4 Configure port management ip.

```
#The switch should be in the same segment as the radius server
Console(config)#interface vlan-interface 1
Console(config-if-vlanInterface-1)#ip address 192.168.2.1 255.255.255.0
Console(config-if-vlanInterface-1)#exit
```

Step 5 Verify configuration results.

1.Execute the **show dot1x** command configuration information.

2.Users start the 802.1x client on the terminal, enter the username and password, and begin to authenticate.

3.If the user's user name and password are validated correctly, the client page displays the authentication information. After that, the user can access the network.

4.After the user is online, the administrator can execute the **show dot1x session** command on the device to view the online 802.1x user information.

Configuration file

Configuration file of Switch:
Console(config)#show running-config if radius dot1x vlan

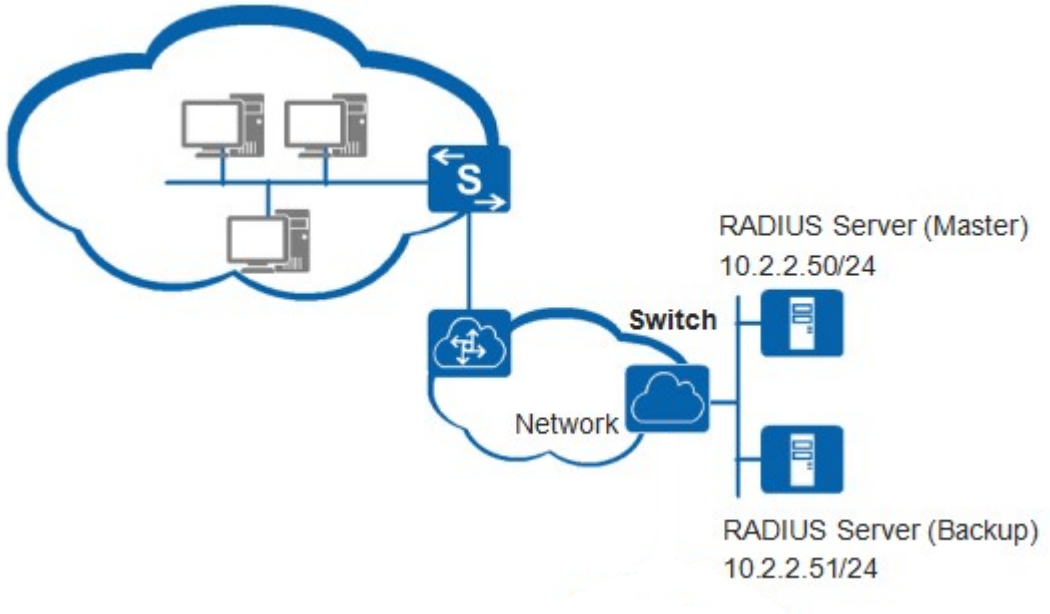
```
![VLAN]
vlan 10
exit
![DOT1X]
dot1x method macbased interface ethernet 0/0/1
![RADIUS]
aaa
radius host Test-Dot1x
primary-auth-ip 192.168.2.30 1812
primary-acct-ip 192.168.2.30 1813
auth-secret-key 1234
acct-secret-key 1234
username-format without-domain
exit
domain test_dot1x
radius host binding test-dot1x
state active
exit
exit
![IF]
interface vlan-interface 1
ip address 192.168.2.1 255.255.255.0
exit
```

3. Example for AAA configuration

3.1 Configuration uses the RADIUS protocol for authentication examples

Networking requirements

As shown in the following figure, Switch is used as the destination network to access the server. The user needs to pass the server's remote authentication to the Telnet on the Switch. The remote authentication methods on Switch are as follows:
1. Use the RADIUS server to authenticate the access user.
2. RADIUS server 10.2.2.50/24 is used as the Master authentication server, and the RADIUS server 10.2.2.51/24 is a backup authentication server, and the authentication port number is default to 1812.



Configuration thinking

The RADIUS protocol is used to authenticate users with the following ideas.
1. Configure the RADIUS server.
2. Configure AAA login and enable to log in as radius mode.
3. The switch and the server are in the same segment.

Operating steps

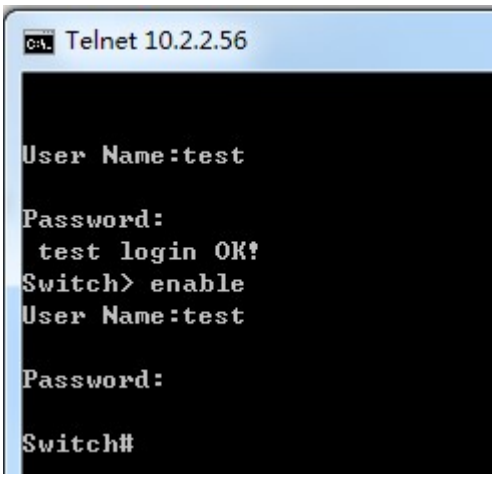
Step 1 Configure the VLANIF interface ip.
Console(config)#hostname Switch
Console(config)#interface vlan-interface 1
Console(config-if-vlanInterface-1)#ip address 10.2.2.56 255.255.255.0

Console(config-if-vlanInterface-1)#exit
Step 2 Configure the RADIUS server
Console(config)#aaa
Console(config-aaa)#radius host Test_Radius
Console(config-aaa-radius-test_radius)#primary-auth-ip 10.2.2.50 1812
Console(config-aaa-radius-test_radius)#primary-acct-ip 10.2.2.50 1813
Console(config-aaa-radius-test_radius)#second-auth-ip 10.2.2.51 1812
Console(config-aaa-radius-test_radius)#second-acct-ip 10.2.2.51 1813
Console(config-aaa-radius-test_radius)#auth-secret-key 1234
Console(config-aaa-radius-test_radius)#acct-secret-key 1234
Console(config-aaa-radius-test_radius)#username-format without-domain
Console(config-aaa-radius-test_radius)#exit

Step 3 Configure the domain and associate it with the Radius server
Console(config-aaa)#domain Test_Domain
Console(config-aaa-domain-test_domain)#radius host binding Test_Radius
Console(config-aaa-domain-test_domain)#state active
Console(config-aaa-domain-test_domain)#exit
Console(config-aaa)#exit

Step 4 Configure the user login to use the radius method.
Console(config)#muser radius Test_Radius chap

Step 5 Verify the configuration
Use the CMD Telnet switch on the window7 and use the radius server user to authenticate.



Configuration View:
Console(config)#show radius host

ServerName = Test_Radius
PrimAuthServerIP = 10.2.2.50 PrimAcctServerIP = 10.2.2.50
SecAuthServerIP = 10.2.2.51 SecAcctServerIP = 10.2.2.51
PrimAuthPort = 1812 PrimAcctPort = 1813
SecAuthPort = 1812 SecAcctPort = 1813

```
Auth-secretKey    = 1234                Acct-secretKey    = 1234
UserNameFormat = without-domain
RealTimeAcctSwitch = open             RealTimeAcctTime = 12
RadiusClientIP    = 0.0.0.0
------------------------------------------------------------------------

Total [1] item(s), printed [1] item(s).

Console(config-aaa-domain-test_domain)#show domain
  There is no default domain
  DomainName            : Test_Domain
  RADIUSServerName : Test_Radius
  Access-limit         : disabled
  AccessedNum          : 0
  Scheme                 : radius
  State                   : Active
------------------------------------------------------------------------

  Total [1] item(s).
```

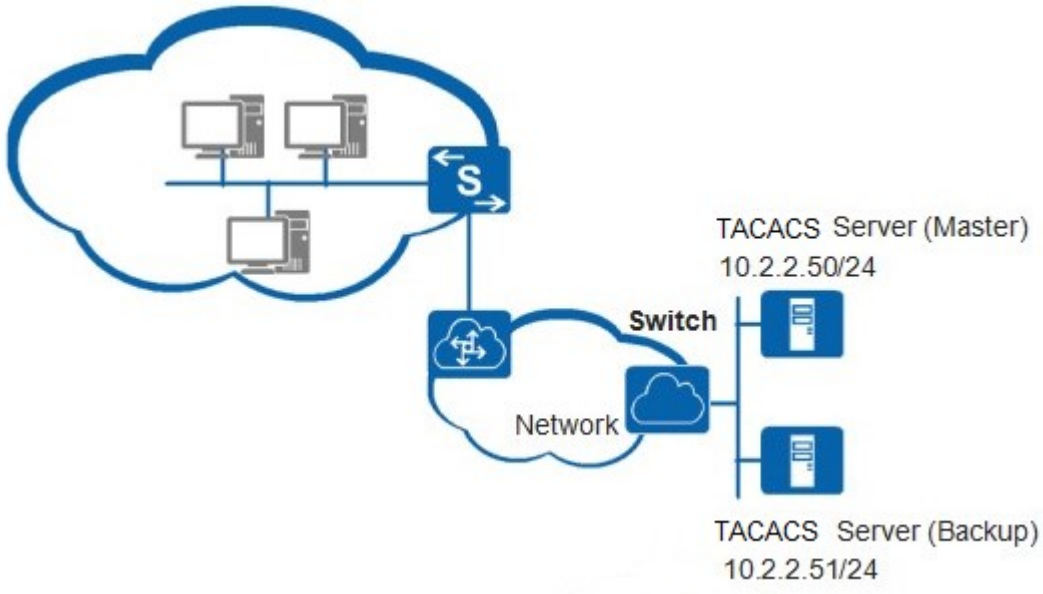
Configuration file

```
Configuration file of the switch
Console(config-aaa)#show ru radius if
![RADIUS]
aaa
radius host Test_Radius
primary-auth-ip 10.2.2.50 1812
second-auth-ip 10.2.2.51 1812
primary-acct-ip 10.2.2.50 1813
second-acct-ip 10.2.2.51 1813
auth-secret-key 1234
acct-secret-key 1234
username-format without-domain
exit
radius host binding
exit
domain Test_Domain
radius host binding test_radius
state active
exit
![OAM]
muser radius Test_Radius chaphostname Switch
![IF]
interface vlan-interface 1
ip address 10.2.2.56 255.255.255.0
Exit
```

3.2 Configure use the TACACS protocol for authentication examples

Networking requirements

As shown in the following figure, Switch is used as the destination network to access the server. The user needs to pass the server's remote authentication to the Telnet on the Switch. The remote authentication methods on Switch are as follows:
1. Use the TACACS server to authenticate the access user.
2. Tacacs server 10.2.2.50/24 is used as the primary authentication server, and the TACACS server 10.2.2.51/24 is a standby authentication server, and the authentication port number is default to 1812.



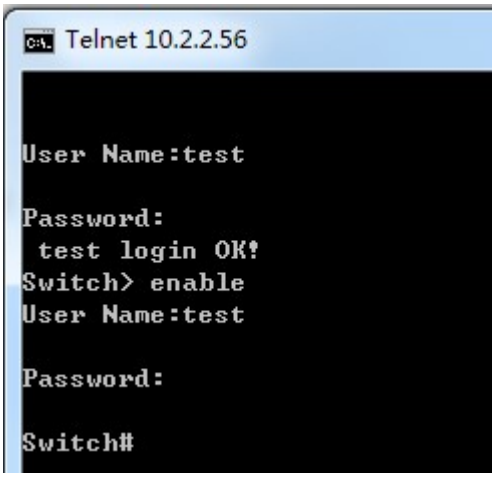
Configuration thinking

The TACACS protocol is used to authenticate users with the following ideas.
1.Configure the TACACS server.
2.Configure AAA login and enable to log in as the TACACS mode.
3.The switch and the server are in the same segment.

Operating steps

Step 1 Configure the VLANIF interface ip.
Console(config)#hostname Switch
Console(config)#interface vlan-interface 1
Console(config-if-vlanInterface-1)#ip address 10.2.2.56 255.255.255.0
Console(config-if-vlanInterface-1)#exit
Step 2 Configure the RADIUS server .

Console(config)#tacacs+ primary server 10.2.2.50 key 1234
Console(config)#tacacs+ secondary server 10.2.2.51 key 1234
Step 3 Configure user login to use Tacacs authentication.
Console(config)#muser tacacs+
Step 4 Verification configuration
Use the CMD Telnet switch on the window7 and use the TACACS server user to authenticate.



View the configuration .
Console(config)#show tacacs+
Primary Server Configurations:
IP address: : 10.2.2.50
Connection port: : 49
Connection timeout: : 5
Key: : 1234

Secondary Server Configurations:
IP address: : 10.2.2.51
Connection port: : 49
Connection timeout: : 5
Key: : 1234

Configuration file

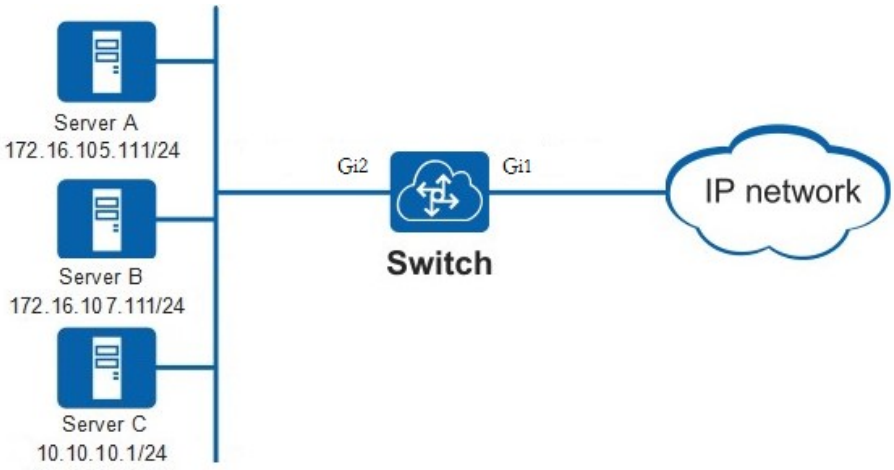
Configuration file for Switch
Console(config)#show running-config if tacacs+ oam
![TACACS+]
tacacs+ primary server 10.2.2.50 key 1234
tacacs+ secondary server 10.2.2.51 key 1234
![OAM]
muser tacacs+
hostname Switch
![IF]
interface vlan-interface 1
ip address 10.2.2.56 255.255.255.0
exit

4. Example for ACL configuration

4.1 Configure the IP ACL example

Networking requirements

As shown below, Switch as a gateway equipment, hanging the Server for tenement. It isrequired to configure ACL, prohibit all users of subnet 172.16.105.0/24 to access the external network at any time, prohibit all users of the subnet 172.16.107.0/24 to access the external network in a certain time range, and allow other users to access the external network.



Configuration thinking

The following ideas are used to configure message filtering based on ACL:
1.Configuration time period;
2.Configure a standard ACL rule that is marked with a number.
3.This rule is applied to the interface Gi2.

Operating steps

Step 1 Configuration time

```
Console(config)#time-range test
Console(config-timerange-test)#periodic weekdays 9:00:00 to 17:00:00
Console(config-timerange-test)#exit
```

Step 2 Configure ip acl

```
Console(config)#access-list 1 deny 172.16.105.111/24 time-range test
```

Step 3 Apply this rule on the ingress port direction.
Console(config)#access-group ip-acl 1 in
Step 4 Verify the configuration results
Use the show time-range command to see if the configured time period is active.
Console(config)#show time-range all
Current time is: 15:48:13 2014/01/01 Wednesday

time-range: test (Active)
periodic: weekdays 09:00:00 to 17:00:00

Total entries: 1
Use the show access-list command IP acl configuration.
Console(config)#show access-list config all
The step of ACL subitem number: 1

IP Access List 1, match-order is config, 1 rule:
0 : deny 172.16.105.111/24 time-range test

total config rules: 1 rules

View the applied ACLs.
Console(config)#show access-list runtime all
access-list 1 subitem 0 running inbound

total runtime rules: 1 rules

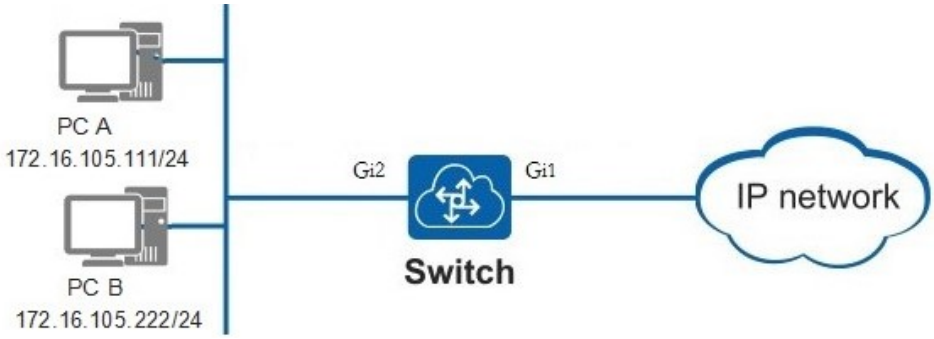
Configuration file

Configuration file for Switch
Console(config)#show running-config qacl
![QACL]
time-range test
periodic weekdays 09:00:00 to 17:00:00
exit
access-list ip-acl 1
0 deny 172.16.105.111/24 time-range test
exit
access-group ip-acl 1 in

4.2 Configure the mix ACL example

Networking requirements

As shown below, Switch is a gateway device, which requires ACL to be configured, forbid the source IP is 172.16.105.111, and destination IP is 172.16.105.8, 172.16.105.10, 172.16.105.12, 172.16.105.14 UDP message, allowing other UDP messages to pass.



Configuration thinking

The following ideas are used to configure message filtering based on ACL:
1.Configure an extended ACL rule that is marked with a number.
2.This rule is applied to the interface Gi2.

Operating steps

Step 1 Configure mix ACL
Console(config)#access-list 2000 deny ip-pro udp 172.16.105.111/32 172.16.105.8/32

Step 2 Apply this rule in the ingress port direction of Gi2
Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#access-group hybrid-acl 2000 in
Console(config-if-ethernet-0/0/2)#exit

Step 3 Verify configuration results.
View the ACL configuration.
Console(config)#show access-list config all
The step of ACL subitem number: 1

Hybrid Access List 2000, match-order is config, 1 rule:
0 : deny udp 172.16.105.111/32 172.16.105.8/32

total config rules: 1 rules

View applied ACL.
Console(config)#show access-list runtime all
access-list 2000 subitem 0 running interface e0/0/2 inbound

total runtime rules: 1 rules

Configuration file

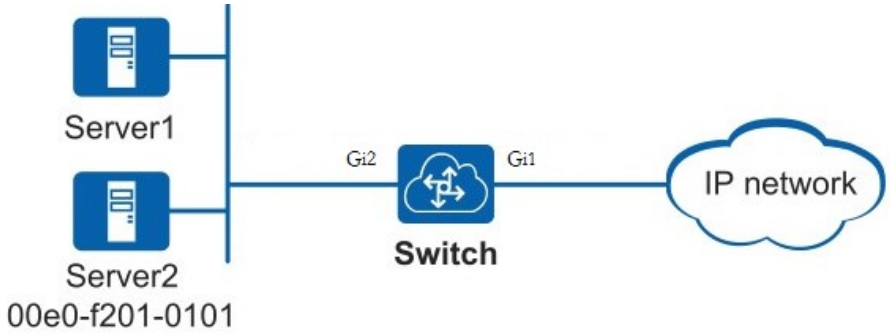
Configuration file for Switch
Console(config)#show running-config qacl

![QACL]
access-list hybrid-acl 2000
0 deny udp 172.16.105.111/32 172.16.105.8/32
exit
interface ethernet 0/0/2
access-group hybrid-acl 2000 in
Exit

4.3 Configure the Mac ACL example

Networking requirements

As shown below, Switch is a gateway device, which requires ACL to be configured. The source MAC address is 00e0-f201-0101, and the destination MAC address is 0260-e207-0002 message.



Configuration thinking

The following ideas are used to configure message filtering based on ACL:
1.Configure a MAC ACL rule that is marked with a number.
2.Application of this rule at the interface Gi2.

Operating steps

Step 1 Configure a number - based MAC ACL rule
Console(config)#access-list 1000 deny 00:e0:f2:01:01:01 a-host 02:60:e2:07:00

:02 a-host

Step 2 Apply this rule in the direction of the Gi2 ingress

```
Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#access-group mac-acl 1000 in
Console(config-if-ethernet-0/0/2)#exit
```

Step 3 Verify the configuration results

Use the show access-list command to view the mac acl configuration.

```
Console(config)#show access-list config all
The step of ACL subitem number: 1

Mac Access List 1000, match-order is config, 1 rule:
   0 : deny 00:e0:f2:01:01:01 ff:ff:ff:ff:ff:ff 02:60:e2:07:00:02 ff:ff:ff:ff:ff:ff

total config rules: 1 rules
```

Use the **show access-group** command to view the ports on which acl has been applied.

```
Console(config)#show access-list runtime all
  access-list 1000 subitem 0 running interface e0/0/2 inbound

total runtime rules: 1 rules
```

Configuration file

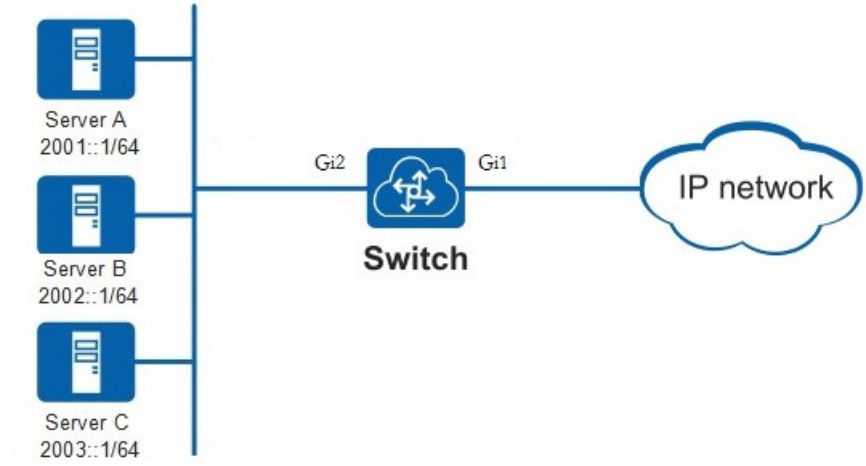
Switch configuration file

```
Console(config)#show running-config qacl

![QACL]
access-list mac-acl 1000
0 deny 00:e0:f2:01:01:01 ff:ff:ff:ff:ff:ff 02:60:e2:07:00:02 ff:ff:ff:ff:ff:ff

exit
interface ethernet 0/0/2
access-group mac-acl 1000 in
exit
```

4.4 Configure the IPV6 standard ACL example

Networking requirements

As shown below, Switch as a gateway equipment, under the tenant Server. It is required to configure ACL, prohibit all users of subnet 1 (2001:: 1/64) to access the external network at any time and allow other users to access the external network.



Configuration thinking

The following ideas are used to configure message filtering based on ACL:

1. Configuration time period;
2. Configure a IPv6 standard ACL rule that is identified by the name.
3. This rule is applied to the interface Gi2.

Operating steps

Step 1 Configuration time

```
Console(config)#time-range test
Console(config-timerange-test)#periodic weekdays 9:00:00 to 17:00:00
Console(config-timerange-test)#exit
```

Step 2 Configuration standard ACL

```
Console(config)#access-list ip-acl 1
Console(config-ip-nacl-1)#deny 2001::1/64 time-range test
```

Step 3 Apply this rule in the direction of the Gi2 ingress

```
Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#access-group ip-acl 1 in
Console(config-if-ethernet-0/0/2)#exit
```

Step 4 Verify the configuration results

Use the show time-range command to see if the configured time period is active.

```
Console(config)#show time-range all
Current time is: 00:09:20      2014/01/01    Wednesday

time-range: test ( Inactive )
   periodic:    weekdays    09:00:00    to    17:00:00

Total entries: 1
```

View the ipv6 standard acl configuration.

```
Console(config)#show access-list config all
The step of ACL subitem number: 1

 IP Access List 1, match-order is config, 1 rule:
  0 : deny 2001::1/64 time-range test

total config rules: 1 rules
```

View applied acl.

```
Console(config)#show access-list runtime all
 access-list 1 subitem 0 not running interface e0/0/2 inbound

total runtime rules: 1 rules
```

Configuration file

Configuration file for Switch

```
Console(config)#show running-config qacl
![QACL]
time-range test
periodic weekdays 09:00:00 to 17:00:00
exit
access-list ip-acl 1
0 deny 2001::1/64 time-range test
exit
interface ethernet 0/0/2
access-group ip-acl 1 in
exit
```

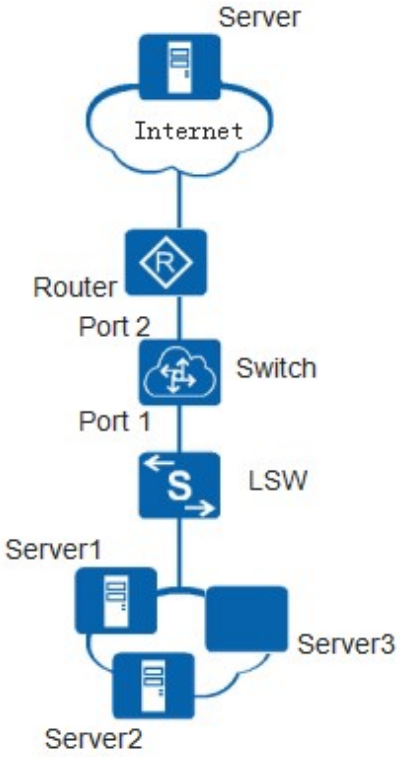
5. Example for ARP configuration

5.1 Configure the ARP example

Networking requirements

1. As shown in the figure below, Switch interface 10GE1/0/1 connects Server1, Server2 and Server3 through LAN Switch (LSW), interface 10GE1/0/2 connects router Router, and connects to 10GE1/0/2 via router Router. Requirement：Port 1-2 belongs to VLAN2.

2. in order to adapt to the rapid change of the network, ensure the correct forwarding of the message, configure the parameters of the dynamic ARP on the Switch.
3.In order to ensure the safety of communication with Server and prevent the invasion of illegal ARP messages, a static ARP table item is added to Switch interface 2. The IP address of Router is 10.2.2.3, and the corresponding MAC address is 00e0-fc01-0000.



Configuration thinking

The configuration of ARP is as follows:
1. Create VLAN and add the interface to the VLAN.
2. Configure the parameters of the user dynamic ARP.
3. Cconfigure the static ARP table item.

Operating steps

Step 1　Create the VLAN and add the interface to the VLAN
Console(config)#vlan 2
Console(config-if-vlan)#exit
Console(config)#interface range ethernet 0/0/1 t e 0/0/2
Console(config-if-range)#switchport pvid 2
Console(config-if-range)#exit

Step 2　Configure management VLAN interface 2
Console(config)#interface vlan-interface 2
Console(config-if-vlanInterface-2)#ip address 10.2.2.2 255.255.255.0
Console(config-if-vlanInterface-2)#exit

Step 3　Configure dynamic ARP aging time and static binding table items
Configure arp dynamic aging time.
Console(config)#arp aging-time 500

Configure a static ARP table entry:
Console(config)#arp 10.2.2.3 00:00:33:00:33:00 interface ethernet 0/0/2 vlan 2
Add ARP table entry successfully.

Step 4　Verify the configuration results
Use commands of Switch to configure static ARP configuration.
Console(config)#show arp static
Informations of ARP
d - days, h - hours, m - minutes, s - seconds

IpAddress	Mac_Address	Vlan	Port	Type	ExpireTime	Status
10.2.2.3	00:00:33:00:33:00	2	e0/0/2	static	00s	valid

Total entries:1
Use command of switch to view aging- time.
Console(config)#show arp aging-time
ARP age time: 500 minutes.

Configuration file

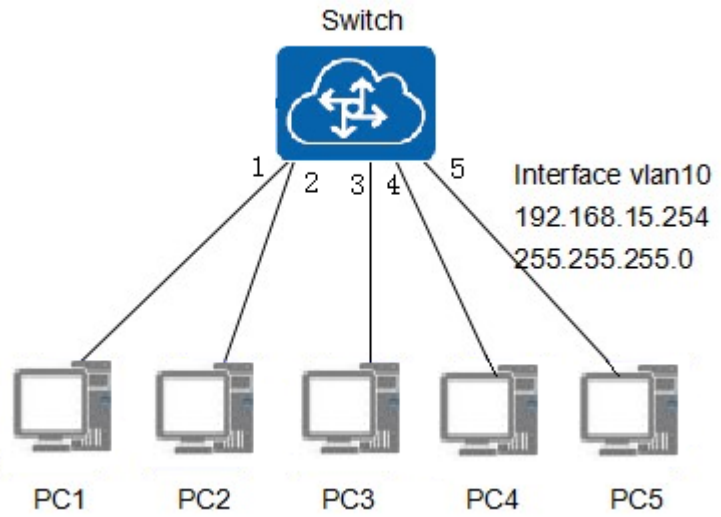
Switch configuration file
Console(config)#show running-config arp if device vlan
![VLAN]
vlan 2
exit
![DEVICE]
interface ethernet 0/0/1
switchport pvid 2

switchport hybrid untagged vlan 2
exit
interface ethernet 0/0/2
switchport pvid 2
switchport hybrid untagged vlan 2
exit
![IF]
interface vlan-interface 2
ip address 10.2.2.2 255.255.255.0
exit
![ARP]
arp aging-time 500
arp 10.2.2.3 00:00:33:00:33:00 vlan 2 interface ethernet 0/0/2

5.2 A typical case of free ARP transmission

Networking requirements

As shown below, the interface VLAN 10 (IP address is 192.168.15.254 and the subnet mask is 255.255.255.0) in the Switch system, there are 5 PC hosts (PC1, PC2, PC3, PC4 and PC4). The free ARP sending function can be configured as follows.



Configuration thinking

The following configuration ideas are as follows:
1.Set management VLAN 10 and add port 1to VLAN 10.
2.Open the ARP free function on switch.Free arp function is sent when port 1 linkup is opened on switch.

Operating steps

Step 1 Create VLANs and add interfaces to VLANs.
Console(config)#vlan 10
Console(config-if-vlan)#switchport ethernet 0/0/1
Console(config-if-vlan)#exit

Step 2 Configuration management VLAN interface 10.
Console(config)#interface vlan-interface 10
Console(config-if-vlanInterface-10)#ip address 192.168.15.254 255.255.255.0

Step 3 The free arp feature is sent when linkup is enabled.
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#gratuitous-arp
Console(config-if-ethernet-0/0/1)#exit

Step 4 Verify the configuration results.
Use commands of switch to configure the situation.
Console(config)#show gratuitous-arp interface ethernet 0/0/1
Gratuitous arp learning state: disabled
Gratuitous-arp sending-time: 1
Gratuitous-arp sending-interval: 30 seconds

Port	**Gratuitous-arp**
GE0/0/1	Enabled

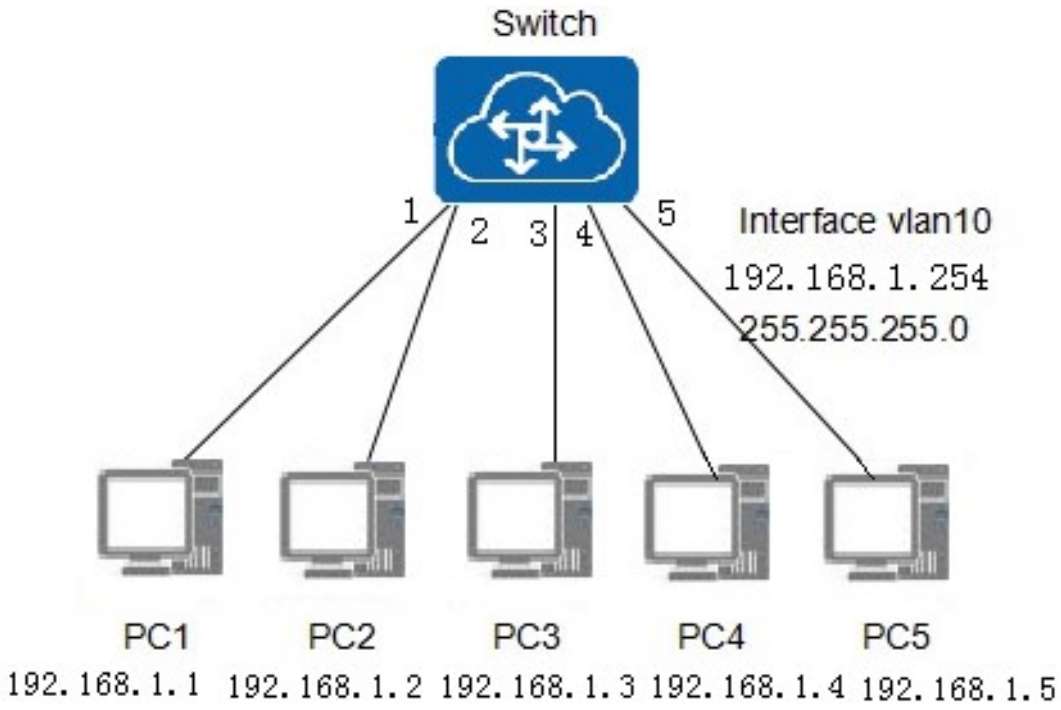
Configuration file

Configuration file for Switch
Console(config)#show running-config arp if device vlan
![VLAN]
vlan 10
exit
![DEVICE]
interface ethernet 0/0/1
switchport hybrid untagged vlan 10
exit
![IF]
interface vlan-interface 10
ip address 192.168.15.254 255.255.255.0
exit
![ARP]
arp aging-time 500
interface ethernet 0/0/1
gratuitous-arp
exit

5.3 An example of ARP detection function

Networking requirements

As shown below, the interface VLAN 10 (IP address is 192.168.1.254 and the subnet mask is 255.255.255.0) in the Switch system, there are 5 PC hosts (PC1, PC2, PC3, PC4 and PC4). The host mac+ip can be learned through the detection function to the ARP detection table item.



Configuration thinking

The following configuration ideas are as follows:
1.Set management VLAN 10 and add port 1-5 to VLAN 10.

2.The detection function is opened on the switch, and the detection range of IP and the time of detection are set up.

Operating steps

Step 1 Create the VLAN and add the interface to the VLAN.
Console(config)#vlan 10

Console(config-if-vlan)#switchport ethernet 0/0/1 to ethernet 0/0/5
Console(config-if-vlan)#exit

Step 2 Configure management VLAN interface 10.
Console(config)#interface vlan-interface 10
Console(config-if-vlanInterface-10)#ip address 192.168.15.254 255.255.255.0
Console(config-if-vlanInterface-10)# exit

Step 3 Configure the ARP detection function.

Open the ARP detection function
Console(config)#arp-probe
#Configure detection range
Console(config)#arp-probe range 192.168.15.0 24

Step 4 Verify the configuration results.
Use commands of switch to probe configuration for arp
Console(config)#show arp-probe
Information of arp-probe
switch: ON
ip list:
ip range list: 192.168.15.0/24
poll timer: 180s
retransmit count: 3, interval: 3s

Configuration file

Switch configuration file
Console(config)#show running-config if arp device vlan
![VLAN]
Vlan 10
exit
![DEVICE]
interface ethernet 0/0/1
switchport hybrid untagged vlan 10
exit
interface ethernet 0/0/2
switchport hybrid untagged vlan 10
exit
interface ethernet 0/0/3
switchport hybrid untagged vlan 10
exit
interface ethernet 0/0/4
switchport hybrid untagged vlan 10
exit
interface ethernet 0/0/5

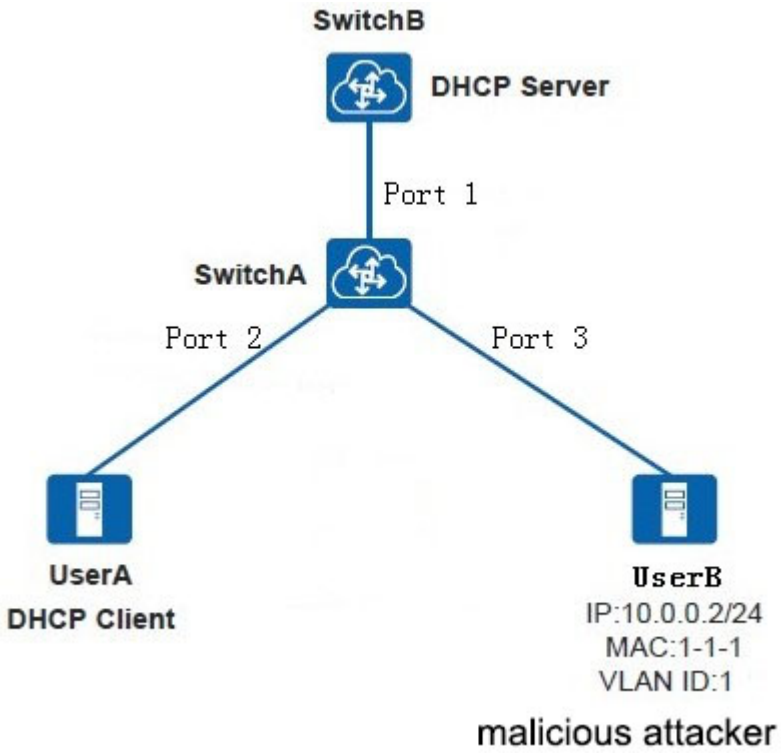
```
switchport hybrid untagged vlan 10
exit
![IF]
interface vlan-interface 10
ip address 192.168.15.254 255.255.255.0
exit
![ARP]
arp-probe range 192.168.15.0 24
arp-probe
```

6 Example of ARP security configuration

6.1 Anti-ARP spoofing configuration example

Networking requirements

As shown in the following figure, the user of a certain sector of the enterprise access the Internet through Switch A. Switch A with some users, using DHCP access IP address, some using static IP address configuration, and all users and DHCP Server are located in the same VLAN. If UserB launches a arp spoofing attack, The arp message source IP is client A, so the administrator wants switch A to prevent ARPspoofing attacks.



Configuration thinking

The configuration ideas are as follows:
The dhcp snooping function is configured on the switch A to generate the binding relation table of the address and port of the dynamic user, to enable the anti-spoofing function of arp and to enable the spoofing function of the arp gateway at the same time.

Operation steps

Step 1 Configure the DHCP Snooping function.

Enable DHCP snooping function globally
Console(config)#dhcp-snooping
Configure interface 1 is DHCP snooping trust interface.
SConsole(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#dhcp-snooping trust
Console(config-if-ethernet-0/0/1)#exit

Step 2 Enable the global arp anti - spoofing feature
Console(config)#arp anti-spoofing

Step 3 Enable spoofing gateway function
Console(config)#arp anti-spoofing gateway-disguiser

Step 4 Verify the configuration results
Configuration view.
Console(config)#show arp anti-spoofing
Information of ARP Anti-Spoofing:
ARP Anti-Spoofing : enabled
Number of ARP Anti-Spoofing bind entry : 0
ARP unknown-packet policy : discard

Status of Arp Anti-Spoofing:
ARP deny gateway disguiser : enabled
ARP source-mac-check : disabled

Configuration file

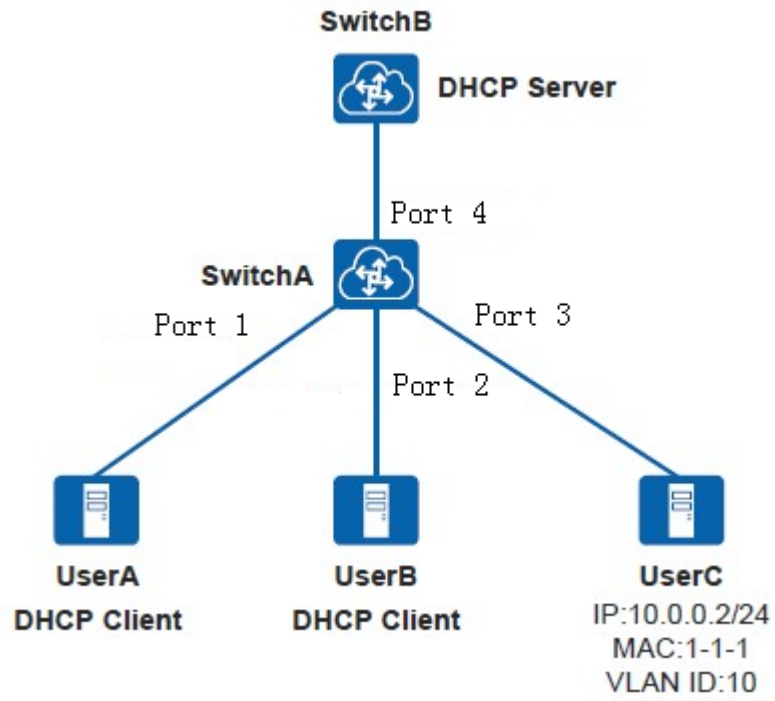
Configuration file of switch A
Console(config)#show running-config dhcpsnooping arp

![DHCPSNOOPING]
dhcp-snooping
interface ethernet 0/0/1
dhcp-snooping trust
exit
![ARP]
arp anti-spoofing
arp anti-spoofing gateway-disguiser

6.2 Typical case of dynamic ARP detection

Networking requirement

As shown in the following figure, some users in a certain enterprise department access Internet .SwitchA to Internet. Users is hung under Switch A, some use DHCP to obtain IP address, others use static configuration IP address, and all users and DHCP Server are located in the same VLAN.The following ARP threats exist in the network: an attacker sends out a large number of IP packets with unreachable destination IP addresses to carry out ARP flooding attacks to cause Switch is overloaded with CPU.



Configuration thinking

Configure on switch A using the following ideas:
Configure the speed limit of arp message to 40 pps. those who exceed the rate are considered to be attackers and discard all packets

Operation steps

Step 1 Enable function
Console(config)#arp anti-flood

Step 2 Configure the action to discard all packets from the attacker
Console(config)#arp anti-flood action deny-all

Step 3 Configure arp message speed limit to 40 pps
Console(config)#arp anti-flood rate-limit 40
Step 4 Verify configuration results.

#View Configuration Results
Console(config)#show arp anti-flood
Information of ARP Anti-Flood:
Arp anti-flood : enabled
Arp rate limit : 40pps
User recovery time : 10 minutes
Deny type : DenyAll
Denied Src MAC Source IP Port Vlan Deny Type Remain Aging Time(m)
Total entry:0.

Configuration file

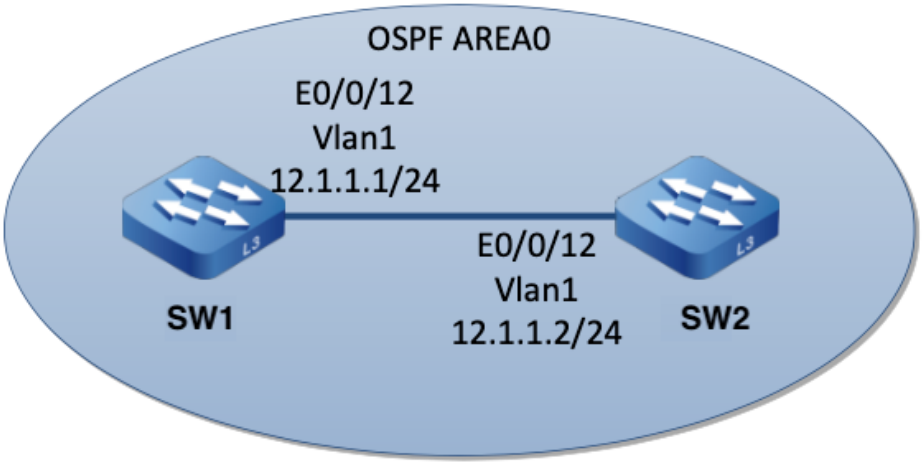
Configuration file of switch A
Console(config)#show running-config arp

![ARP]
arp anti-flood
arp anti-flood action deny-all rate-limit 40

7 Example for BFD configuration

Networking requirements

As shown in the figure, the two switch are connected through the vlanif interface and run the OSPF protocol. The user wants the ospf neighbor route to be updated quickly.



Configuration thinking

1.Configure OSPF on SwitchA and SwitchB , respectively
2.Enable the ospf bfd on the of two devices on a interconnection three-layer interface

Operating steps

Step 1 Create a VLAN and configure the VLANs to which each interface belongs, and configure the IP addresses of each VLANIF interface (/)

Step 2 Two device enable ospf segments

#SW1 configuration

```
Console(config)#vlan 12
Console(config-if-vlan)#interface vlan-interface 12
Console(config-if-vlanInterface-12)#ip address 12.1.1.1 255.255.255.0
Console(config-if-vlanInterface-12)#exit
Console(config)#router ospf
Console(config-router-ospf)# network 12.1.1.1 0.0.0.255 area 0
```

#SW2 configuration

```
Console(config)#vlan 12
Console(config-if-vlan)#interface vlan-interface 12
Console(config-if-vlanInterface-12)#ip address 12.1.1.2 255.255.255.0
Console(config-if-vlanInterface-12)#exit
Console(config)#router ospf
Console(config-router-ospf)# network 12.1.1.2 0.0.0.255 area 0
```

Step 3 Two devices with global enabling bfd,
interconnect three-layer interface enable ospf bfd

#SW1 configuration

```
Console(config)#bfd enable
Console(config)#interface vlan-interface 12
Console(config-if-vlanInterface-12)#ip ospf bfd
```

#SW2 configuration

```
Console(config)#bfd enable
Console(config)#interface vlan-interface 12
Console(config-if-vlanInterface-12)#ip ospf bfd
```

#SW1 View bfd status

```
Console(config)#show bfd session
Total Session Num: 1
Init Mode: Active
Session Working Under Asynch Mode
```

LD	SourceAddr	DestAddr	State	Holdtime Interface
0x841bbb00	12.1.1.1	12.1.1.2	UP	1860ms Vlan12

Configuration file

]

#SW1 configuration file

```
hostname SW1
interface vlan-interface 12
ip address 10.1.1.1 255.255.255.0
exit
bfd enable
router ospf
network 10.1.1.1 0.0.0.255 area 0
exit
```

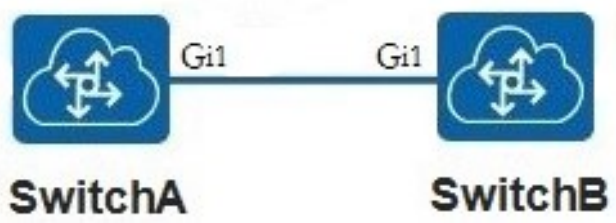
#SW2 configuration file

```
hostname SW2
interface vlan-interface 12
ip address 12.1.1.2 255.255.255.0
exit
bfd enable
router ospf
network 12.1.1.2 0.0.0.255 area 0
exit
```

8. Example for CFM configuration

Networking requirements

As the following figure shows, Switch A and switch B are interlinked via port Gi1, Requirements: Configure CFM function on SwitchA and SwitchB to realize automatic detection of link connectivity fault between the two Switch; The link performance between switch A and switch B is detected by observing the error frame received on switch A.



Configuration thinking

Configure CFM as follows:
1. Enable CFM, other use default configuration;
2. Check the CFM neighbor finding results;

operating steps

Step 1 Configuration switch A
Console(config)#hostname SwitchA
SwitchA(config)#cfm md 1
SwitchA(config-cfm-md-1)#cfm md format string name CFM_example level 7
SwitchA(config-cfm-md-1)#cfm ma 1
SwitchA(config-cfm-md-1-ma-1)#cfm ma format primary-vid name 1 primary-vlan 1
SwitchA(config-cfm-md-1-ma-1)#cfm mep 1 direction down interface ethernet 0/0/1
SwitchA(config-cfm-md-1-ma-1)#cfm mep 1 state enable
SwitchA(config-cfm-md-1-ma-1)#cfm mep 1 cc enable
SwitchA(config-cfm-md-1-ma-1)#cfm rmep 2 mep 1

Step 2 Configure switch B
Console(config)#hostname SwitchB
SwitchB(config)#cfm md 1
SwitchB(config-cfm-md-1)#cfm md format string name CFM_example level 7
SwitchB(config-cfm-md-1)#cfm ma 1
SwitchB(config-cfm-md-1-ma-1)#cfm ma format primary-vid name 1 primary-vlan 1

```
SwitchB(config-cfm-md-1-ma-1)#cfm mep 2 direction down interface ethernet 0/0/1
SwitchB(config-cfm-md-1-ma-1)#cfm mep 2 state enable
SwitchB(config-cfm-md-1-ma-1)#cfm mep 2 cc enable
SwitchB(config-cfm-md-1-ma-1)#cfm rmep 1 mep 2
```

Step 3 Verify configuration results

```
SwitchA(config-cfm-md-1-ma-1)#cfm loopback mep 1 dst-mep 2
CFM loopback rmep 2 [00:0a:6a:00:03:ee]

Reply from dst: 00:0a:6a:00:03:ee
Reply from dst: 00:0a:6a:00:03:ee
Reply from dst: 00:0a:6a:00:03:ee
Reply from dst: 00:0a:6a:00:03:ee
Reply from dst: 00:0a:6a:00:03:ee

Loopback operation: LBM-Sent = 5, LBR-Received = 5, LBR-Lost = 0%

SwitchA(config-cfm-md-1-ma-1)#cfm linktrace mep 1 dst-mep 2
CFM linktrace rmep 2 [00:0a:6a:00:03:ee]
Type CTRL+C to abort. TTL: 64, Per-Hop Timeout: 5, Flag: unuseMPDB
Linktrace sent via e0/0/1

      Hops  MAC               Ingress     IngressAction   RelayAction
        Forwarded               Egress      EgressAction
-------------------------------------------------------------------------------------------
1     00:0a:6a:00:03:ee       e0/0/1          IngOK           RlyHit
      Not Forwarded

Linktrace operation completed!

SwitchA(config)#show cfm ma
mdIdx    maIdx    maFmt          maName    maPvid    ccInterval    maStatus
   1        1    primary-vid         1         1             1      active

Total MA entries: 1
SwitchA(config)#show cfm md

mdIdx   mdFmt     mdName          mdLevel   mdStatus
   1      string   CFM_example        7       active
Total MD entries: 1, MA entries: 1, MP entries: 2

SwitchA(config)#show cfm errors
mdIdx   maIdx   mpId   type   MAC   reason

SwitchA(config)#show cfm cc
Tx CCMs : 220
```

Rx CCMs : 216

SwitchA(config)#show cfm mp local

mdIdx	maIdx	mpId	type	direction	port	admin	ccStatus	pri
1	1	1	MEP	down	e0/0/1	enable	enable	0

Total MEP entries: 1, MIP entries: 0

SwitchA(config)#show cfm mp remote

mdIdx	maIdx	rmepId	mepId	MAC	ingressPort	age(s)
1	1	2	1	00:0a:6a:00:03:ee	e0/0/1	2

Total RMEP entries: 1

Configuration file

#Configuration file of switch A

```
SwitchA(config-cfm-md-1-ma-1)#show running-config cfm
![CFM]
cfm md 1
cfm md format string name CFM_example level 7
cfm ma 1
cfm ma format primary-vid name 1 primary-vlan 1
cfm mep 1 direction down interface ethernet 0/0/1
cfm mep 1 state enable
cfm mep 1 cc enable
cfm rmep 2 mep 1
exit
exit
```

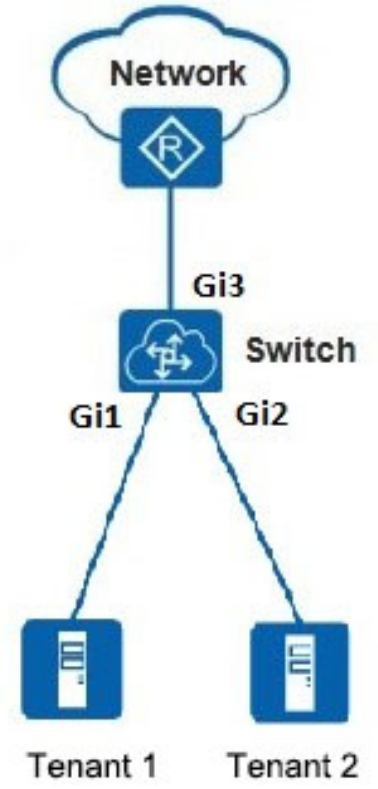
#Configuration file of switch B

```
SwitchB(config-cfm-md-1-ma-1)#show running-config cfm
![CFM]
cfm md 1
cfm md format string name CFM_example level 7
cfm ma 1
cfm ma format primary-vid name 1 primary-vlan 1
cfm mep 2 direction down interface ethernet 0/0/1
cfm mep 2 state enable
cfm mep 2 cc enable
cfm rmep 1 mep 2
exit
exit
```

9. Configure the Cos example

Networking requirements

As shown in the figure below, tenant 1 and tenant 2 rent different servers respectively. The two servers communicate with each other via an exit router and an external network of data centers. Tenant 1, tenant 2 server's message 802.1p value is 0, dscp value respectively is AF12, AF22, the user expects the message from tenant 1 and tenant 2 to send to the router in proportion of 2:1.



Configuration thinking

The following ideas are used to configure the flow speed limit:

3. Configure dscp-map to determine the basis of priority mapping;
4. The queue height is configured using WRR, and the weights of priority 1 and 2 are 2:1;

Operating steps

Step 1 Enable Dscp-map：

Console(config)#queue-scheduler dscp-map

Step 2 Configure queue scheduling

Console(config)#queue-scheduler mode wrr 1 2 1 1 1 1 1 1

Step 3 Verify configuration results

Use the command to see the configuration.

Console(config)#show queue-scheduler

Queue scheduler status : enable

Queue scheduler mode : WRR (Weighted Round Robin)

Queue1 weight is 1

Queue2 weight is 2

Queue3 weight is 1

Queue4 weight is 1

Queue5 weight is 1

Queue6 weight is 1

Queue7 weight is 1

Queue8 weight is 1

Configuration file

Switch configuration file

Console(config)#show running-config device

![DEVICE]

queue-scheduler mode wrr 1 2 1 1 1 1 1 1

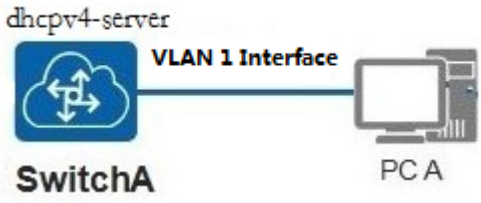
queue-scheduler dscp-map

10. DHCPv4 Configuration example

10.1 Configure the DHCPv4 server example

Networking requirements

As shown in the following figure, SwitchA assigns the IP address to the DHCPv4 server, and PC A directly connects to DHCPv4-Server to get IP.



Configuration thinking

The configuration of DHCPv4 server is as follows:
Create an address pool on switch A to assign addresses dynamically to the client.

Operating steps

Step 1 Create dhcp-server
Console(config)#dhcp-server 1 192.168.1.1

Step 2 Create address pools and configure associated properties (address pool ranges, exit gateways)
Console(config)#dhcp-server ip-pool 1
Console(config-ip-pool-1)#gateway 192.168.1.1 255.0.0.0
Console(config-ip-pool-1)#router 192.168.1.1
Console(config-ip-pool-1)#section 0 192.168.1.2 192.168.1.255
Console(config-ip-pool-1)#exit

Step 3 Configure the IP address of VLANIF1
Console(config)#interface vlan-interface 1
Console(config-if-vlanInterface-1)#ip address 192.168.1.1 255.0.0.0
Console(config-if-vlanInterface-1)#exit

Step 4 Configure the interface association dhcp-server
Console(config)#interface vlan-interface 1

Console(config-if-vlanInterface-1)#dhcp-server 1

Console(config-if-vlanInterface-1)#exit

Step 5 Enable dhcp-relay
Console(config)#dhcp-relay

Step 6 Verify configuration results
View IP address pool configuration at switch.
Console(config)#show dhcp-server ip-pool

IP pool name : 1
GateWay : 192.168.1.1
Mask : 255.0.0.0
Router : 192.168.1.1
Lease time : 1 day 0 hour 0 minute 0 second
Primary DNS : 0.0.0.0
Second DNS : 0.0.0.0
Third DNS : 0.0.0.0
Fourth DNS : 0.0.0.0
Primary NBNS : 0.0.0.0
Second NBNS : 0.0.0.0
Dhcp Option43 : NULL
Domain name : N/A

SectionNo	StartIp	EndIp	Total	Used/Idle
0	192.168.1.2	192.168.1.255	254	0/254
1	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A
5	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A

Total entries: 1 pool(s), printed 1 pool(s)

Configuration file

Configuration file of switch A
Console(config)#show running-config if dhcp ippool

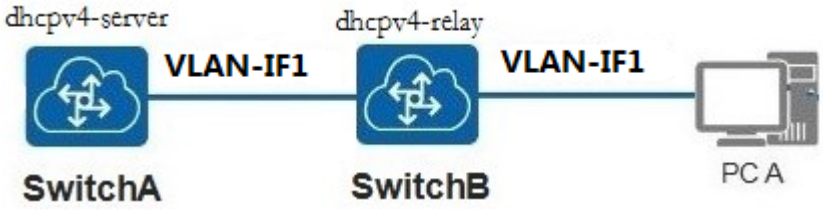
![IF]
interface vlan-interface 1

ip address 192.168.1.1 255.0.0.0
exit
![DHCP]
dhcp-relay
dhcp-server 1 192.168.1.1
interface vlan-interface 1
dhcp-server 1
exit
![IPPOOL]
dhcp-server ip-pool 1
gateway 192.168.1.1 255.0.0.0
router 192.168.1.1
section 0 192.168.1.2 192.168.1.255
exit

10.2 Configure the DHCPv4 relay example

Networking requirements

As shown below, SwitchA as DHCPv4-Server, SwitchB as L3 DHCPv4-Relay , PCA obtain IP through L3 dhcp-relay from DHCP-Server.



Configuration thinking

The configuration of the DHCPv4 relay is as follows:
The DHCPv4 relay function is configured on the switch B to realize the DHCPv4 broadcast message received by switch B and sent to the configured server in unicast form.

Operating steps

#switchB dhcp-realy is configured as follows：

Step 1 Configure switch B interface VLANIF1 for connecting to DHCP-Server of switch A.
SwitchB(config)#interface vlan-interface 1
SwitchB(config-if-vlanInterface-1)#ip address 192.168.1.2 255.0.0.0
SwitchB(config-if-vlanInterface-1)#exit

Step 2 Configure switch B interface VLANIF2 for connecting to DHCP-Client

SwitchB(config)#interface ethernet 0/0/1
SwitchB(config-if-ethernet-0/0/1)#switchport pvid 2
SwitchB(config-if-ethernet-0/0/1)#exit
SwitchB(config)#interface vlan-interface 2
SwitchB(config-if-vlanInterface-2)#ip address 10.1.1.1 255.0.0.0
SwitchB(config-if-vlanInterface-2)#exit

Step 3 Enable DHCPv4 Relay function globally
SwitchB(config)#dhcp-relay

Step 4 destination server address for relay forwarding on switch B
SwitchB(config)#dhcp-server 1 192.168.1.1
SwitchB(config)#interface vlan-interface 2
SwitchB(config-if-vlanInterface-2)#dhcp-server 1
SwitchB(config-if-vlanInterface-2)#exit

Step 5 Verify configuration results
View DHCPv4 relay configuration at SwitchB.
SwitchB(config)#show dhcp-relay

Informations of dhcp relay:

dhcp relay: enable.
dhcp relay hide server ip: disable.
dhcp relay max hops: 8.
dhcp relay source ip: ingress

Informations of port:

Port	Dhcp_Relay_State
GE0/0/1	enable
GE0/0/2	enable
GE0/0/3	enable

Configuration file

Configuration file of switch A
Refer to the DHCP-Sever section for the configuration process;

Console(config)#show running-config if dhcp ippool static_route

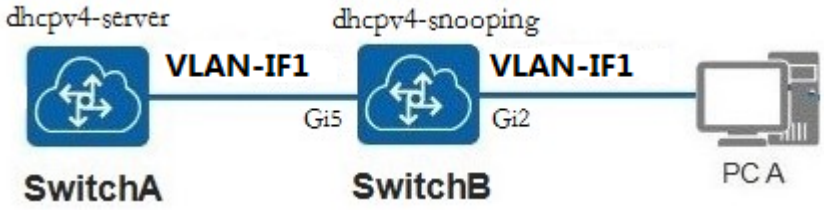
![IF]
interface vlan-interface 1
ip address 192.168.1.1 255.0.0.0
exit
![DHCP]
dhcp-relay

```
    dhcp-server 1 192.168.1.1
    interface vlan-interface 1
    dhcp-server 1
    exit
    ![IPPOOL]
    dhcp-server ip-pool 1
    gateway 10.1.1.1 255.0.0.0
    router 10.1.1.1
    section 0 10.1.1.2 10.1.1.200
    exit
    ![STATIC_ROUTE]
    ip route 0.0.0.0 0.0.0.0 192.168.1.2

# Configuration file for SwitchB
SwitchB(config)#show running-config device if dhcp

![DEVICE]
interface ethernet 0/0/1
switchport pvid 2
switchport hybrid untagged vlan 2
exit
no alarm all-packets
![IF]
interface vlan-interface 1
ip address 192.168.1.2 255.0.0.0
exit
interface vlan-interface 2
ip address 10.1.1.1 255.0.0.0
exit
![DHCP]
dhcp-relay
dhcp-server 1 192.168.1.1
interface vlan-interface 2
dhcp-server 1
exit
```

10.3 Configure DHCP v4 Snooping Example

Networking requirements

As shown in the figure below, SwitchA is used as a DHCP v4 - Server, SwitchB as a DHCP v4 - Snooping, and PCA acquires IP from a DHCPv4 - Server through a DHCP v4 - Snooping .



Configuration thinking

The configuration of DHCPv4-Snooping is as follows:
Configure DHCPv4-Snooping function, port 5 connect to DHCPv4-Server, configure as trust port, The tester B is connected to port 2, and the simulation user acquires ips;
Configure dh

Operating steps

Step 1 Configure DHCP4 snooping function
SwitchB(config)#dhcp-snooping

Step2 Configure the trust port (port connected to dhcp-server)
SwitchB(config)#interface ethernet 0/0/2
SwitchB(config-if-ethernet-0/0/2)#dhcp-snooping trust
SwitchB(config-if-ethernet-0/0/2)#exit

Step 3 Verify configuration results
SwitchB(config)#show dhcp-snooping clients
DHCP client information:
d - days, h - hours, m - minutes, s - seconds

IPAddress	mac	vlan	port	LeaseTime	ExceedTime
10.1.1.3	00:00:02:10:10:02	2	e0/0/20	1d0h0m0s	23h59m58s

Total entries: 1. Printed entries: 1.

Configuration file

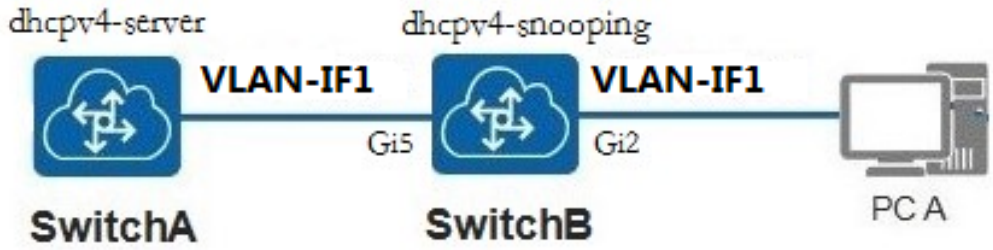
Configuration file of switch A
Refer to the DHCP-Sever section for the configuration process;

```
# Configuration file for SwitchB
SwitchB(config)#show running-config dhcpsnooping

![DHCPSNOOPING]
dhcp-snooping
interface ethernet 0/0/2
dhcp-snooping trust
exit
```

10.4 Configure the DHCP option 82 example

Networking requirements

As shown below, Switch A as DHCPv4-Server, switch B as DHCPv4-Snooping and Enable option82 function, PCA obtain IP.DHCP option 82 from DHCPv4-Server via DHCPv4-snooping. DHCP Option82 must be used with DHCP Relay or DHCP snooping.



Configuration thinking

The configuration of DHCP-Option82 is as follows:
1. Enable the DHCPv4 - snooping function
2. Modify circuit-idi-id to customize content;

operating steps

Step 1 Configure DHCP4 snooping function
SwitchB(config)#dhcp-snooping

Step 2 Configure the trust port (port connected to dhcp-server)
SwitchB(config)#interface ethernet 0/0/2
SwitchB(config-if-ethernet-0/0/2)#dhcp-snooping trust
SwitchB(config-if-ethernet-0/0/2)#exit

Step 3 Enable dhcp option82
SwitchB(config)#dhcp-option82

Configureoption82 circuit/remote-id
SwitchB(config)#interface ethernet 0/0/1
SwitchB(config-if-ethernet-0/0/1)#dhcp-option82 circuit-id user-defined test
SwitchB(config-if-ethernet-0/0/1)#dhcp-option82 remote-id user-defined ABCDEF

Step 4 Verify configuration results
#Check the DHCP option82 configuration.
SwitchB(config)#show dhcp-option82 interface ethernet 0/0/1
Status: Enabled
Format: Normal
Information format: hex

Interface Ethernet GE0/0/1:
DHCP-Option82: Enable
Strategy: Replace
Circuit ID User Defined: : test
Remote ID User Defined: : ABCDEF

Configuration file

Configuration file for SwitchA
Refer to the DHCP-Sever section for the configuration process;

Configuration file of switch B
SwitchB(config)#show ru dhcp dhcpsnooping

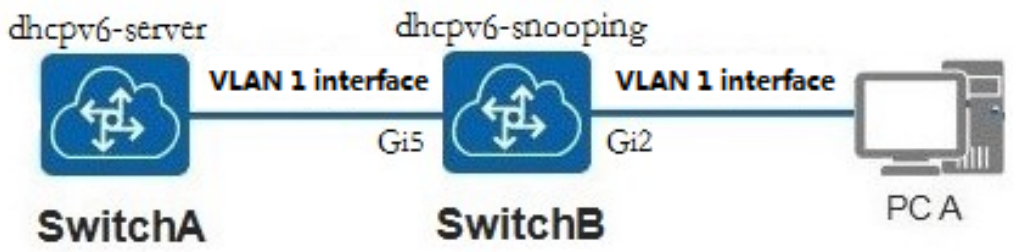
![DHCP]
dhcp-relay
dhcp-option82
interface ethernet 0/0/1
dhcp-option82 circuit-id user-defined test
dhcp-option82 remote-id user-defined ABCDEF
exit
![DHCPSNOOPING]
dhcp-snooping
interface ethernet 0/0/2
dhcp-snooping trust
exit

11 Example for DHCPv6 configuration

11.1 Configure the DHCPv6 -snooping example

Networking requirements

As shown in the following figure, SwitchA as DHCP-Server, SwitchB as DHCPv6 Snooping, PCA obtain IP from DHCPv6-Server via DHCPv6-Snooping.



Configuration thinking

The configuration of DHCPv6 snooping is as follows:
Configure the DHCPv6 - Snooping on SwitchB. Connect port5 to DHCPv6-Server, and then configure port5 as trust port; PCA connect to port2 to cbtain ip.

Operating steps

Step 1 Enable dhcpv6-snooping function
SwitchB(config)#dhcpv6-snooping

Step 2 Configure trust ports
SwitchB(config)#interface ethernet 0/0/5
SwitchB(config-if-ethernet-0/0/5)#dhcpv6-snooping trust

Step 3 Verify configuration results
Use the **show ipv6 dhcp snooping** command to view the DHCPv6 snooping configuration.

```
SwitchB(config)#show dhcpv6-snooping interface ethernet 0/0/5
Config information of DHCPv6 Snooping:
DHCPv6 Snooping status:Enable
DHCPv6 Snooping port-down-action fast-remove:Enable
Port information:
```

Port	mode	maxclients	clients
e0/0/5	trust	2048	0

Configuration file

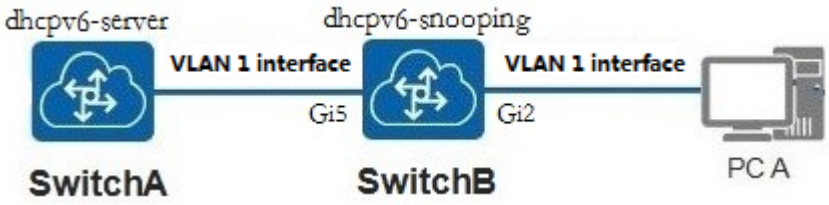
Configuration file of switch B
SwitchB(config)#show running-config dhcpv6snooping

![DHCPv6SNOOPING]
dhcpv6-snooping
interface ethernet 0/0/5
dhcpv6-snooping trust
Exit

11.2 Configure the DHCPv6 option18/37 example

Networking requirements

As shown in the following figure, SwitchA as DHCP-Server, SwitchB as DHCPv6 Snooping, PCA obtain IP from DHCPv6-Server via DHCPv6-Snooping. Enable option 18/37 function on SwitchB.



Configuration thinking

The configuration of DHCPv6 option18/37 is as follows:
1. The DHCPv6-Snooping function is configured on the switch B to connect the DHCPv6-Server to port5 and configure port5 as trust port; PCA connect to Port2 to cbtain ip.

Operating steps

Step 1 Enable dhcpv6-snooping function
SwitchB(config)#dhcpv6-snooping

Step 2 Configure trust port
SwitchB(config)#interface ethernet 0/0/5
SwitchB(config-if-ethernet-0/0/5)#dhcpv6-snooping trust
Step 3 Configure option18/37
SwitchB(config)#dhcpv6-snooping information option 18
SwitchB(config)#dhcpv6-snooping information interface-id user-defined test_option18
SwitchB(config)#dhcpv6-snooping information option 37
SwitchB(config)#dhcpv6-snooping information remote-id user-defined test_option37

Step 4 Verify configuration results

View configuration

```
SwitchB(config)#show dhcpv6-snooping information
Option 18 status: Enabled
Interface-id: user-defined: test_option18
Option 37 status: Enabled
Remote-id: user-defined: test_option37
```

Configuration file

#Configuration file of switch B

```
SwitchB(config)#show running-config dhcpv6snooping

![DHCPv6SNOOPING]
dhcpv6-snooping
interface ethernet 0/0/5
dhcpv6-snooping trust
exit
dhcpv6-snooping information option 18
dhcpv6-snooping information interface-id user-defined "test_option18"
dhcpv6-snooping information option 37
dhcpv6-snooping information remote-id user-defined "test_option37"
```

12. Example for EAPS configuration

Networking requirements

In order to do link backup and improve network reliability, redundant links are usually used in Ethernet switch networks. But the use of redundant links will lead to loop on the switchnetwork, resulting in broadcast storms and unstable MAC address table, resulting in poor communication quality and even communication disruption.
In order to solve the loop problem caused by redundant link, EAPS protocol can be deployed on devices that make up the ring network.
As shown below, two switches form a single loop, eliminating the loop through EAPS.

Configuration thinking

The configuration of EAPS is as follows:
Configure Master node on Device1 and EAPS message go control-vlan 4000;
The transmit node is configured on Device2 and EAPS message go control-vlan 4000;

Operating steps

Step 1 Disable stp function of EAPS port.

#Configure Device1

```
Console(config)#hostname Device1
Device1(config)#interface range ethernet 0/0/1 to ethernet 0/0/2
Device1(config-if-range)#no stp
Device1(config-if-range)#exit
```

#Configure Device2

```
Console(config)#hostname Device2
Device2(config)#interface range ethernet 0/0/1 to ethernet 0/0/2
Device2(config-if-range)#no stp
Device2(config-if-range)#exit
```

Step 2 configure EAPS

#Configure Device1

```
Device1(config)#interface ethernet 0/0/1
Device1(config-if-ethernet-0/0/1)#no stp
Device1(config-if-ethernet-0/0/1)#exit
Device(config)#interface ethernet 0/0/2
Device1(config-if-ethernet-0/0/2)#no stp
Device1(config-if-ethernet-0/0/2)#exit
Device1(config)#eaps
Device1(config)#eaps domain 0
Device1(config-eaps-domain-0)#control-vlan 4000
Device1(config-eaps-domain-0)#ring 1 role master primary-port ethernet 0/0/2 secondary-port
ethernet 0/0/1 level 0
Device1(config-eaps-domain-0)#ring 1 enable
Device1(config-eaps-domain-0)#exit
Device1(config)#eaps
```

#Configure Device2

```
Device2(config)#interface ethernet 0/0/1
Device2(config-if-ethernet-0/0/1)#no stp
Device2(config-if-ethernet-0/0/1)#exit
Device2(config)#interface ethernet 0/0/2
Device2(config-if-ethernet-0/0/2)#no stp
Device2(config-if-ethernet-0/0/2)#exit
Device2(config)#eaps
Device2(config)#eaps domain 0
Device2(config-eaps-domain-0)#control-vlan 4000
Device2(config-eaps-domain-0)#ring 1 role transmit primary-port ethernet 0/0/2 secondary-port
ethernet 0/0/1 level 0
Device2(config-eaps-domain-0)#ring 1 enable
Device2(config-eaps-domain-0)#exit
Device2(config)#eaps
```

Step 3 Verify configuration results.

```
Device1(config)#show eaps
EAPS state: enable

domain 0 info: control-vlan 4000, work-mode standard, topo-collect disable
Timer value: helloTimer 1, FailTimer 6, majorFaultTimer 5, preForwardTimer 6,
preUpTimer 0
   ring 1 info:
      status: active
      role    : master
      level : 0
      stm     : COMPLETE
      query solicit: disable
      primary port: GE0/0/2 forwarding
      secondary/edge port: GE0/0/1    blocking
```

```
Total 1 ring(s).

Device2(config)#s eaps
EAPS state: enable

domain 0 info: control-vlan 4000, work-mode standard, topo-collect disable
Time value: helloTimer 1, FailTimer 6, majorFaultTimer 5, preForwardTimer 6, p
reUpTimer 0
   ring 1 info:
      status: active
      role    : transit
      level : 0
      stm     : LINK-UP
      query solicit: disable
      primary port: GE0/0/2 forwarding
      secondary/edge port: GE0/0/1 forwarding
Total 1 ring(s).

Total 1 domain(s), total 1 ring(s).
```

Configuration file

Device1 configuration file

```
Device1(config)#show running-config stp eaps

![STP]
interface ethernet 0/0/1
no stp
exit
interface ethernet 0/0/2
no stp
exit
![EAPS]
eaps
eaps domain 0
control-vlan 4000
ring 1 role master primary-port ethernet 0/0/2 secondary-port ethernet 0/0/1 l
evel 0
ring 1 enable
exit
```

Configuration file for Device2

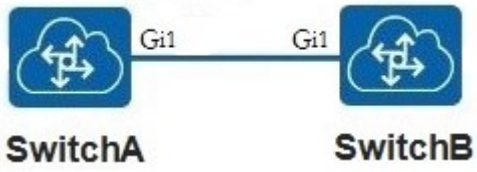
```
Device2(config)#show running-config stp eaps

![STP]
interface ethernet 0/0/1
no stp
```

```
exit
interface ethernet 0/0/2
no stp
exit
![EAPS]
eaps
eaps domain 0
control-vlan 4000
ring 1 role transit primary-port ethernet 0/0/2 secondary-port ethernet 0/0/1 level 0
ring 1 enable
exit
```

13. Example for EFM configuration

Networking requirements

As shown below, as shown below, Switch A and Switch B are requested through the port Gi1 interconnection: by configuring the EFM function in Switch A and Switch B, automatic detection of link connectivity fault between the two; through the observation of Switch received error frame A, to test the link between performance Switch A and Switch B.



Configuration thinking

The following ideas are used to configure EFM:
Enable EFM, and other use default configuration;
Check the EFM neighbor finding results;

Operating steps

Step 1 Configure Switch A
SwitchA(config)#interface ethernet 0/0/1
SwitchA(config-if-ethernet-0/0/1)#efm
SwitchA(config-if-ethernet-0/0/1)#exit

Step 2 Configure Switch B
SwitchB(config)#interface ethernet 0/0/1
SwitchB(config-if-ethernet-0/0/1)#efm
SwitchB(config-if-ethernet-0/0/1)#exit

Step 3 Verify configuration results
View the neighbor's findings:
Console(config)#show efm discovery interface ethernet 0/0/1
Interface: e0/0/1
Local Client:
EFM Mode : active
Unidirection : disable

```
    Link Monitor     : enable
    Remote Loopback: disable
    MIB Retrieval    : enable
    MTU size           : 1500
    Port Status       : operational
    Loopback Status: noLoopback
    Discovery State: sendAny
    OAMPDU Revision: 11
Remote Client:
    MAC Address       : 00:0a:6a:00:03:ee
    Vendor ID          : 0000ddff
    OUI                   : 0180c2
    OAMPDU Revision: 2
    EFM Mode           : active
    Unidirection     : disable
    Link Monitor     : enable
    Remote Loopback: disable
    MIB Retrieval    : enable
    MTU size           : 1500

Total entries: 1.
```

Configuration file

```
#Configuration file of switch A
SwitchA(config)#show running-config efm

![EFM]
interface ethernet 0/0/1
efm
exit

#Configuration file of switch B
SwitchB(config)#show running-config efm

![EFM]
interface ethernet 0/0/1
efm
exit
```

14. Example for ERPS configuration

Networking requirements

In order to make link backup and improve the reliability of the network, redundant links are usually used in Ethernet switching network. But using redundant links will generate loops on the switching network, resulting in the broadcast storm and the instability of MAC address table. This leads to poor user communication quality and even communication interruption.
In order to solve the loop problem caused by redundant links, the ERPS protocol can be deployed on the devices that constitute the ring network. The ERPS protocol is a two level breaking protocol standard defined by ITU-T, and the convergence speed is fast, which can meet the convergence speed to meet the reliability requirements of the carrier level.
As shown in the following figure, two switches make up a single loop and eliminate the loop through ERPS.

Configuration thinking

The configuration of ERPS is as follows:
Configure the ower node on the Device1, the ERPs message goes to VLAN 4000, port 2 is RPL port, port 1 is non RPL port, and the WTR timer is configured for 1 minutes.
The neighbor node is configured on Device2, the ERPs message goes to VLAN 4000, port 2 is RPL port, and port 1 is non RPL port.

Operating steps

Step 1 Disable stp function of erps port
#Configuring Device1
Device1(config)#interface range ethernet 0/0/1 to ethernet 0/0/2
Device1(config-if-range)#no stp
Device1(config-if-range)#switchport link-type trunk
Device1(config-if-range)#ex

#Configuring Device2
Device2(config)#interface range ethernet 0/0/1 to ethernet 0/0/2
Device2(config-if-range)#no stp
Device2(config-if-range)#switchport link-type trunk

```
Device2(config-if-range)#ex
```

Step 2 Configure erps

```
#Configure Device1
Device1(config)#erps instance 1
Device1(config-erps-inst-1)#control-vlan 4000
Device1(config-erps-inst-1)#port0 ethernet 0/0/2 owner
Device1(config-erps-inst-1)#port1 ethernet 0/0/1
Device1(config-erps-inst-1)#protected-instance 0
Device1(config-erps-inst-1)#ring 1
Device1(config-erps-inst-1)#ring level 0
Device1(config-erps-inst-1)#ring enable
Device1(config-erps-inst-1)#exit
Device1(config)#erps

#Configure Device2
Device2(config)#erps instance 1
Device2(config-erps-inst-1)#control-vlan 4000
Device2(config-erps-inst-1)#port0 ethernet 0/0/2 neighbor
Device2(config-erps-inst-1)#port1 ethernet 0/0/1
Device2(config-erps-inst-1)#protected-instance 0
Device2(config-erps-inst-1)#ring 1
Device2(config-erps-inst-1)#ring level 0
Device2(config-erps-inst-1)#ring enable
Device2(config-erps-inst-1)#exit
Device2(config)#erps
Note: STP and erps ports are mutually exclusive, and port generation tree is enabled by default.
```

Step 3 Verify configuration results.

```
Device1(config)#show erps
ERPS state    : enable
Instance Id          : 1
Mel                  : 0
Work-mode            : revertive
WTR Timer            : 5 min
Guard Timer          : 500 ms
Holdoff Timer        : 0 s
Ring 1 info     :
Control vlan         : 4000
Status               : enable
protected-instance : 0
Role                 : Owner
Sub-ring             : No
Stm                  : Idle
-------------------------------------------------------------
port     portId     role      state       nodeId                BPR
-------------------------------------------------------------
```

```
port0   GE0/0/2   Owner     Blocking   00:00:00:00:00:00   0
port1   GE0/0/1   Common    Forwarding 00:00:00:00:00:00   0

Total 1 ring(s).

Device2(config)#show erps
ERPS state: enable

Instance Id : 1
Mel              : 0
Work-mode     : revertive
WTR Timer              : 5 min
Guard Timer            : 500 ms
Holdoff Timer          : 0 s
Ring 1 info     :
Control vlan           : 4000
Status                 : enable
protected-instance : 0
Role                   : Neighbour
Sub-ring               : No
Stm                    : Idle
-------------------------------------------------------------
port     portId     role       state        nodeId                BPR
-------------------------------------------------------------
port0   GE0/0/2   Neighbour      Blocking   00:00:00:00:00:00   0
port1   GE0/0/1   Common    Forwarding   00:0a:6a:00:02:bb   0

Total 1 ring(s).
```

Configuration file

Device1 configuration file

```
Device1(config)#s ru if device erps

![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
exit
interface ethernet 0/0/2
switchport link-type trunk
Exit
![STP]
interface ethernet 0/0/1
no stp
exit
interface ethernet 0/0/2
no stp
```

```
exit
![ERPS]
erps
erps instance 1
ring 1
control-vlan 4000
port0 ethernet 0/0/2 owner
port1 ethernet 0/0/1
protected-instance 0
ring enable
exit
```

Device2 configuration file

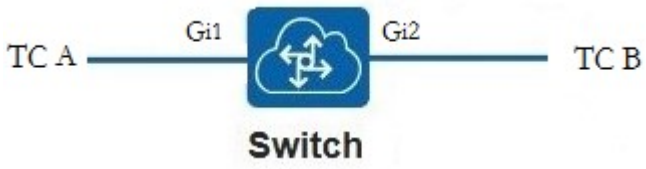
```
Device2(config)#show running-config

!LanSwitch BuildRun
enable
configure terminal
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
exit
interface ethernet 0/0/2
switchport link-type trunk
exit
![OAM]
hostname Device2
![STP]
interface ethernet 0/0/1
no stp
exit
interface ethernet 0/0/2
no stp
exit
![SNMP]
snmp-server name Device2
![ERPS]
erps
erps instance 1
ring 1
control-vlan 4000
port0 ethernet 0/0/2 neighbour
port1 ethernet 0/0/1
protected-instance 0
ring enable
exit
```

15. Example For Forwarding Control Configuration

15.1. Example for BandWidth-Control configuration

Networking requirements

Bandwidth-control mainly realizes the bandwidth limit of input or output, which limits the total rate of input and output messages from the port, as shown in the following figure. After configuring the input rate of port 1, the receiving packet rate of port B of tester will also decrease.



Configuration thinking

The configuration thinking of BandWidth-Control is as follows:
1. Configure input speed of port 1 as 1024Kbps.
2. The port A of tester sends the unknown message at line speed , the check receiving rate of port B of tester

Operating steps

Step 1 Configure bandwidth control rate of port 1 .

```
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#bandwidth ingress 1024
Set ingress bandwidth control successfully.
```

Step 2 Verify the configuration results.

view the BandWidth-Control configuration.

```
Console(config)#show bandwidth-control
port          Ingress bandwidth control Egress bandwidth control
GE0/0/1       1024 kbps                 disable
e0/0/2          disable                 disable
e0/0/3          disable                 disable
e0/0/4          disable                 disable
```

The tester A sends unknown message at line speed, tester B can only receive the packet at speed of 1024 Kbps

Configuration file

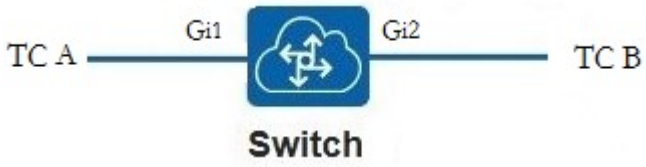
Configuration file for Switch1

```
Console(config)#show running-config device
![DEVICE]
interface ethernet 0/0/1
bandwidth ingress 1024
exit
```

15.2. Example for MAC Address Management Configuration

Networking requirements

As shown in the following figure, when the number of users is small, you can add static mac table items to the user host in the mac table of the switch to prevent mac address attacks.



Configuration thinking

The configuration thinking is as follows:
Add static mac, blackhole mac, and permanent mac; modify mac learning quantity and modify mac expression time;

Operating steps

Step1 Configure static mac addresses

```
Console(config)#mac-address-table age-time 600

Console(config)#mac-address-table max-mac-count 1000

Console(config)#mac-address-table blackhole 00:00:11:00:00:11 vlan 1
Console(config)#mac-address-table permanent 00:00:22:00:00:22 interface ethernet 0/0/1 vlan
1
Console(config)#mac-address-table static 00:00:33:00:00:22 interface ethernet 0/0/1 vlan 1
```

Step2 Verify configuration results

See the static mac configuration.

```
There is no configuration about this module.
Console(config)#show mac-address-table
```

MAC Address	VLAN ID	port	status
00:00:11:00:00:11	1	-	blackhole
00:00:22:00:00:22	1	0/0/1	permanent
00:00:33:00:00:22	1	0/0/1	static
00:0a:6a:00:02:bb	1	cpu	static

Total entries: 4

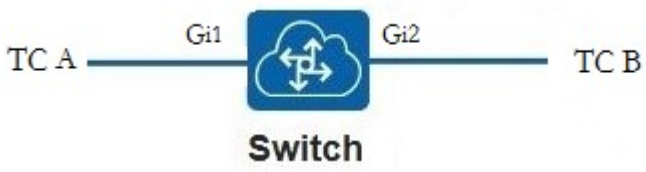
Configuration file

```
# Configuration file for Switch
Console(config)#show running-config arl

![ARL]
mac-address-table max-mac-count 1000
mac-address-table age-time 600
mac-address-table blackhole 00:00:11:00:00:11 vlan 1
mac-address-table permanent 00:00:22:00:00:22 interface ethernet 0/0/1 vlan 1
```

15.3 Example for DLF-Control Configuration

Networking requirements

The DLF-control function is mainly used to control the forwarding of unknown unicast and unknown multicast. As shown in the following figure, the switch disable unknown unicast or multicast message forwarding. The unknown unicast or unknown multicast message sent by the port A of tester will be discarded in port 1 and will not be sent to port 2.



Configuration thinking

The configuration thinking of DLF-Control is as follows:

1. Switch settings do not forward unknown unicast messages;
2. The port A of tester sends unknown unicast message to view the receiving packets of the port B.

Operation steps

Step 1 Disable unicast message forwarding of all ports.

```
Console(config)#no unknown-discard unicast vlan 1
Console(config)#interface ethernet 0/0/1
```

```
Console(config-if-ethernet-0/0/1)#unknown-discard unicast
Console(config-if-ethernet-0/0/1)#exit
```

Step2 The port A of the tester sends unknown unicast message

Step3 Verify configuration results

Test Port B do not receive a message

```
Console(config)#show unknown-discard ethernet 0/0/1
Port          Discarding Unknown Unicast      Discarding Unknown Multicast
GE0/0/1         enable                          disable
```

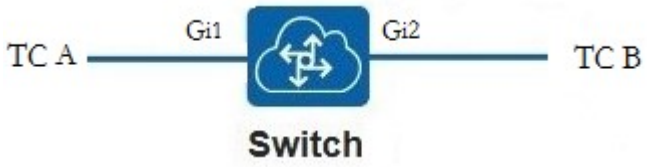
Configuration file

```
# Configuration file for Switch
Console(config)#show running-config unknown_discard
![UNKNOWN_DISCARD]
interface ethernet 0/0/1
unknown-discard unicast
exit
```

15.4 Example for flow-control Configuration

Networking requirements

As shown below, when the port A of tester and port 1 of switch enable the flow control function, if the switch becomes congested, it will send message to the tester. Notify the opposite end to temporarily stop sending messages or slow down the speed of sending messages, after receiving the message, the tester will stop sending messages to this end or slow down the speed of sending messages. Thus avoiding the occurrence of message loss and ensuring the normal operation of network services.



Configuration thinking

The configuration thinking of DHCP-Snooping is as follows:
1.The port A of the tester and the port 1 of the switch enable the flow control;
2.The output bandwidth of port 2 of switch is 10M;
3.Port A of the tester sends known unicast message to port B with linear speed.

Operating steps

Step 1 Enable flow control function of port 1.

```
Console(config)#interface range ethernet 0/0/1 to ethernet 0/0/2
Console(config-if-range)#flow-control
Setting successfully! flow-control is enable

Setting successfully! flow-control is enable
```

Step 2 Configure output bandwidth of port 2.

```
Console(config-if-range)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#bandwidth egress 10240
Config bandwidth egress successfully.

Console(config-if-ethernet-0/0/2)#exit
```

Step 3 Tester A Enables flow control and sends known unicast message with linear speed.

Step 4 Verify configuration results

Tester A receives the flow control frame from DUT and automatically adjusts the sending packet rate to 10M.

view the configuration of flow control of port.

```
Console(config)#show flow-control interface ethernet 0/0/1 ethernet 0/0/2
port       flow-control-state
GE0/0/1    enable
GE0/0/2    enable
Total entries: 2 .
```

Configuration file

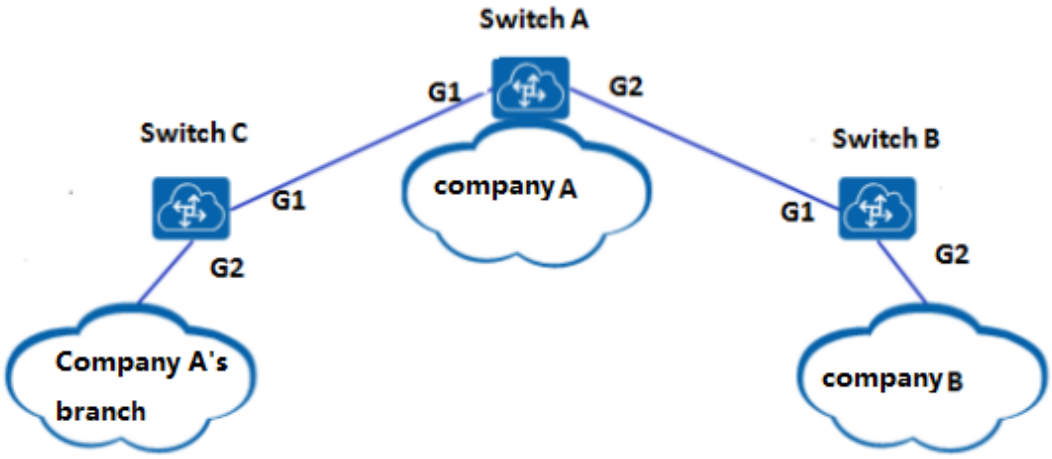
Configuration file for Switch

```
[Console(config)#show running-config device
![DEVICE]
interface ethernet 0/0/1
flow-control
exit
interface ethernet 0/0/2
flow-control
bandwidth egress 10240
exit
```

16. Example for GVRP configuration

Networking requirements

As shown in the following chart, the company A and the sub company are connected by a number of exchange equipment to meet the mutual communication between the branch and the general company. With the expansion of the company's business, the company A B company sales department and purchasing department to establish business relations, now need B purchasing department to achieve through the GVRP function (VLAN 100, VLAN 102 ~ 105 VLAN) and A company's sales department (VLAN 100, VLAN 102 ~ VLAN 105) communicate with each other.



Configuration thinking

The following ideas are used to configure the GVRP function:
1. Port 1 and Port 2 on SwitchA in vlan100,102-105, and enable GVRP;
2. Port 2 of SwitchB and SwitchC in vlan 100,102-105, and enable vlan 100, 102-105.
3. Verify that port 1 on switch B and switch C joins vlan100 102-105 through gvrp;

Operating steps

Step 1 Configuration of switch A, the configuration of switch B and Switch C is similar to that of switch A#Global enable；

SwitchA(config)# gvrp

#Create a VLAN to configure the trunk mode in the port
SwitchA(config)#vlan 100,102-105

```
SwitchA(config-if-vlan)#switchport ethernet 0/0/1 t e 0/0/2
SwitchA(config-if-vlan)#exit
SwitchA(config)#interface range ethernet 0/0/1 t e 0/0/2
SwitchA(config-if-range)#switchport link-type trunk
# Enable GVRP function of port.
SwitchA(config-if-range)#gvrp
SwitchA(config-if-range)#exit

#Release registered vlan.
SwitchA(config)#garp permit vlan 100,102-105
```

Step 2 Configure on switch B;

```
# Global enable;
SwitchB(config)# gvrp

# Create a VLAN to configure the trunk mode in the port
SwitchB(config)#vlan 100,102-105
SwitchB(config-if-vlan)#switchport ethernet 0/0/2
SwitchB(config-if-vlan)#exit

SwitchB(config)#interface range ethernet 0/0/1 t e 0/0/2
SwitchB(config-if-range)#switchport link-type trunk

#Enable port gvrp function
SwitchB(config-if-range)#gvrp
SwitchB(config-if-range)#exit

#Release registered vlan.
SwitchB(config)#garp permit vlan 100,102-105
```

Step 3 Configure switch C configuration

```
#Global enable;
SwitchC(config)# gvrp

#Create a VLAN to configure the trunk mode in the port
SwitchC(config)#vlan 100,102-105
SwitchC(config-if-vlan)#switchport ethernet 0/0/2
SwitchC(config-if-vlan)#exit

SwitchC(config)#interface range ethernet 0/0/1 t e 0/0/2
SwitchC(config-if-range)#switchport link-type trunk

# Enable port gvrp function
SwitchC(config-if-range)#gvrp
SwitchC(config-if-range)#exit

#Release registered vlan
```

SwitchC(config)#garp permit vlan 100,102-105

Step 4 Verify configuration results
View VLAN 100 of switch B and switch C;
SwitchB(config)#show vlan 100
show VLAN information
VLAN ID : 100
VLAN status : static
VLAN member : e0/0/1-e0/0/2.
Static tagged ports : e0/0/2.
Static untagged Ports :
Dynamic tagged ports : e0/0/1.

Total entries: 1 vlan.

SwitchC(config)#show vlan 100
show VLAN information
VLAN ID : 100
VLAN status : static
VLAN member : e0/0/1-e0/0/2.
Static tagged ports : e0/0/2.
Static untagged Ports :
Dynamic tagged ports : e0/0/1.

Total entries: 1 vlan.

Configuration file

Configuration file of switch A；

SwitchA(config)#show running-config vlan device garp

![VLAN]
vlan 100,102-105
exit
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
switchport trunk allowed vlan 100,102-105
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 100,102-105
exit
![GARP]
garp permit vlan 100,102-105

```
gvrp
interface ethernet 0/0/1
gvrp
exit
interface ethernet 0/0/2
gvrp
exit
```

Configuration file of switch B；

```
SwitchB(config)#show running-config vlan device garp

![VLAN]
vlan 100,102-105
exit
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 100,102-105
exit
![GARP]
garp permit vlan 100,102-105
gvrp
interface ethernet 0/0/1
gvrp
exit
interface ethernet 0/0/2
gvrp
exit
```

Configuration file of switch C；

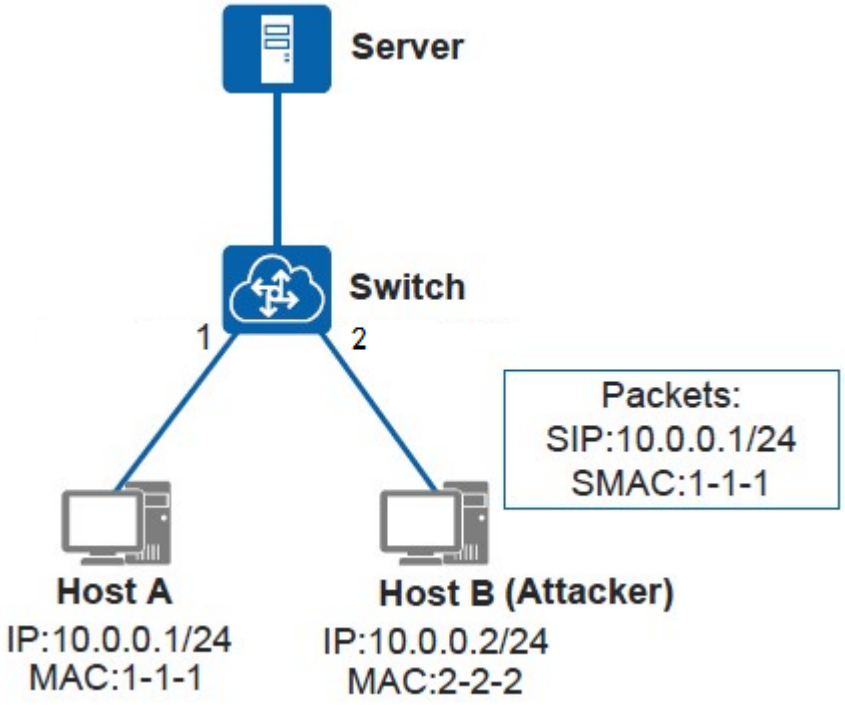
```
SwitchC(config)#show running-config vlan device garp

![VLAN]
vlan 100,102-105
exit
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 100,102-105
```

```
exit
![GARP]
garp permit vlan 100,102-105
gvrp
interface ethernet 0/0/1
gvrp
exit
interface ethernet 0/0/2
gvrp
exit
```

17 Example for IPSG configuration

Networking requirements

As shown in the following figure, HostA and HostB are connected to the 10GE1/0/1 and 10GE1/0/2 interfaces of Switch, respectively. It is required that HostB can't fake HostA's IP and MAC to cheat Server, so that the IP message of the HostA can be sent to normal.



Configuration thinking

Configure the IPSG function on switch using the following approach (assuming that the user's IP address is statically assigned):
1. Enable ip-source function on port of switch 1 and switch2
2. Configure static bind table, port1 allows 10.0.0.1 00: 01: 01: 01 communication and port2 allows 10.0.0.2 00: 03: 00: 00: 03: 03: 03 communication;

Operating steps

Step 1 Configure IP message checking function
Console(config)#interface range ethernet 0/0/1 t ethernet 0/0/2

Console(config-if-range)#ip-source
Console(config-if-range)#exit

Step 2 Configure static bind table items
Console(config)#ip-source bind 10.0.0.1 00:01:00:01:00:01 interface ethernet 0/0/1 vlan 1
Console(config)#ip-source bind 10.0.0.2 00:03:00:03:00:03 interface ethernet 0/0/2 vlan 2

Step 3 Verify configuration results
View the binding table information on the switch.
Console(config)#show ip-source bind

IP	MAC	PORT	VLAN	Active
10.0.0.2	00:03:00:03:00:03	GE0/0/2	2	YES
10.0.0.1	00:01:00:01:00:01	GE0/0/1	1	YES

Total entries: 2.

After the above configuration, the Attacker 10.0.0.2 / 24 mac 2-2-2 message will be discarded;

Configuration file

Switch configuration file
Console(config)#show running-config dhcpsnooping

```
![DHCPSNOOPING]
interface ethernet 0/0/1
ip-source ip-mac-vlan
exit
interface ethernet 0/0/2
ip-source ip-mac-vlan
exit
ip-source bind 10.0.0.2 00:03:00:03:00:03 interface ethernet 0/0/2 vlan 2
ip-source bind 10.0.0.1 00:01:00:01:00:01 interface ethernet 0/0/1 vlan 1
```

18. Example for Upgrade File configuration

18.1 Example for file operation via FTP

Networking requirements

As shown below, the remote server provides FTP Server function whose IP address is 10.2.2.50 / 24.The device acts as a FTP client, the IP address of the device is 10.2.2.56 / 24 and can reach between the server and the server.
The device needs to be upgraded by downloading system software to the device from the FTP server and backup the configuration file of current device to the FTP server.

Configuration thinking

Configure FTP accessing to other device files in the following way:
1. Upgrade the version through the ftp tool (host file and bootrom file);
2. Upgrade the backup host file through ftp tool;
3. Import the configuration file through the ftp tool;
4. Export the configuration file through ftp tool;
5. Export the host file through ftp tool;

Operating steps

Step 1 Run the FTP software on the FTP server and set up the related information of the FTP user.
Step2 Upgrade the version through the ftp tool (host file and bootrom file);
Upgrade host file
Console#load application ftp inet 10.2.2.50 host.7z test test
Upgrade bootrom file
Console#load whole-bootrom ftp inet 10.2.2.50 bootrom.bin test test

Note：After the restart, the upgraded file will be automatically used.

Step3 Upgrade the backup host file through the ftp tool；

```
    # Upgrade backup host files
Console#load secondary application ftp inet 10.2.2.50 host.7z test test
    # Configure to use the backup host file to run; (effective after restart)
Console#startup secondary application
    # Resume using the master host file to run; (effective after restart)
Console#no startup secondary application
```

Step4 Import the configuration file through the ftp tool;

```
    # Download configuration file
Console#load configuration ftp inet 10.2.2.50 configrue.txt test test
Startup config will be updated, are you sure(y/n)? [n]y
Downloading config file via FTP...
    # Use the imported configuration file (you can also load the configuration file after starting)
Console#copy startup-config running-config
```

Step5 Export the configuration file through ftp tool;

```
Console#upload configuration ftp inet 10.2.2.50 con.txt test test
```

Step6 Export the host file through ftp tool;

```
Console#upload application ftp inet 10.2.2.50 host.7z test test
```

Configuration file

Configuration file for Switch
None

18.2 Example for file operation through TFTP

Networking requirements

As shown below, the remote server provides TFTP Server function whose IP address is 10.2.2.50 / 24. The device acts as a TFTP client, the IP address of the device is 10.2.2.56 / 24 and can reach between the server and the server.
The device needs to be upgraded by downloading system software to the device from the TFTP server and backup the configuration file of current device to the TFTP server.

TFTP Server ---------- DUT

Configuration thinking

Configure TFTP accessing to other device files in the following way:
1. Upgrade the version through the tftp tool (host file and bootrom file);
2. Upgrade the backup host file through the tftp tool;

3. Import the configuration file through the tftp tool;
4. Export the configuration file through the tftp tool;
5. Export the host file through the tftp tool;

Operating Steps

Step1 Run tftp software on the tftp server and set tftp related information.

Step2 Upgrade the version through the tftp tool (host file and bootrom file);

```
    # Upgrade the host file
Console#load application tftp inet 10.2.2.50 host.7z
    # Upgrade bootrom file
Console#load whole-bootrom tftp inet 10.2.2.50 bootrom.bin
```

Note：After the restart, the upgraded file will be automatically used.

Step3 Upgrade the backup host file through the tftp tool;

```
    # Upgrade backup host files
Console#load secondary application tftp inet 10.2.2.50 host.7z
    # Configure to use the backup host file to run; (effective after restart)
Console#startup secondary application

    # Resume using the master host file to run; (effective after restart)
Console#no startup secondary application
```

Step4 Import the configuration file through the tftp tool;

```
   #Download the configuration file
Console#load configuration tftp inet 10.2.2.50 configrue.txt
Startup config will be updated, are you sure(y/n)? [n]y
Downloading config file via TFTP...

   # Use the imported configuration file (you can also load the configuration file after starting)
Console#copy startup-config running-config
```

Step5 Export the configuration file through the tftp tool;

```
Console#upload configuration tftp inet 10.2.2.50 con.txt
```

Step6 Export the host file through the tftp tool;

```
Console#upload application tftp inet 10.2.2.50 host.7z
```

Configuration file

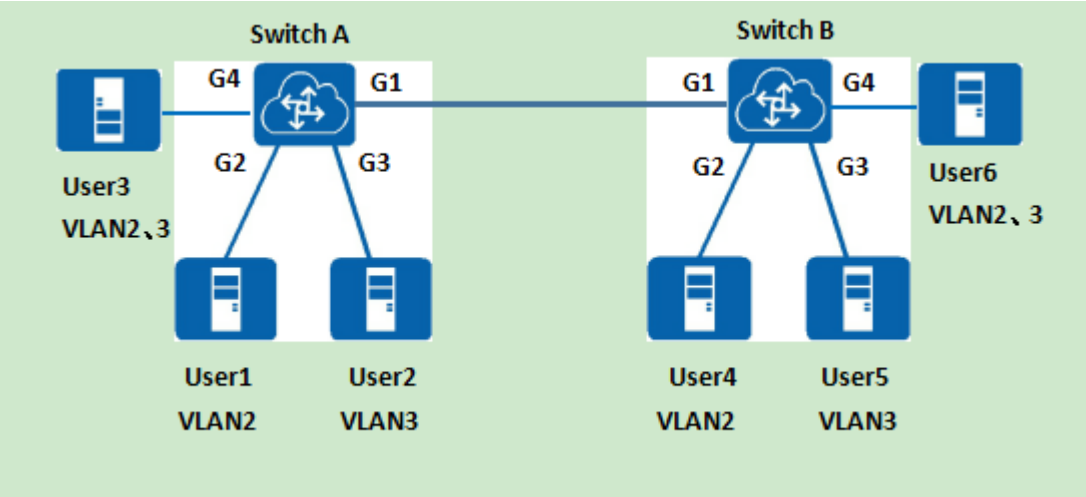
Configuration file for Switch
None

19. Example for VLAN configuration

19.1 802.1Q VLAN Configuration

Networking requirements

As the following figure shows, the switch in a data center has many user sides connected, and the same service users are connected to the network through different devices. Among them, both User 1 and User3 belong to service 1. User3 is the user of service 1-2 and both User4 and User5 belong to service 2. User6 is the user of service 1-2. They are connected to the network through Switch A and Switch B. in order to ensure the security of communication and to avoid broadcast storms, administrators hope that the users of the same service can access each other. The users of the different service can not access each other
It can divide VLAN based on interface in Switch, and the interface connected to same service users can be divided into the same VLAN, so that the users belonging to different VLAN can not directly carry out layer 2 communication. Users within the same VLAN can communicate directly with each other.



Configuration thinking

Configure VLAN as follows:
1. Create VLAN and add the interface connected user to VLAN to realize layer 2 flow isolation between different service users.
2. Configure the link type and the VLAN between Switch A and Switch B to realize the same service users communicate with each other through Switch A and Switch B.

Operating steps

Step 1 Create vlan 2 and vlan 3 in Switch A, and add the interface connected to User1 and User2 to vlan 2 and vlan 3 respectively. The interface of User3 is configured as hybird port, Add it to vlan 2-3. The configuration of

Switch B is similar to that of Switch A and will not be restated.

```
Console(config)#vlan 2-3
Console(config-if-vlan)#exit
Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#switchport pvid 2
Console(config-if-ethernet-0/0/2)#interface ethernet 0/0/3
Console(config-if-ethernet-0/0/3)#switchport pvid 3
Console(config-if-ethernet-0/0/3)#interface ethernet 0/0/4
Console(config-if-ethernet-0/0/4)#switchport hybrid untagged vlan 2-3
Console(config-if-ethernet-0/0/4)#exit
```

Step 2 Configure the interface type connected to Switch B on Switch A as trunk port, via vlan 2 / VLAN3; The configuration of Switch B is similar to that of Switch A and will not be restated.

```
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#switchport link-type trunk
Console(config-if-ethernet-0/0/1)#switchport trunk allowed vlan 2-3
Console(config-if-ethernet-0/0/1)#exit
```

Step 3 Verify configuration results

Carry out show interface gigabitethernet 1-4 in any view, the configuration of Switch B is similar to that of Switch A and will not be restated.

```
Console(config)#show interface ethernet 0/0/1

 Ethernet e0/0/1 current state: down
 shutdown: false
 Time duration of linkup is    05 hour 00 minute 36 second
 Hardware address is 00:0a:6a:00:02:bb
 SetSpeed is auto, LinkSpeed is unknown, Duplex mode is full
 Current port type: 1000BASE-T
 Priority is 0
 Flow control is disabled
 PVID is 1
 Port link-type: trunk

 Vlan          allowed : 2-3
 Input    : 0 packets, 0 bytes
              0 broadcasts, 0 multicasts, 0 unicasts
 Output : 0 packets, 0 bytes
              0 broadcasts, 0 multicasts, 0 unicasts

Console(config)#show interface ethernet 0/0/2

 Ethernet e0/0/2 current state: up
 shutdown: false
 Time duration of linkup is    05 hour 04 minute 20 second
 Hardware address is 00:0a:6a:00:02:bb
 SetSpeed is auto, LinkSpeed is 1000M, Duplex mode is full
```

```
  Current port type: 1000BASE-T
  Priority is 0
  Flow control is disabled
  PVID is 2
  Port link-type: hybrid

  Untagged    VLAN ID : 1-2
  Input    : 4 packets, 256 bytes
                0 broadcasts, 4 multicasts, 0 unicasts
  Output : 75 packets, 4800 bytes
                0 broadcasts, 75 multicasts, 0 unicasts

Console(config)#show interface ethernet 0/0/3

  Ethernet e0/0/3 current state: down
  shutdown: false
  Time duration of linkup is    05 hour 07 minute 05 second
  Hardware address is 00:0a:6a:00:02:bb
  SetSpeed is auto, LinkSpeed is unknown, Duplex mode is full
  Current port type: 1000BASE-T
  Priority is 0
  Flow control is disabled
  PVID is 3
  Port link-type: hybrid

  Untagged    VLAN ID : 1,3
  Input    : 0 packets, 0 bytes
                0 broadcasts, 0 multicasts, 0 unicasts
  Output : 0 packets, 0 bytes
                0 broadcasts, 0 multicasts, 0 unicasts

Console(config)#show interface ethernet 0/0/4

  Ethernet e0/0/4 current state: down
  shutdown: false
  Time duration of linkup is    05 hour 07 minute 21 second
  Hardware address is 00:0a:6a:00:02:bb
  SetSpeed is auto, LinkSpeed is unknown, Duplex mode is full
  Current port type: 1000BASE-T
  Priority is 0
  Flow control is disabled
  PVID is 1
  Port link-type: hybrid

  Untagged    VLAN ID : 1-3
  Input    : 0 packets, 0 bytes
                0 broadcasts, 0 multicasts, 0 unicasts
```

Output : 0 packets, 0 bytes
0 broadcasts, 0 multicasts, 0 unicasts

Configuration file

The configuration file of the Switch A, the configuration of the Switch B is similar to that of the SwitchA, will not be restated.
Console(config)#show running-config device vlan

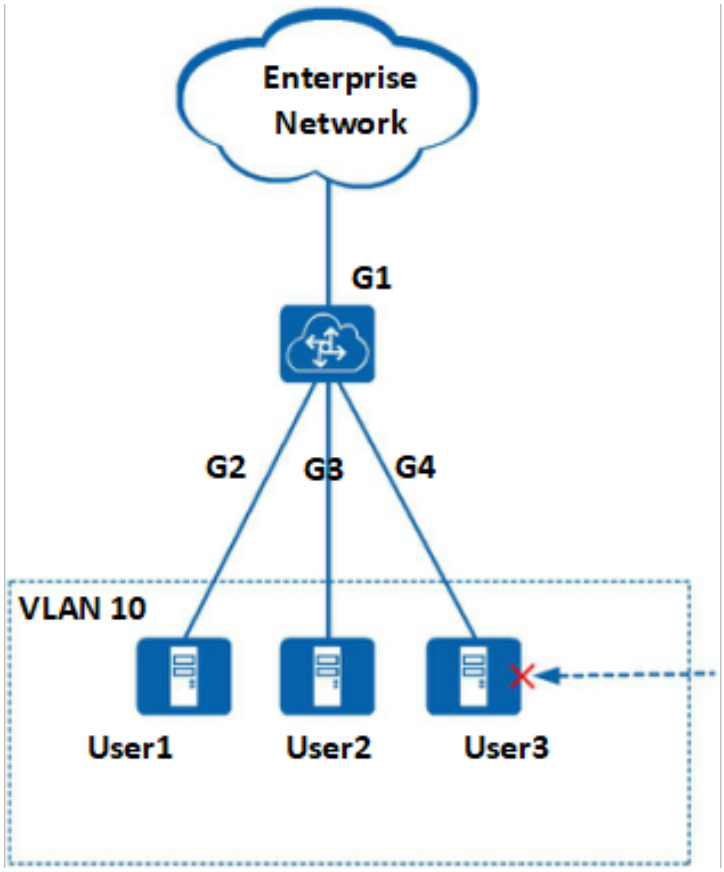
```
![VLAN]
vlan 2-3
exit
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
switchport trunk allowed vlan 2-3
exit
interface ethernet 0/0/2
switchport pvid 2
switchport hybrid untagged vlan 2
exit
interface ethernet 0/0/3
switchport pvid 3
switchport hybrid untagged vlan 3
exit
interface ethernet 0/0/4
switchport hybrid untagged vlan 2-3
exit
```

19.2 MAC-VLAN Configuration

Networking requirements

In a company's network, network managers divide users in the same department into the same VLAN. To improve information security within the department. Only users of this department are required to have access to the company's network. As shown in the following figure, the user 1, user 2 and User3 access company's more secure confidential departments. Only these three users are required to access the company's network via Switch, and other External users are not allowed to access the company's network.

To improve the information security of the confidential department, you can configure the VLAN based on MAC address to bind the MAC addresses of User1, User2 and User3 to VLAN. In order to achieve this requirement.



Configuration thinking

Configure MAC-VLAN in the following way:
1. Create VLAN and determine the VLAN to which the user belongs.
2. Each Ethernet interface is configured to join VLAN in the right way, and achieve interface allows VLAN packets to pass.
3. Configure the MAC address of User1, User2, User3 to be associated with VLAN to achieve that make sure VLAN according to source MAC address in message.

Operating steps

Step 1 Create vlan 10,
Console(config)# vlan 10

Step2 Configure port 1 as hybird pvid to 10, add port 1 to vlan 10 with the tagged port, port 2 to 4 as the hybird port, and add vlan 10 as the untagged port.
Console(config)#vlan 10
Console(config-if-vlan)#switchport ethernet 0/0/1 t e 0/0/4
Console(config-if-vlan)#interface eth 0/0/1
Console(config-if-ethernet-0/0/1)#switchport pvid 10
Console(config-if-ethernet-0/0/1)#switchport hybrid tagged vlan 10
Console(config-if-ethernet-0/0/1)#interface range eth 0/0/2 t e 0/0/4
Console(config-if-range)#switchport hybrid untagged vlan 10
Console(config-if-range)#exit

Step 3 Configure MAC address of User1-3 to be associated with VLAN10

Console(config)#vlan-mac-table 00:33:33:33:33:c1 10 1
Console(config)#vlan-mac-table 00:33:33:33:33:c2 10 1
Console(config)#vlan-mac-table 00:33:33:33:33:c3 10 1

Step 4 Verify the configuration results
Execute **show** vlan-mac-table in any view;
Console(config)#show vlan-mac-table

MAC Address	VLAN ID	priority
00:33:33:33:33:c1	10	1
00:33:33:33:33:c2	10	1
00:33:33:33:33:c3	10	1

Total entries: 3 .

It can be seen from the above information that the mac address is 00 : 33 : 33 : 33 : 33 : c1 , 00 : 33 : 33 : 33 : 33 : 33 : c2 , 00 : 33 : 33 : 33 : 33 : 33 : c3 binded with vlan 10 ;

Communication verification
Port 2 / 3 / 4 of tester send untagged message whose source mac is 00:33:33:33:33:c1 or 00:33:33:33:33:c2 or 00:33:33:33:33:c3, Port 1 can receive tagged message with vlan 10, if port 2 / 3 / 4 send message from other source mac, Port 1 can not receive message. So User1, User2 and User3 has access to the corporate network, other foreign users can not access to the corporate network .

Configuration file

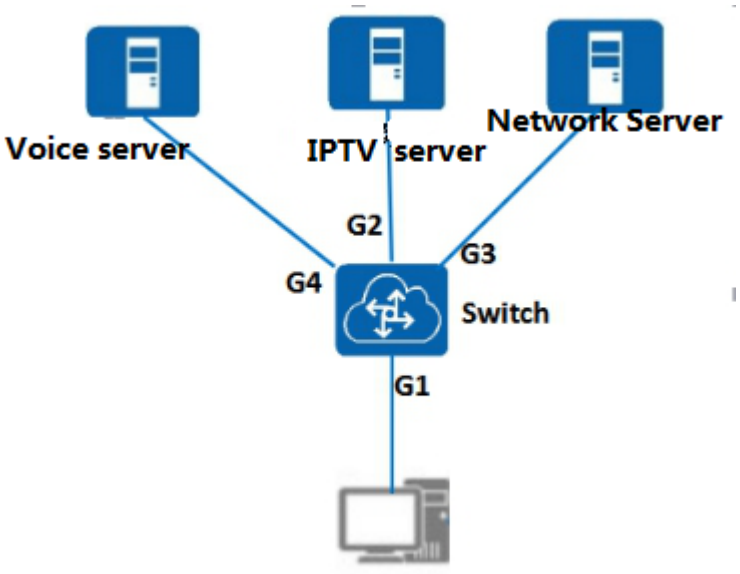
Configuration file for Switch
Console(config)#show running-config vlan device

```
![VLAN]
vlan 10
exit
vlan-mac-table 00:33:33:33:33:c1 10 1
vlan-mac-table 00:33:33:33:33:c2 10 1
vlan-mac-table 00:33:33:33:33:c3 10 1
![DEVICE]
interface ethernet 0/0/1
switchport pvid 10
switchport hybrid tagged vlan 10
exit
interface ethernet 0/0/2
switchport hybrid untagged vlan 10
exit
interface ethernet 0/0/3
switchport hybrid untagged vlan 10
exit
interface ethernet 0/0/4
switchport hybrid untagged vlan 10
exit
```

19.3 Subnet-VLAN Configuration

Networking requirements

A certain enterprise network distributes IP subnet according to service type, which requires users of different IP subnet to access upstream server with different transmission paths.
As shown below, the Switch receives the user message data, IPTV, voice and other service, the IP Address of all kind of service is different. Configure vlan based on sub net on Switch, it can divide these message to specified VLAN according to different source IP automatically after device received all kind of message and transmit to upper server.



Configuration thinking

Configure the VLAN- Subnet- as the following lines
1.Create VLAN and determine VLAN to which each service belongs to.
2. Associate subnet with VLAN, it could make sure VLAN according to Source IP Address or specified segment.
3.Configure port to join VLAN to realize subnet-based VLAN through the current interface.

Operating steps

Step 1 Create vlan 100, vlan 200, vlan 300；

```
 Console(config)#vlan 100,200,300
Console(config-if-vlan)#exit
```

Step 2 Vlan is divided according to the network segment;

```
Console(config)#vlan-subnet 192.168.1.2 255.255.255.255 100 1
Console(config)#vlan-subnet 192.168.2.2 255.255.255.255 200 1
Console(config)#vlan-subnet 192.168.3.2 255.255.255.255 300 1
```

Step 3 Configure port to be added to vlan

```
# Configure port 1 as hybird port, add port 1 as untagged port to vlan 100, vlan200 and vlan300 ;
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#switchport hybrid untagged vlan 100,200,300
Console(config-if-ethernet-0/0/1)#exit

# Configuration port 2 as trunk port, add port 2 to vlan 100, port 3 as trunk port, join vlan 200, port 4 as trunk port, join vlan 300;
Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#switchport link-type trunk
Console(config-if-ethernet-0/0/2)#switchport trunk allowed vlan 100
Console(config-if-ethernet-0/0/2)#interface eth 0/0/3
Console(config-if-ethernet-0/0/3)#switchport link-type trunk
Console(config-if-ethernet-0/0/3)#switchport trunk allowed vlan 200
Console(config-if-ethernet-0/0/3)#interface eth 0/0/4
Console(config-if-ethernet-0/0/4)#switchport link-type trunk
Console(config-if-ethernet-0/0/4)#switchport trunk allowed vlan 300
Console(config-if-ethernet-0/0/4)#exit
```

Step 4 Verify configuration results

```
# View the configuration in any view.
Console(config)#show vlan-subnet
ipAddress       netMask              VLAN ID    priority
192.168.1.2    255.255.255.255    100          1
192.168.2.2    255.255.255.255    200          1
192.168.3.2    255.255.255.255    300          1
Total entries: 3 .
```

From the above information, we can see that the network segment 192.168.1.2 / 24 / 192.168.2 / 24 / 192.168.3.2 / 24 is divided into vlan 100, Vlan 200 , Vlan300 respectively;

Communication verification
Port 1 sends untagged message whose source IP address is 192.168.1.2 or192.168.2.2 or 192.168.3.2.Port 2 can receive tagged message with vlan 100 whose source IP is 192.168.1.2, port 3 can receive tagged message with vlan 200 whose source IP is 192.168.2.2, port 4 can receive tagged message with vlan 300 whose source IP is 192.168.3.2.

Configuration file

Switch configuration file;
Console(config)#show running-config

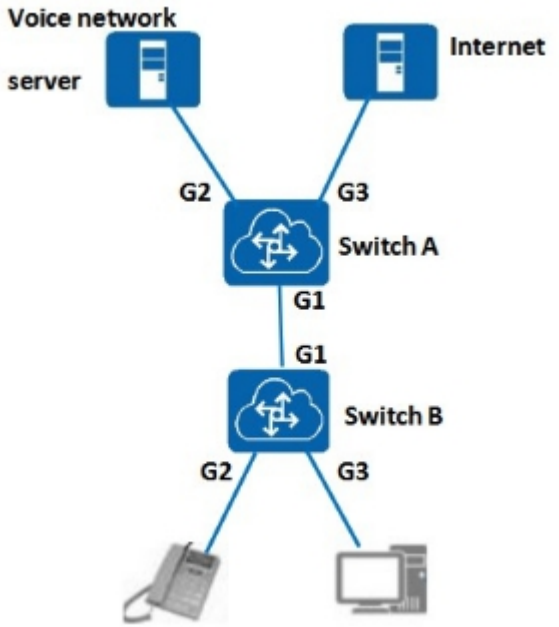
```
!LanSwitch BuildRun
enable
configure terminal
![VLAN]
vlan 100,200,300
exit
ip-subnet-vlan 192.168.1.2 255.255.255.255 100 1
ip-subnet-vlan 192.168.2.2 255.255.255.255 200 1
ip-subnet-vlan 192.168.3.2 255.255.255.255 300 1
![DEVICE]
interface ethernet 0/0/1
switchport hybrid untagged vlan 100,200,300
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 100
exit
interface ethernet 0/0/3
switchport link-type trunk
switchport trunk allowed vlan 200
exit
interface ethernet 0/0/4
switchport link-type trunk
switchport trunk allowed vlan 300
Exit
```

19.4 Protocol-VLAN configuration

Networking requirements

As shown in the figure below, a certain enterprise has a many service, such as IPTV, VoIP, Internet, etc, and the protocols used in each service are different.In order to facilitate management and reduce the workload of manual configuring VLAN, it is necessary to divide the same type of service into the same VLAN, and different types of service are divided into different vlans.

In this example, the users of VLAN 100 adapts IPv4 Protocol to communicate with remote users while the users of VLAN 200 adapts IPv6 Protocol to communicate with remote server, it could divide the different type of service into different VLAN, so that divide flow to different remote server to realize service could communicate with each other.



Configuration thinking

Configure the Protocol-VLAN along with the following lines
1. Create VLAN and make sure that Protocol-VLAN to which each service belongs
2. Associate Protocol, VLAN and port. Realize that attribute different VLAN ID to data frame according to Network Layer type which data frame receiving by Port belongs to.
3. Configure the port to join the VLAN and allow the protocol-based VLAN to pass through the current port.

Operating steps

Step 1 Create VLAN 100 and VLAN200 on Switch A. VLAN100 is configured as voice service vlan, and VLAN200 is configured as network service vlan;

```
Console(config)#vlan 100,200
Console(config-if-vlan)#exit
```

Step 2 Associate Protocol, VLAN with port on the Switch A, associate the ipv4 protocol with the vlan 100 on port 1, associate the ipv6 protocol with the vlan 200 on port 1;

```
Console(config)#vlan-protocol frametype ethernet2 800 interface ethernet 0/0/1 100
Console(config)#vlan-protocol frametype ethernet2 86dd interface ethernet 0/0/1 200
```

Step 3 Configure the port type and the allowed VLAN on the Switch A, port 1 is set as the hybird port, and add it to vlan 100 as untagged por . In vlan 200, port 2 is trunk port, join vlan 100. Port 3 is trunk port and join vlan 200;

```
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#switchport hybrid untagged vlan 100,200
Console(config-if-ethernet-0/0/1)#interface eth 0/0/2
Console(config-if-ethernet-0/0/2)#switchport link-type trunk
Console(config-if-ethernet-0/0/2)#switchport trunk allowed vlan 100
Console(config-if-ethernet-0/0/2)#interface eth 0/0/3
Console(config-if-ethernet-0/0/3)#switchport link-type trunk
Console(config-if-ethernet-0/0/3)#switchport trunk allowed vlan 200
Console(config-if-ethernet-0/0/3)#exit
```

Step 4 verify the configuration results

Perform the configuration check result in any view:

```
Console(config)#show vlan-protocol
frametype      ethertype   PORT ID   VLAN ID
Ethernet II    0800        e0/0/1    100
Ethernet II    86dd        e0/0/1    200
```

From the above information, we can see that the ipv4 protocol encapsulated in ether2 on port 1 is associated with vlan 100, and the ipv6 protocol encapsulated by ether2 is associated with vlan 200 on port 1.

Communication verification

Ipv4 protocol message encapsulated by Ether2 and ipv6 protocol message encapsulated by Ether2 are sent on port 1, and ipv4 protocol message with vlan 100 are received on port 2. The ipv6 protocol message with vlan 200 can be received in port 2;

Configuration file

Switch configuration file;

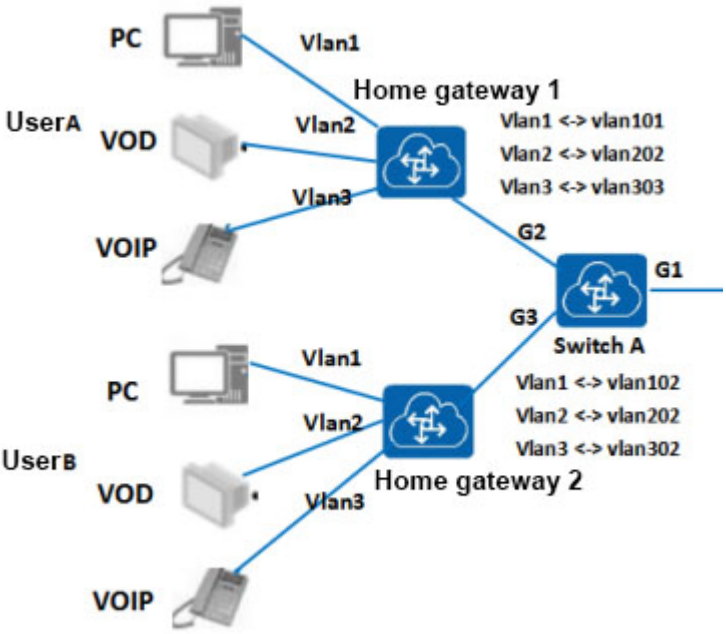
```
Console(config)#show running-config vlan device

![VLAN]
vlan 100,200
exit
vlan-protocol frametype ethernet2    800 interface ethernet 0/0/1 100
vlan-protocol frametype ethernet2 86dd interface ethernet 0/0/1 200
![DEVICE]
```

```
interface ethernet 0/0/1
switchport hybrid untagged vlan 100,200
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 100
exit
interface ethernet 0/0/3
switchport link-type trunk
switchport trunk allowed vlan 200
exit
```

20. Example for Vlan swap configuration

Networking requirements

As the follows figure shows:



Configuration thinking

The configuration roadmap is as follows:
1. Create a vlan and determine the vlan before and after the service vlan has been converted.
2. Enable the port vlan swap function and configure the corresponding vlan conversion rules.
3. Configure the type of the port and the VLAN that it passes through so that the packets corresponding to the VLAN can pass through the port.

Operating steps

Step1 On Switch A, create vlan 1, 2, 3, 101, 201, 301, 102, 202 and 302;
Console(config)#vlan 1-3
Console(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/2 ethernet 0/0/3
Console(config-if-vlan)#exit
Console(config)#vlan 101,201,301
Console(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/2
Console(config-if-vlan)#exit
Console(config)#vlan 102,202,302

```
Console(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/3
Console(config-if-vlan)#exit
```

Step2 Configure the corresponding vlan conversion rules on Switch A.

```
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#switchport link-type trunk
Console(config-if-ethernet-0/0/1)#vlan swap 101 101 1 0
Console(config-if-ethernet-0/0/1)#vlan swap 201 201 2 0
Console(config-if-ethernet-0/0/1)#vlan swap 301 301 3 0
Console(config-if-ethernet-0/0/1)#vlan swap 102 102 1 0
Console(config-if-ethernet-0/0/1)#vlan swap 202 202 2 0
Console(config-if-ethernet-0/0/1)#vlan swap 302 302 3 0
Console(config-if-ethernet-0/0/1)#exit

Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#switchport link-type trunk
Console(config-if-ethernet-0/0/2)#vlan swap 1 1 101 0
Console(config-if-ethernet-0/0/2)#vlan swap 2 2 201 0
Console(config-if-ethernet-0/0/2)#vlan swap 3 3 301 0
Console(config-if-ethernet-0/0/2)#exit

Console(config)#interface ethernet 0/0/3
Console(config-if-ethernet-0/0/3)#switchport link-type trunk
Console(config-if-ethernet-0/0/3)#vlan swap 1 1 102 0
Console(config-if-ethernet-0/0/3)#vlan swap 2 2 202 0
Console(config-if-ethernet-0/0/3)#vlan swap 3 3 302 0
Console(config-if-ethernet-0/0/3)#exit
```

Step3 Verify the configuration results

Execute show vlan swap in any view;

```
Console(config)#show vlan swap
```

port ID	original start vlan	original end vlan	swap vlan	priority
0/0/1	101	101	1	0
0/0/1	102	102	1	0
0/0/1	201	201	2	0
0/0/1	202	202	2	0
0/0/1	301	301	3	0
0/0/1	302	302	3	0
0/0/2	1	1	101	0
0/0/2	2	2	201	0
0/0/2	3	3	301	0
0/0/3	1	1	102	0
0/0/3	2	2	202	0
0/0/3	3	3	302	0

Total entries: 12 .

Configuration file

Configuration file for Switch
Console(config)#show running-config device vlan

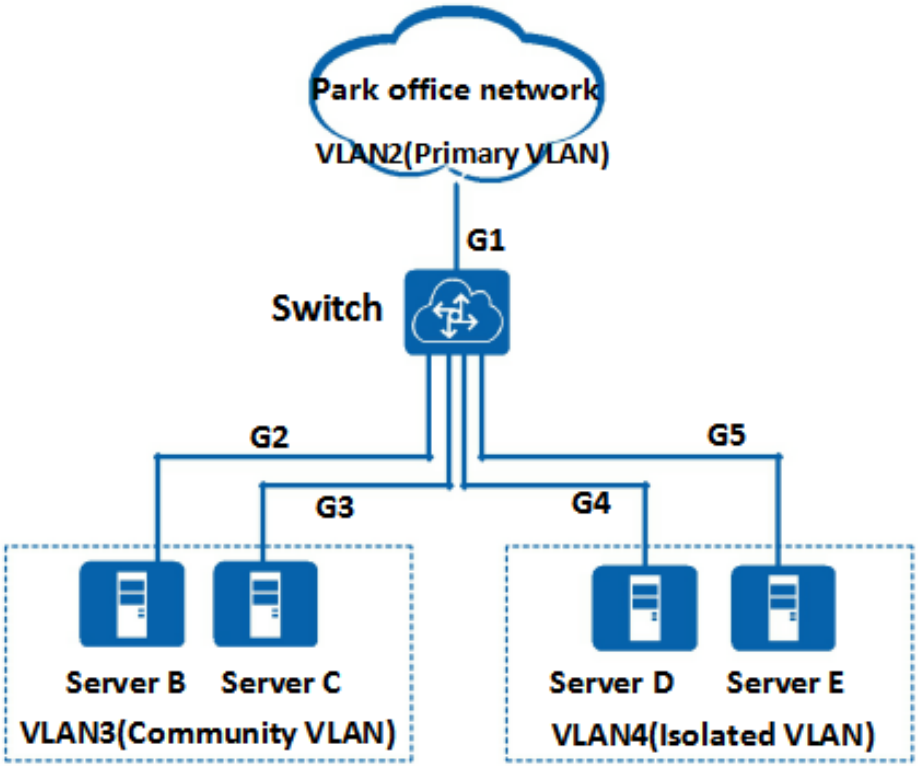
```
![VLAN]
vlan 2-3,101-102,201-202,301-302
exit
interface ethernet 0/0/1
vlan swap 101 101 1 0
vlan swap 102 102 1 0
vlan swap 201 201 2 0
vlan swap 202 202 2 0
vlan swap 301 301 3 0
vlan swap 302 302 3 0
exit
interface ethernet 0/0/2
vlan swap 1 1 101 0
vlan swap 2 2 201 0
vlan swap 3 3 301 0
exit
interface ethernet 0/0/3
vlan swap 1 1 102 0
vlan swap 2 2 202 0
vlan swap 3 3 302 0
exit
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
switchport trunk allowed vlan 2-3,101-102,201-202,301-302
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 2-3,101,201,301
exit
interface ethernet 0/0/3
switchport link-type trunk
switchport trunk allowed vlan 102,202,302
exit
```

21. Example for PVLAN configuration

Networking requirements

As shown below, a data center network with office business server ServerB, ServerC, ServerD and ServerE, all the server can access the park office network, but for data center administrators hope inside the data center of ServerB and ServerC can access each other, while ServerD and ServerE are isolated, not to be able to access each other.

In order to solve the above problems, we can deploy Private VLAN features on the switches connected to servers, connect the office network with Promiscuous port, Isolated port connection does not need to visit each other's servers, Community port connections need to visit each other's servers. This can not only realize the demand, but also save the VLAN ID, which is easy to maintain by the network manager.



Configuration thinking

The following ideas are used to configure the PVLAN function:
1. Configure primary VLAN, community VLAN, isolated VLAN, and primary VLAN associated community VLAN and isolated VLAN;
2. Configure promiscuous ports, community ports, isolated ports, and associated private VLAN;

Operating steps

Step 1 Configure VLAN roles
#Configure main VLAN
Console(config)#vlan 2
Console(config-if-vlan)#private-vlan primary
Console(config-if-vlan)#exit

#Configure isolated VLAN
Console(config)#vlan 4
Console(config-if-vlan)#private-vlan isolated
Console(config-if-vlan)#exit

#Configure group VLAN
Console(config)#vlan 3
Console(config-if-vlan)#private-vlan community
Console(config-if-vlan)#exit

Step 2 Add the associated port in VLAN2 / 4 / 3 and configure the default VLAN for the host port to correspond to the VLAN
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#switchport hybrid untagged vlan 2-4
Console(config-if-ethernet-0/0/1)#exit

Console(config)#interface range ethernet 0/0/2 to ethernet 0/0/3
Console(config-if-range)#switchport pvid 3
Console(config-if-range)#switchport hybrid untagged vlan 2-3
Console(config-if-range)#exit

Console(config)#interface range ethernet 0/0/4 ethernet 0/0/5
Console(config-if-range)#switchport pvid 4
Console(config-if-range)#switchport hybrid untagged vlan 2,4
Console(config-if-range)#exit

Step 3 configure port roles
Configure port as hybrid port and associate primary VLAN
Console(config)interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#switchport private-vlan promiscuous
Console(config-if-ethernet-0/0/1)#switchport private-vlan promiscuous 2
Console(config-if-ethernet-0/0/1)#exit

#Configure the port as a host property and associate the associated VLAN
Console(config)#interface range ethernet 0/0/2 to ethernet 0/0/3
Console(config-if-range)#switchport private-vlan host
Console(config-if-range)#switchport private-vlan host 3
Console(config-if-range)#exit

Step 4 verify the configuration results

```
Console(config)#show private-vlan interface ethernet 0/0/1 to ethernet 0/0/5
   Port            Mode          PromiscuousVlan          HostVlan
GE0/0/1       promiscuous              2                     2
GE0/0/2       host                                           3
GE0/0/3       host                                           3
GE0/0/4       --
GE0/0/5       --
```

Configuration file

Switch configuration file

```
Console(config)#show running-config vlan device
![VLAN]
vlan 2
private-vlan primary
exit
vlan 3
private-vlan community
exit
vlan 4
private-vlan isolated
exit
interface ethernet 0/0/1
switchport private-vlan promiscuous
switchport private-vlan promiscuous 2
exit
interface ethernet 0/0/2
switchport private-vlan host
switchport private-vlan host 3
exit
interface ethernet 0/0/3
switchport private-vlan host
switchport private-vlan host 3
exit
![DEVICE]
interface ethernet 0/0/1
switchport hybrid untagged vlan 2-4
exit
interface ethernet 0/0/2
switchport pvid 3
switchport hybrid untagged vlan 2-3
exit
interface ethernet 0/0/3
switchport pvid 3
switchport hybrid untagged vlan 2-3
exit
```

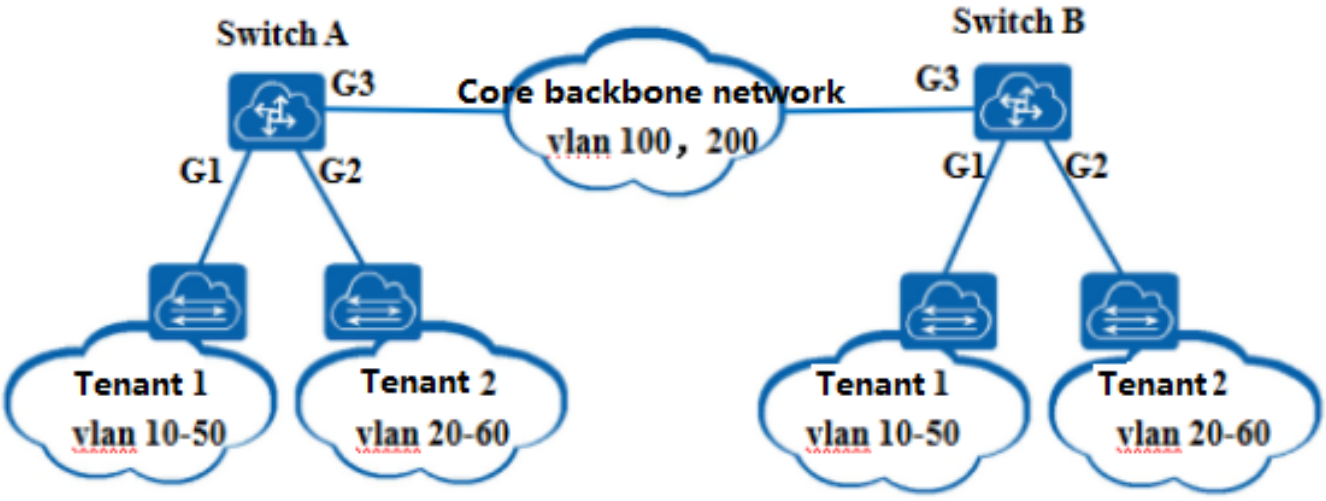
```
interface ethernet 0/0/4
switchport pvid 4
switchport hybrid untagged vlan 2,4
exit
interface ethernet 0/0/5
switchport pvid 4
switchport hybrid untagged vlan 2,4
exit
```

22. Example for QinQ configuration

22.1 Configure the static QINQ example

Networking requirements

As shown in the following figure, the tenant 1 of a data center is located in different geographical locations, and the tenant 2 is located in different geographical locations. SwitchA and SwitchB are the edge devices of the data center, which are connected through the core / backbone network. Now, we need to achieve: (1) 1 of tenants and 2 of tenants are divided into VLAN independently, neither of them affects each other. (2) the traffic between two tenants is transmitted transparently through the core / backbone network, and the same tenants are interworking with each other, and different tenants are isolated from each other.
The above requirements can be realized by configuring QinQ. The VLAN100 provided by core / backbone network enables data center tenant 1 to work interactively, and VLAN200 is used by core / backbone network to interconnect 2 tenants of data center, and different tenants are isolated from each other.



Configuration thinking

The following ideas are used to configure the QinQ function:
1. Create VLAN to confirm core backbone network;
2. Configure the type of port connected to the user and the VLAN passed, enable QINQ to function to imple different tenants to add different outer VLAN tag;
3. The type of port connected to the core network and the VLAN passed, so that the message with the upper VLAN can pass through the core backbone network;

Operating steps

Step 1 Establish VLAN 100, 200; VLAN 100 as a tenant 1 transmission network, VLAN 200 as a tenant 2 transmission network;

Console(config)#vlan 100,200
Console(config-if-vlan)#switchport ethernet 0/0/1 t ethernet 0/0/3
Console(config-if-vlan)#exit

Step 2 Enable QINQ function in global mode; Enable QINQ function in global mode, Configure the QINQ mode of port 1 to customer; Configure pvid of port2 as 200, Configure port 2's QINQ mode to customer.Switch B configuration is similar to switch A. Here no loger say.
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#switchport pvid 100
Console(config-if-ethernet-0/0/1)#exit

Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#qinq mode customer
Console(config-if-ethernet-0/0/1)#exit

Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#switchport pvid 200
Console(config-if-ethernet-0/0/2)#exit

Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#qinq mode customer
Console(config-if-ethernet-0/0/2)#exit

Step 3 Configure port 3 is hybird port. The configuration of switch B with tagged port in vlan 100200 is similar to switch A.Here no longer say.
Console(config)#interface ethernet 0/0/3
Console(config-if-ethernet-0/0/3)#switchport link-type hybrid
Console(config-if-ethernet-0/0/3)#switchport hybrid tagged vlan 100,200
Console(config-if-ethernet-0/0/3)#exit

Step 4 Verify configuration results
Execute **show dot1q-tunnel** under any views; Switch B configuration is similar to switch A and here no longer say.
Console(config)#show qinq
Current qinq status: enabled
inner-tpid: 0x8100

interface	**qinq-mode**	**outer-tpid**
e0/0/1	customer	0x8100
e0/0/2	customer	0x8100
e0/0/3	uplink	0x8100

……
From the above information we can see that the QINQ function of port 1-2 has been enabled;

Configuration file

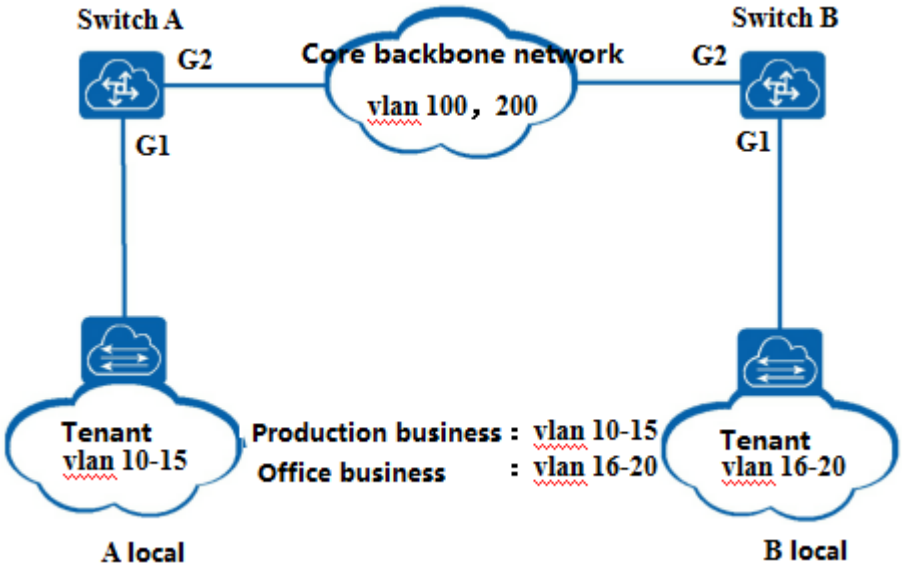
Configuration file of switch A;
Console(config)#show running-config vlan device
![VLAN]
vlan 100,200
exit
qinq
interface ethernet 0/0/1
qinq mode customer
exit
interface ethernet 0/0/2
qinq mode customer
exit
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
switchport pvid 100
switchport trunk allowed vlan 1,200
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 100,200
exit
interface ethernet 0/0/3
switchport hybrid tagged vlan 100,200
exit

The configuration file of switch B is exactly the same as the switch A configuration file.

22.2 Configure dynamic QINQ example

Networking requirements

As shown below, a data center, office tenant has a service server and server business, which VLAN10 ~ VLAN15 bearing VLAN16 ~ VLAN20 bearing production business, the business office, the tenants in different geographical locations of A and B, and the core / backbone network of SwitchA and SwitchB are connected by. In order to ensure the safety between businesses and save the core / backbone network VLAN ID, traffic in both locations is transparent through core / backbone network. The same business can be interconnected, and different businesses are isolated from each other.



Configuration thinking

The QinQ function is configured as follows:
1. Establish Vlan and identify core backbone networks.
2. Configure the type of port connected to the user and the VLAN passed, enable QINQ function to realize different tenants to add different outer VLAN tag;
3. The type of port connected to the core network and the VLAN through which the message with upper vlan can pass through the core backbone network;

Operating steps

Step 1 SwitchA establishes vlan 10-15, 100, VLAN100 as the transport network of tenant1, switchB set up vlan 16-20, 200. VLAN200 as the transmission network of tenant 2;
Console(config)#vlan 10-15,100
Console(config-if-vlan)#switchport ethernet 0/0/1 e 0/0/2
Console(config-if-vlan)#exit

Step 2 Configure SwitchA qinq function; The configuration of SwitchB is similiar to SwitchA, here no longer say.

#Enable QINQ function;
Console(config)#qinq

#Configure port 1 as hybird port;
Console(config)#interface ethernet 0/0/1

#Configure flexible QINQ rules
Console(config-if-ethernet-0/0/1)#qinq mode customer
Console(config-if-ethernet-0/0/1)#vlan insert 10 15 100
Console(config-if-ethernet-0/0/1)#exit

Step 3 Configure port2 as trunk port and join vlan100 as tagged port; Switch B configuration is similar to switch A, here no longer say.

add vlan 100 to port port ;
SwitchB ' s configuration is similar to SwitchA and will not be repeated .

Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#switchport link-type trunk
Console(config-if-ethernet-0/0/2)#switchport trunk allowed vlan 100
Console(config-if-ethernet-0/0/2)#exit

Step 4 Verify configuration results
#Switch B configuration is similar to switch A, here no longer say.
Console(config)#show qinq
Current qinq status: enabled
inner-tpid: 0x8100
interface qinq-mode outer-tpid
e0/0/1 customer 0x8100
e0/0/2 uplink 0x8100

Console(config)#show vlan insert
port ID inner start vlan inner end vlan outer vlan
0/0/1 10 15 100
0/0/1 16 20 200
Total entries: 2 .

Configuration file

Configuration file of switch A;
Console(config)#show running-config device vlan

```
![VLAN]
vlan 10-15,100
exit
qinq
interface ethernet 0/0/1
qinq mode customer
vlan-insert 10 15 100
exit
![DEVICE]
interface ethernet 0/0/1
switchport hybrid untagged vlan 10-15,100
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 10-15,100
Exit
```

The configuration file of switch B is completely similar to that of switch A.
Console(config)#show running-config device vlan

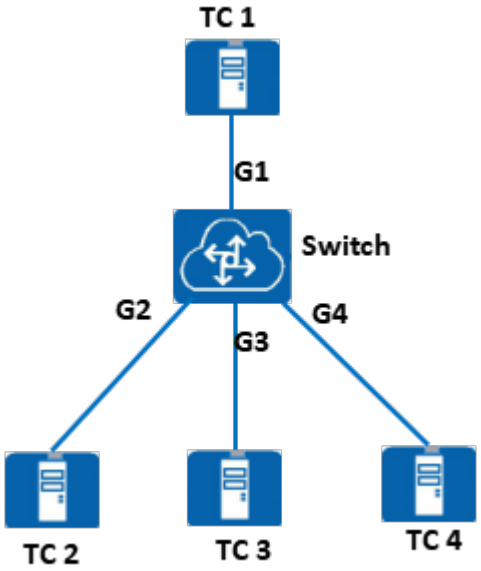
```
![VLAN]
vlan 16-20,200
exit
qinq
interface ethernet 0/0/1
qinq mode customer
vlan-insert 16 20 200
exit
![DEVICE]
interface ethernet 0/0/1
switchport hybrid untagged vlan 16-20,200
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 16-20,200
exit
```

23. Example for Port configuration

23.1 Port rate and duplex mode configuration

Networking requirements

Configure the port rate and duplex of the switch as shown in the following figure.



Configuration thinking

Configure the port rate and duplex mode as follows:

1. Configure rate of Port 1-4 of Switch as auto and duplex mode of rate of Port 1-4 of Switch as auto ;
2. The rate of port configuration is forced to 1000 Mbps, 100 Mbps, 10 Mbps;
3. Configure duplex mode of port to force it as full, half;

Operating steps

Step 1 The port 1-4 of Switch is configured at the rate of auto and duplex mode is auto (rate and duplex mode default is auto)

```
Console(config)#interface range ethernet 0/0/1 to ethernet 0/0/4
Console(config-if-range)#speed auto
Console(config-if-range)#exit
Console(config)#show interface brief ethernet 0/0/1 t e 0/0/4
Interface Link Shutdn Speed          Primary-IP        Description
GE0/0/1      up     false   auto-f1000   --
GE0/0/2      down   false   auto         --
```

GE0/0/3 down false auto --
GE0/0/4 down false auto --
Total entries: 4 .
From the above information, port 2 automatically negotiated the rate as 1000 Mbps;

Step 2 At port 2,3,4, the setting rates is 1000Mbps, 100Mbps, and 10Mbps respectively;
Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#speed 1000
Console(config-if-ethernet-0/0/2)#interface ethernet 0/0/3
Console(config-if-ethernet-0/0/3)#speed 100
Console(config-if-ethernet-0/0/3)#interface ethernet 0/0/4
Console(config-if-ethernet-0/0/4)#speed 10
Console(config)#show interface brief ethernet 0/0/1 t e 0/0/4
Interface Link Shutdn Speed Primary-IP Description
GE0/0/1 up false auto-f1000 --
GE0/0/2 down false f1000 --
GE0/0/3 down false 100a --
GE0/0/4 down false 1000a --
Total entries: 4 .

Step 3 Configure port 1-2 as full duplex mode and reconfigures port 3-4 as half-duplex mode;
Console(config)#interface range ethernet 0/0/1 t e 0/0/2
Console(config-if-range)#duplex full
Console(config-if-range)#interface range ethernet 0/0/3 t e 0/0/4
Console(config-if-range)#duplex half

Configuration file

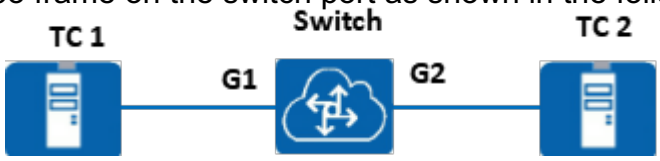
Switch configuration file;
![DEVICE]
interface ethernet 0/0/1
speed 1000
duplex full
exit
interface ethernet 0/0/2
speed 1000
duplex full
exit
interface ethernet 0/0/3
speed 100
duplex half
exit

interface ethernet 0/0/4
speed 1000
duplex half
exit

20.2 Example for Jumbo frame Configuration

Networking requirements

Set the Jumbo frame on the switch port as shown in the following figure



Configuration thinking

Configure the port rate and duplex mode as follows:
1. Set the jumbo frame size of the Switch;
2. verification results

Operating steps

Step 1 Set the switch's jumbo frame size to 3000;
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#mtu 3000

Step 2 verification results
When port 1 sends message of 4000 bytes, the message will not be forwarded; when port 1 sends message of 2999 bytes, the message can be forwarded.
Console(config-if-ethernet-0/0/1)#show mtu interface ethernet 0/0/1
port mtu size
GE0/0/1 3000 bytes

Total entries: 1.

Configuration file

Switch configuration file;
Console(config)#show running-config device

![DEVICE]

interface ethernet 0/0/1
mtu 3000
exit

20.3 Example for Configure the port vlan mode

Networking requirement

Note

Configuration thinking

Configure the port rate and duplex mode as follows:
1. Set Switch 1 port to access mode.
2. Set the Switch 2 port to hybrid mode.
3. Set the Switch 3 port to trunk mode.

Operating steps

Step1 Set Switch 1 port to access mode;
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#switchport link-type access

Step2 Set the Switch 2 port to hybrid mode;（default configuration）
Console(config-if-ethernet-0/0/1)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#switchport link-type hybrid

Step3 Set the Switch 3 port to trunk mode;
Console(config-if-ethernet-0/0/2)#interface ethernet 0/0/3
Console(config-if-ethernet-0/0/3)#switchport link-type trunk

Step4 verify the results

Configuration file

Configuration file of Switch A:
Console(config-if-ethernet-0/0/3)#show running-config device

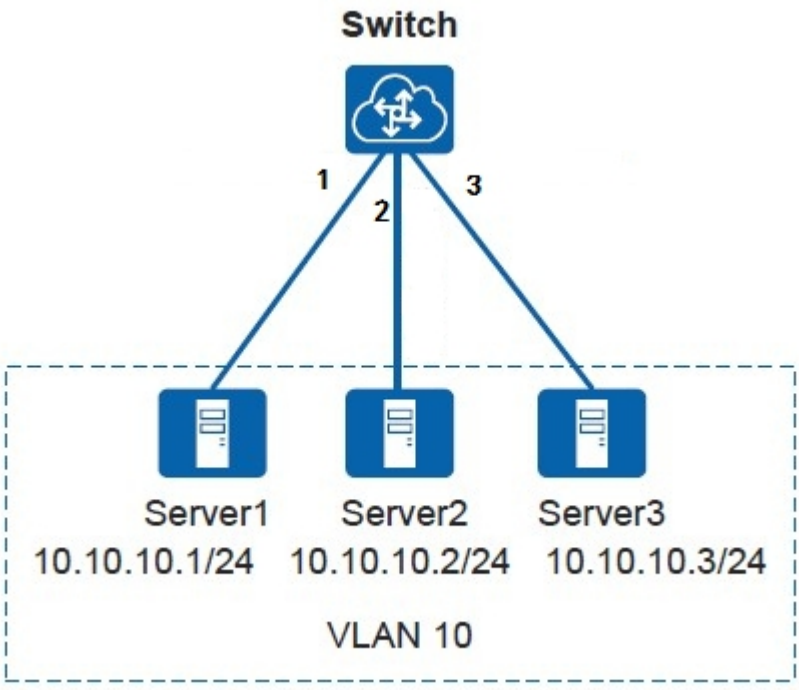
![DEVICE]
interface ethernet 0/0/1
switchport link-type access
exit

```
interface ethernet 0/0/2
speed 1000
exit
interface ethernet 0/0/3
switchport link-type trunk
exit
```

21. Example for Port isolation configuration

Networking requirements

As shown in the figure below, Server1, Server2 and Server3 belong to VLAN10, and users hope that they cannot access each other in VLAN10 between Server1 and Server2, and Server1 and Server3 can access each other, and Server2 and Server3 can access each other.



Configuration thinking

Configure port isolation as follows:
1.Configure the interface to join VLAN.
2.The device's default port isolation is layer 2. Only the interface is isolated each other, and the isolation of data of layer 2 between the interfaces within the isolated group can be isolated.

Operating steps

Step 1 Create VLAN10 on the Switch and add the interfaces that connect to the user to VLAN10 respectively.

```
Console(config)#vlan 10
Console(config-if-vlan)#interface range ethernet 0/0/1 t e 0/0/3
Console(config-if-range)#switchport pvid 10
Console(config-if-range)#exit
```

Step 2 Configure port isolation function.
Configure port 1 and port 2 to isolate each other.
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#no isolate-port uplink ethernet 0/0/2
Config successfully.

Console(config-if-ethernet-0/0/1)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#no isolate-port uplink ethernet 0/0/1
Config successfully.

Console(config-if-ethernet-0/0/2)#exit

Step 3 Verify configuration results
Server1 can not ping Server2 successfully.
Server1 can ping Server3 successfully.
Server2 can ping Server3 successfully.

Console(config)#show isolate-port
isolation port : uplink port
GE0/0/1 : GE0/0/1,GE0/0/3-10GE0/1/2
GE0/0/2 : GE0/0/2-10GE0/1/2

Configuration file

Configuration file for Switch
Console(config)#show running-config

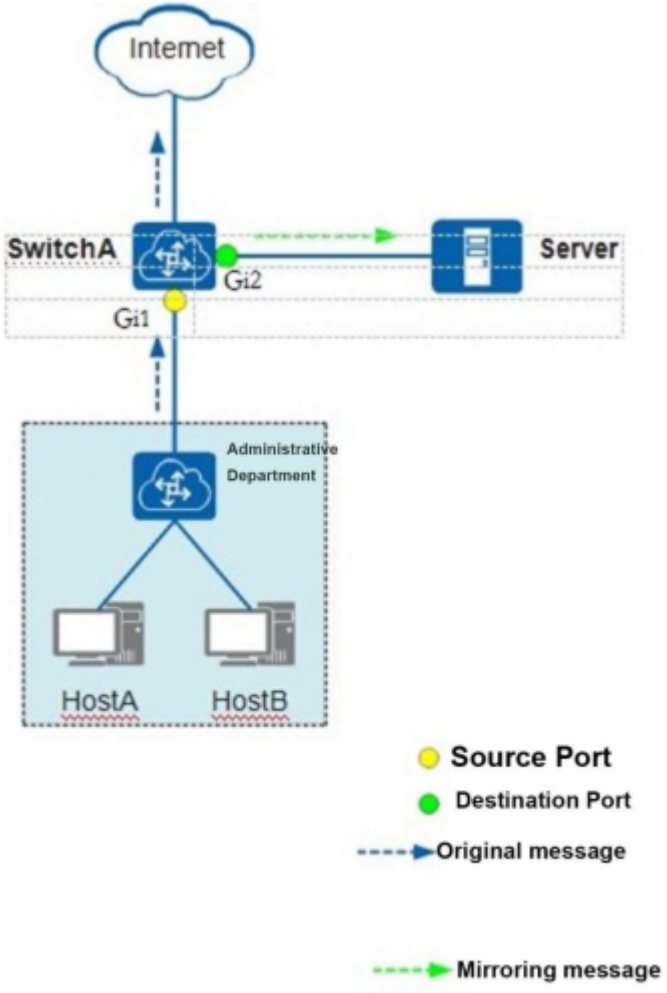
!LanSwitch BuildRun
enable
configure terminal
![VLAN]
vlan 10
exit
![DEVICE]
interface ethernet 0/0/1
switchport pvid 10
switchport hybrid untagged vlan 10
exit
interface ethernet 0/0/2
switchport pvid 10
switchport hybrid untagged vlan 10

```
exit
interface ethernet 0/0/3
switchport pvid 10
switchport hybrid untagged vlan 10
exit
![ISOLATE-PORT]
interface ethernet 0/0/1
no isolate-port uplink all
isolate-port uplink ethernet 0/0/1 ethernet 0/0/3 to ethernet 0/1/2
exit
interface ethernet 0/0/2
no isolate-port uplink all
isolate-port uplink ethernet 0/0/2 to ethernet 0/1/2
exit
```

22. Example for Port mirroring configuration

Networking requirements

As shown in the figure below, the administrative department of a company communicates with an external Internet via Switch A. Between Monitoring equipment Server and Switch A is direct connection. Users want to monitor the flow of access to Internet for administrative department through monitoring equipment Server.



Configuration thinking

The configuration of the local port mirroring is as follows:

1.Configure the interface Gi2 of Switch A as the local source port and direct connected monitor device Server can receive the mirror message;

2.The interface Gi1 of Switch A is configured as destination port to monitor the message of interface.

Operating steps

Step 1 Configure the mirror source port.

Console(config)#mirror source ethernet 0/0/1 ingress

Console(config)#

Step 1 Configure the mirror destination port.

Console(config)#mirror monitor ethernet 0/0/2

Console(config)#

Step 3 Verify configuration results.

view the configuration of the mirrored group.

Console(config)#show mirror

Information about mirror port(s)

The monitor port : GE0/0/2

The mirrored egress ports :

The mirrored ingress ports : GE0/0/1.

Configuration file

Configuration file for Switch A

Console(config)#show running-config mirror

![MIRROR]

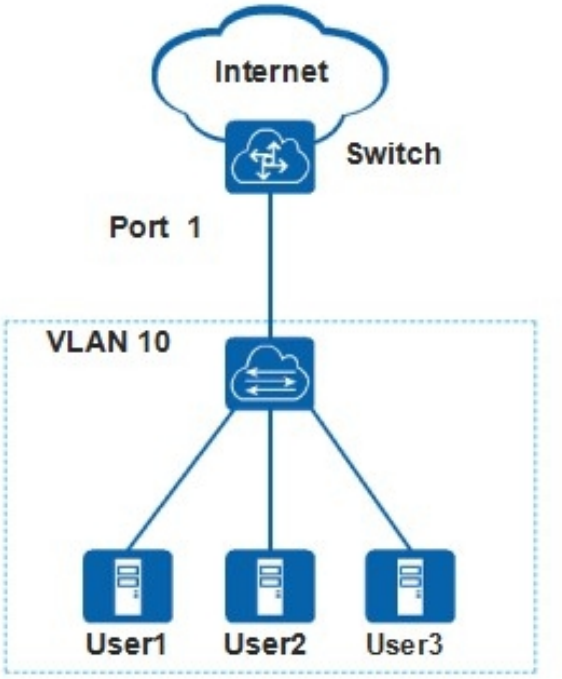
mirror monitor ethernet 0/0/2

mirror source ethernet 0/0/1 ingress

23. Example for Port security configuration

Networking requirements

As shown in the figure below, the company in order to improve the information security, enable port security function of port of switch connected to User-side and set the maximum number of interface to learn the MAC address for the total number of trusted device, so that Foreign personnel use their mobile terminal can not access the network of the company.



Configuration thinking

Configure port security as follows

1. Configure VLAN to realize layer 2 forwarding function.
2. Configure port security function to achieve the learning MAC address table items are not aging.

Operating steps

Step 1 Create VLAN and configure the link type of the interface

```
Console(config)#vlan 10
Console(config-if-vlan)#switchport ethernet 0/0/1
Console(config-if-vlan)#exit
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#switchport link-type trunk
Console(config-if-ethernet-0/0/1)#exit
```

Step 2 Configure port security features
Enable port security function
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#port-security enable

Configure the protection action of the port security function
Console(config-if-ethernet-0/0/1)#port-security violation protect

Configure interface MAC address learning limit number
Console(config-if-ethernet-0/0/1)#port-security maximum 4

Enable interface Sticky MAC function
Console(config-if-ethernet-0/0/1)#port-security permit mac-address sticky
Remarks: Sticky MAC achieve that paste the learning dynamic mac to static, it needs four devices to learn the dynamic address before setting up this command.
For other interfaces that require port security, repeat the above configuration.

Step 3 Verify configuration results
Console(config)#show port-security interface ethernet 0/0/1
tips: ViMode(violation mode) AT(AgingTime) AS(AgingStatic) ST(shutdown)

Port	Status	MaxNum	UserNum	ViMode	AT(min)	AS	Sticky	ST
GE0/0/1	enable	4	0	protect	3	disable	enable	FALSE

Total entries: 1

Configuration files

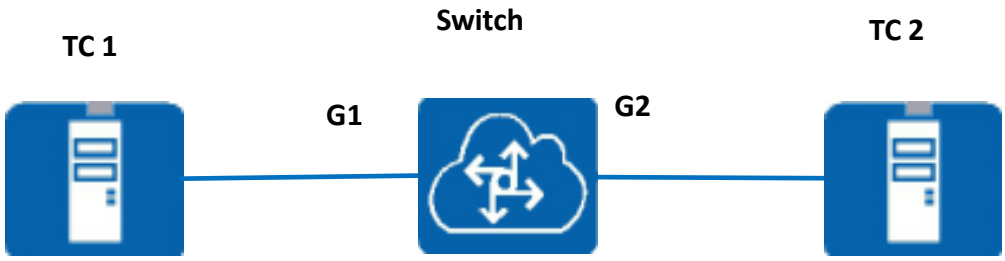
Configuration file for Switch
Console(config)#show running-config interface ethernet 0/0/1

Building configuration...
![ethernet 0/0/1]
switchport link-type trunk
switchport trunk allowed vlan 10
port-security enable
port-security maximum 4
port-security permit mac-address sticky
end

24. Example for Port statistics configuration

Networking requirements

Statistics of switch port flow as shown in the following figure.



Configuration thinking

The following thinking are used to the port flow statistics:
1. Clear flow statistics of all ports of the switch;
2. View port 1 statistics.
3. Check the number of CPU packets on port 1;
4. Modify the port real-time rate statistics time;
5. View real-time packet statistics.

Operating steps

Step1 Clear flow statistics of all ports of the switch;
Console(config)#clear interface ethernet 0/0/1

Step2 check port flow statistics;
Console(config)#show statistics interface ethernet 0/0/1

Port number : GE0/0/1
last 5 minutes input rate 0 bits/sec, 0 packets/sec
last 5 minutes output rate 24 bits/sec, 0 packets/sec
64 byte packets:0
65-127 byte packets:0
128-255 byte packets:0
256-511 byte packets:0
512-1023 byte packets:0
1024-1518 byte packets:0
Input(total): 0 packets, 0 bytes , 0 discarded packets

Input(normal): 0 unicasts, 0 multicasts, 0 broadcasts
Input: 0 errors, 0 FCS error, 0 symbol error
0 false carrier, 0 runts, 0 giants
Output(total): 0 packets output, 0 bytes, 0 discarded packets
Output(normal): 0 unicasts, 0 multicasts, 0 broadcasts
Output: 0 errors, 0 deferred, 0 collisions
0 late collisions
Total entries: 1.

Step3 Check the number of CPU packets on port 1;
Console(config)#show cpu-statistics ethernet 0/0/1
Show packets sent to cpu statistic information

port	64Byte	128Byte	256Byte	512Byte	1024Byte	2048Byte
GE0/0/1	0	0	0	0	0	0

Step4 Modify the port real-time rate statistics
Console(config)#port-rate-statistics interval 2
Port rate statistics interval has been changed, and will restart calculating port average rate!

Step5 View real-time packet statistics
Console(config)#show statistics dynamic interface

Port Statistics Wed Jan 1 01:46:04 2014

port	link Status	Tx Pkt Count	Tx Byte Count	Rx Pkt Count	Rx Byte Count	Rx Bcast	Rx Mcast
e0/0/1	down	0	0	0	0	0	0
e0/0/2	up	0	0	109	6976	0	109
e0/0/3	down	0	0	0	0	0	0
e0/0/4	down	0	0	0	0	0	0
e0/0/5	down	0	0	0	0	0	0
e0/0/6	down	0	0	0	0	0	0
e0/0/7	down	0	0	0	0	0	0
e0/0/8	down	0	0	0	0	0	0
e0/0/9	down	0	0	0	0	0	0
e0/0/10	down	0	0	0	0	0	0
e0/0/11	down	0	0	0	0	0	0
e0/0/12	down	0	0	0	0	0	0
e0/0/13	down	0	0	0	0	0	0

e0/0/14 down 0 0 0 0 0 0
e0/0/15 down 0 0 0 0 0 0
e0/0/16 down 0 0 0 0 0 0
e0/0/17 down 0 0 0 0 0 0
==========0->Clear Counters U->page up D->page down CR->exit==========

Notes:If you see a E number, you can use the command "line width" to get more information.

```
Switch(config)#show statistics dynamic interface

Port Statistics        Wed Jan 1 01:46:04 2014
port  link   Tx Pkt       Tx Byte       Rx Pkt       Rx Byte       Rx          Rx
      Status Count        Count         Count        Count         Bcast       Mcast
=============================================================================================
e0/0/1  down 0            0             0            0             0           0
e0/0/2  up   0            0             109          6976          0           109
e0/0/3  down 0            0             0            0             0           0
e0/0/4  down 0            0             0            0             0           0
e0/0/5  down 0            0             0            0             0           0
e0/0/6  down 0            0             0            0             0           0
e0/0/7  down 0            0             0            0             0           0
e0/0/8  down 0            0             0            0             0           0
e0/0/9  down 0            0             0            0             0           0
e0/0/10 down 0            0             0            0             0           0
e0/0/11 down 0            0             0            0             0           0
e0/0/12 down 0            0             0            0             0           0
e0/0/13 down 0            0             0            0             0           0
e0/0/14 down 0            0             0            0             0           0
e0/0/15 down 0            0             0            0             0           0
e0/0/16 down 0            0             0            0             0           0
e0/0/17 down 0            0             0            0             0           0
==========0->Clear Counters U->page up D->page down CR->exit==========

Notes:If you see a E number, you can use the command "line width" to get more information.
```

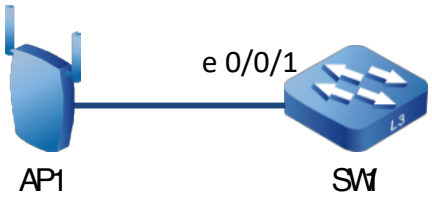
Configuration file

Configuration file for Switch;
None

25. Example for POE configuration

Networking requirements

As shown in the following figure, the switch is used as a network access layer device in the current network environment. The IP phones placed under the equipment are placed outside, AP is located on the external wall of the office, and the location is remote, so it is not convenient to access the power. Users want to directly supply the power through the switchboard, so as to save the cost of equipment deployment.



Configuration thinking

Switch devices that support Poe function are required and are not need to be configured normally. For high power AP cases, the following ideas are used to configure the basic Poe function

1. Configure global power limits
2. Configure POE port power constraints, configure power supply priority

Operating steps

Step 1 Configure global power limit, POE Port Configuration Power Limit, Configure power priority.

```
Console(config)#poe max-power 300
Console(config)#interface et 0/0/1
Console(config-if-ethernet-0/0/1)#poe max-power 32
Console(config-if-ethernet-0/0/1)#poe priority high
```

Step 1 Verification result

```
Console(config)#show poe interface ethernet 0/0/1
  GE0/0/1: enable
  standard is ieee802.3at,          priority is high,          class is 3
  power limit is 32W,      power consumption is 1W,      voltage is 55.9V
status: Port is on - Valid resistor detected
```

```
Console(config)#show poe
  power supply          : internal power supply
  power limit           : 300W
  power consumption : 1W
```

Configuration file

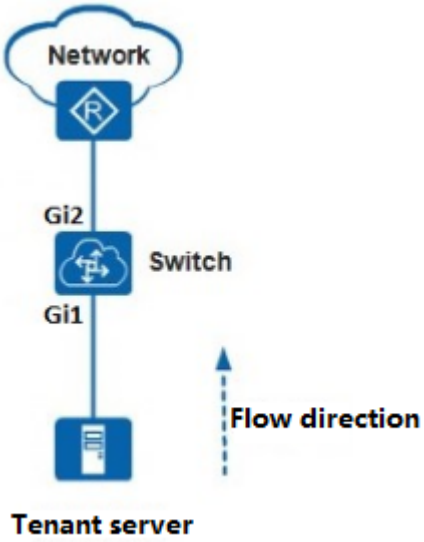
```
#SW1 configuration file;
Console(config)#show running-config poe

![POE]
poe max-power 300
interface ethernet 0/0/1
poe max-power 32
poe priority high
exit
```

26. Example for QACL configuration

26.1 Configure flow speed limit example

Networking requirements

As shown in the following figure, the tenant server sends messages over the Switch and interacts with the external network of the data center via the export router. The user asks the tenant server to send a message with a bandwidth of no more than 100Mbit/s.



Configuration thinking

Configure the flow speed limit along the following lines:

5. Configure a standard ACL rule marked by numbers;
6. Limit the speed of ACL flow;

Operating steps

Step 1 Configure standard acl

```
Console(config)#access-list ip-acl 1
Console(config-ip-nacl-1)#permit 192.168.1.100/32
```

Step 2 Limit flow rate

```
Console(config)#rate-limit input ip-acl 1 102400
```

Step 3 verify the configuration results

Use the command to view the acl configuration.
Console(config)#show access-list config 1
The step of ACL subitem number: 1
IP Access List 1, match-order is config, 1 rule:
0 : permit 192.168.1.100/32

Check the flow limit configuration.
Console(config)#show qos-interface rate-limit
rate-limit
Input:
Matches: access-list 1 subitem 0 running
Target-rate: 102400 Kbps
Exceed action: drop

Configuration file

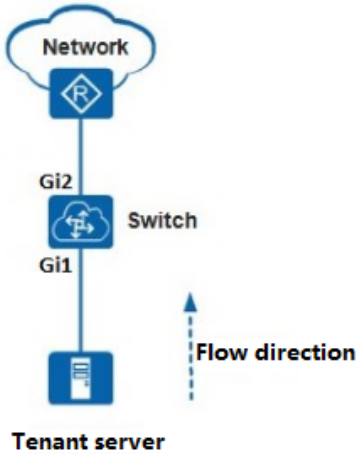
Switch configuration file
Console(config)#show running-config qacl

![QACL]
access-list ip-acl 1
0 permit 192.168.1.100/32
exit
rate-limit input ip-acl 1 102400 yellow drop

26.2 Configure the copy-to-cpu Example

Networking requirements

As shown in the following figure, the tenant server sends messages over the Switch and interacts with the external network of the data center via the export router. Users require tenant traffic as copy-to-cpu.



Configuration thinking

The following ideas are used to configure the flow speed limit:

1.Configure a standard ACL rule marked by numbers;

2.The application of cpu on ACL;

Operating steps

Step 1 Configure standard acl

```
Console(config)#access-list ip-acl 1
Console(config-ip-nacl-1)#permit 192.168.1.100/32
```

Step 2 CPU on the configuration stream

```
Console(config)#traffic-copy-to-cpu ip-acl 1
```

Step 3 Verify the configuration results

Use the command to view the acl configuration.

```
Console(config)#show access-list config 1
The step of ACL subitem number: 1

  IP Access List 1, match-order is config, 1 rule:
    0 : permit 192.168.1.100/32
```

View the copy-to-cpu configuration.

```
Console(config)#show qos-info traffic-copy-to-cpu
traffic-copy-to-cpu:
  Matches: access-list 1 subitem 0 running
```

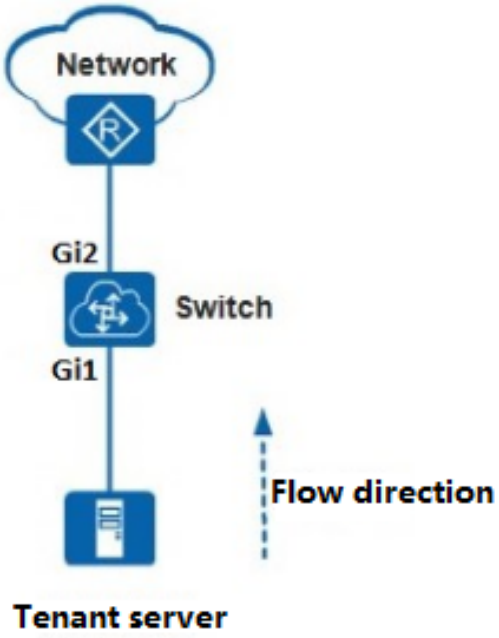
Configuration file

```
  # Switch configuration file
Console(config)#show running-config qacl

![QACL]
access-list ip-acl 1
0 permit 192.168.1.100/32
exit
traffic-copy-to-cpu ip-acl 1
```

26.3 Configure the priority example of the modification stream

Networking requirements

As shown in the following figure, the tenant server sends messages over the Switch and interacts with the external network of the data center via the export router. The user asks the tenant server to send the message the priority processing.



Configuration thinking

Configure the flow speed limit along the following lines:

1. Configure a standard ACL rule marked by numbers;
2. Increase priority for ACL flow;

Operating steps

Step 1 Configure standard acl

```
Console(config)#access-list ip-acl 1
Console(config-ip-nacl-1)#permit 192.168.1.100/32
```

Step 2 Modify the priority of the flow

```
Console(config)#traffic-priority ip-acl 1 cos 7
```

Step 3 Verify the configuration results

Use the command to view the acl configuration.

```
Console(config)#show access-list config 1
```

The step of ACL subitem number: 1
IP Access List 1, match-order is config, 1 rule:
0 : permit 192.168.1.100/32
View the modified stream priority configuration .
Console(config)#show qos-info traffic-priority
traffic-priority:
Matches: access-list 1 subitem 0 running
Priority action: cos network-management

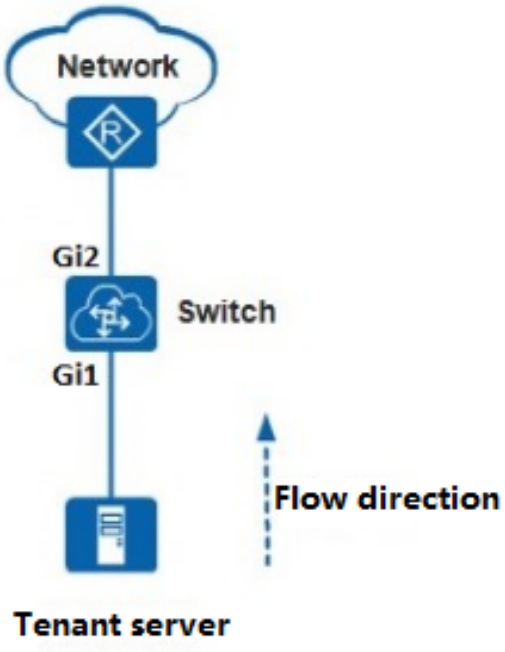
Configuration file

Switch configuration file
Console(config)#show running-config qacl
![QACL]
access-list ip-acl 1
0 permit 192.168.1.100/32
exit
traffic-priority ip-acl 1 cos network-management

26.4 Configure stream redirection example

Networking requirements

As shown in the following figure, the tenant server sends messages via switch and communicates with the external network of the data center via an outlet router. The user requires the tenant server to forward the message from the G3 port.



Configuration thinking

The following ideas are used to configure the flow speed limit:

1.Configure a standard ACL rule marked by numbers;

2.Redirect ACL flow;

Operating steps

Step 1 Configure standard acl

```
Console(config)#access-list ip-acl 1
Console(config-ip-nacl-1)#permit 192.168.1.100/32
```

Step 2 Configure stream redirected to 0 / 0 / 3 port

```
Console(config)#traffic-redirect ip-acl 1 interface ethernet 0/0/3
```

Step 3 Verify the configuration results

```
# Use the command to view the acl configuration.
Console(config)#show access-list config 1
The step of ACL subitem number: 1

 IP Access List 1, match-order is config, 1 rule:
  0 : permit 192.168.1.100/32
#  View the flow redirection configuration.
Console(config)#show qos-info traffic-redirect
traffic-redirect:
   Matches: access-list 1 subitem 0 running
      Redirected to: interface e0/0/3
```

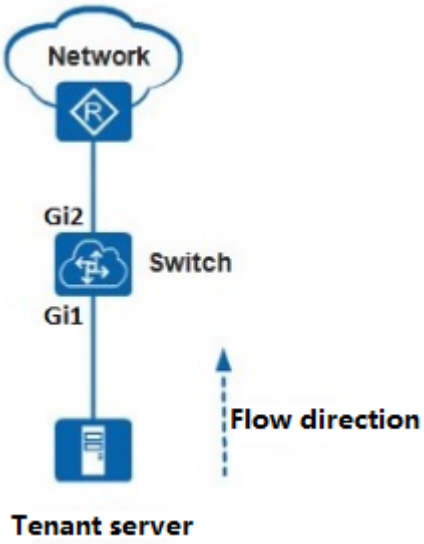
Configuration file

```
  #  Switch configuration file
Console(config)#show running-config qacl

![QACL]
access-list ip-acl 1
0 permit 192.168.1.100/32
exit
traffic-redirect ip-acl 1 interface ethernet 0/0/3
```

26.5 Configure example of specified flow statistics

Networking requirements

As shown in the following figure, the tenant server sends messages over the Switch and interacts with the external network of the data center via the export router. The user requests the tenant server to send a message to perform statistics .



Configuration thinking

Configure the flow speed limit along the following lines:

1. Configure a standard ACL rule marked by numbers;
2. ACL flow statistics;

Operating steps

Step 1 Configure standard acl

```
Console(config)#access-list ip-acl 1
Console(config-ip-nacl-1)#permit 192.168.1.100/32
```

Step 2 Limit flow rate

```
Console(config)#traffic-statistic ip-acl 1 in
```

Step 3 Verify the configuration results

Use the command to view the acl configuration.

```
Console(config)#show access-list config 1
The step of ACL subitem number: 1
```

```
    IP Access List 1, match-order is config, 1 rule:
      0 : permit 192.168.1.100/32
```

View traffic statistics configuration.

```
  Console(config)#show qos-info traffic-statistic
  traffic-statistic:
    Matches: access-list 1 subitem 0 running
      0 packet
```

Configuration file

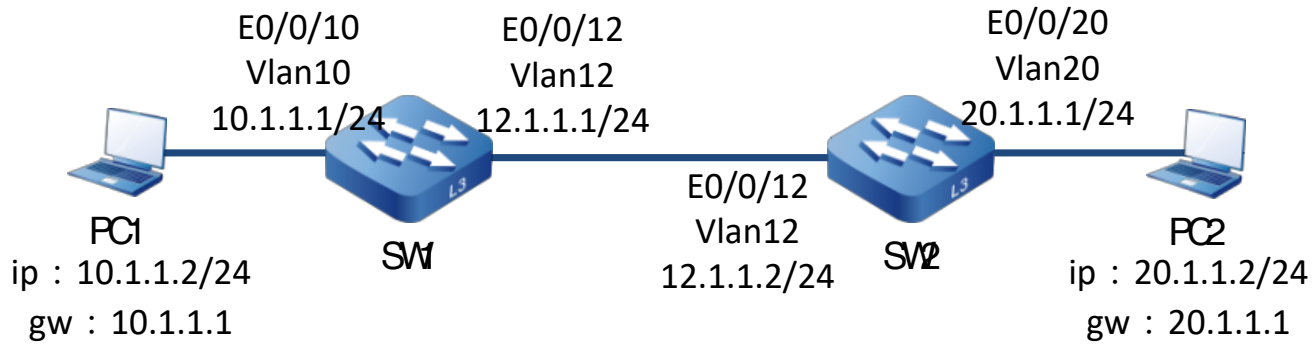
Switch configuration file

```
Console(config)#show running-config qacl

![QACL]
access-list ip-acl 1
0 permit 192.168.1.100/32
exit
traffic-statistic ip-acl 1 in
```

27. Example for Static Route configuration

Networking requirements

Hosts belonging to different network segments are connected through two switches. Users do not need to configure dynamic routing protocols to implement interworking between any two hosts on different network segments.



Configuration thinking

I. Configuring the VLAN and IP address to which each interface belongs

2. Configure IP and gw for the two hosts. Static routes are configured on the switch. If no dynamic routing protocol is configured, any two hosts on different network segments can communicate with each other.

Operating steps

Step 1 Create VLANs and configure the VLANs to which each interface belongs. Configure the IP address of each VLANIF interface.

Step 2 Two hosts configure ip, gw (slightly)

Step 3 Configure static routes on the switch.

#Configure SW1

SW1(config)#ip route 20.1.1.0 255.255.255.0 12.1.1.2

#Configure SW2

SW2(config)#ip route 10.1.1.0 255.255.255.0 12.1.1.1

#PC2 ping PC1

C:\Users\Administrator>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:
Reply from 10.1.1.1: bytes=32 time=4ms TTL=61
Reply from 10.1.1.1: bytes=32 time=4ms TTL=61
Reply from 10.1.1.1: bytes=32 time=4ms TTL=61
Reply from 10.1.1.1: bytes=32 time=4ms TTL=61

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms

Configuration file

```
#Configuration file for SW1
hostname SW1
vlan 10,12
interface vlan-interface 10
ip address 10.1.1.1 255.255.255.0
exit
interface vlan-interface 12
ip address 12.1.1.1 255.255.255.0
exit
interface ethernet 0/0/10
switchport link-type access
switchport pvid 10
exit
interface ethernet 0/0/12
switchport link-type access
switchport pvid 12
exit
ip route 20.1.1.0    255.255.255.0 12.1.1.2
exit

#Configuration file for SW2
hostname SW2
vlan 12,20
interface vlan-interface 20
ip address 20.1.1.1 255.255.255.0
exit
interface vlan-interface 12
ip address 12.1.1.2 255.255.255.0
exit
```

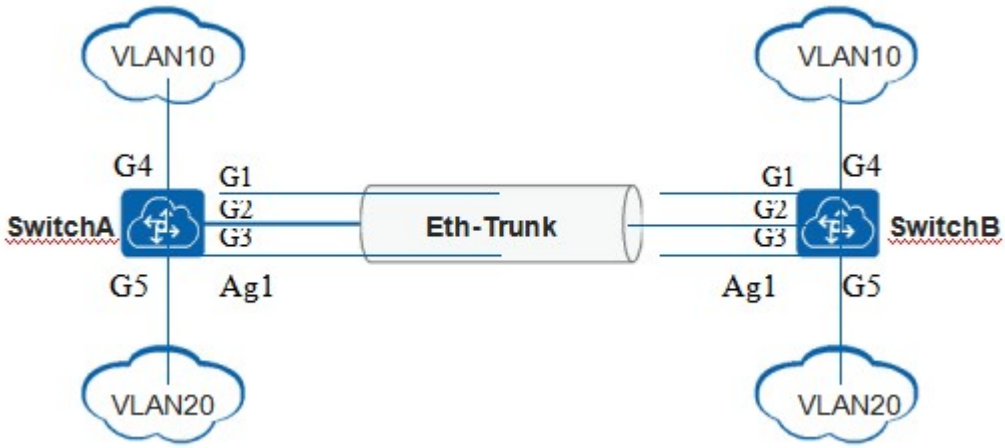
```
interface ethernet 0/0/20
switchport link-type access
switchport pvid 20
exit
interface ethernet 0/0/12
switchport link-type access
switchport pvid 12
exit
ip route 10.1.1.0    255.255.255.0 12.1.1.1
```

28. Example for LACP configuration

28.1 Configure an example of static link aggregation

Networking requirements

As shown in the following diagram, SwitchA and SwitchB are connected to the network of VLAN10 and VLAN20 through the Ethernet link respectively, and there is a larger data flow between SwitchA and SwitchB.
Users hope that SwitchA and SwitchB can provide large link bandwidth to enable the same VLAN to communicate with each other. At the same time, users also want to provide a certain degree of redundancy to ensure the reliability of data transmission and link.



Configuration thinking

The following ideas are used to configure the load sharing link aggregation.
1.Create VLAN and add the port to VLAN.
2.Add the member ports to the static aggregation group to increase the link bandwidth.
3.The load sharing mode is configured to realize the load sharing between the ports of the members of the aggregate group and increase the reliability.

Operating steps

Step 1 Create VLAN and add the port to VLAN.
Create VLAN10 and VLAN20 and add port. Switch B configuration similar to switch A. Here no longer say.
SwitchA(config)#vlan 10,20

```
SwitchA(config-if-vlan)#switchport ethernet 0/0/1 to ethernet 0/0/5
SwitchA(config-if-vlan)#exit
SwitchA(config)#interface range ethernet 0/0/1 to e 0/0/5
SwitchA(config-if-range)#switchport link-type trunk
SwitchA(config-if-range)#exit
```

Step 2 Add member ports to static aggregation groups on switch A and switch B.

```
#Configuration of switch A
SwitchA(config)#interface eth-trunk 1
SwitchA(config-if-eth-trunk-1)#link-aggregation members ethernet 0/0/1 to ethernet 0/0/3
SwitchA(config-if-eth-trunk-1)#link-aggregation mode static
SwitchA(config-if-eth-trunk-1)#exit

#Configuration of switch B
SwitchB(config)#interface eth-trunk 1
SwitchB(config-if-eth-trunk-1)#link-aggregation members ethernet 0/0/1 to ethernet 0/0/3
SwitchB(config-if-eth-trunk-1)#link-aggregation mode static
SwitchB(config-if-eth-trunk-1)#exit
```

Step 3 Configure load sharing way of Eth-Trunk1. Switch B is similar to switch A.Here no longer say.

```
SwitchA(config-if-eth-trunk-1)#link-aggregation load-balance dst-mac
SwitchB(config-if-eth-trunk-1)#link-aggregation load-balance dst-mac
```

Step 4 Verify configuration results

Execute the **show lacp** command under any view.

```
SwitchA(config)#show lacp local

eth-trunk ID: 1, load balance: dst-mac, status: static
Port        State   A-Key   O-Key   Priority   Logic-port   Actor-state
GE0/0/1     bndl    -       -       -          1            -
GE0/0/2     bndl    -       -       -          1            -
GE0/0/3     bndl    -       -       -          1            -

actor-state: activity/timeout/aggregation/synchronization
                collecting/distributing/defaulted/expired
```

Configuration file

The configuration file of switch A is the same as that of switch B.Here no longer say.

```
SwitchA(config)#show running-config
!LanSwitch BuildRun
enable
configure terminal
![VLAN]
vlan 10,20
exit
![LACP]
interface eth-trunk 1
link-aggregation load-balance dst-mac
exit
interface ethernet 0/0/1
link-aggregation eth-trunk 1
exit
interface ethernet 0/0/2
link-aggregation eth-trunk 1
exit
interface ethernet 0/0/3
link-aggregation eth-trunk 1
exit
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
switchport trunk allowed vlan 10,20
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 10,20
exit
interface ethernet 0/0/3
switchport link-type trunk
switchport trunk allowed vlan 10,20
exit
interface ethernet 0/0/4
switchport link-type trunk
switchport trunk allowed vlan 10,20
exit
interface ethernet 0/0/5
switchport link-type trunk
switchport trunk allowed vlan 10,20
exit
```

28.2 Configuration dynamic link aggregation example

Networking requirements

As shown in the following figure, a dynamic link aggregation group is configured on two Switch devices to improve the bandwidth and reliability between two devices and require load sharing.

Configuration thinking

The following ideas are used to configure dynamic link aggregation:
1. Create VLAN and add the port to VLAN.
2. Add the member ports to the dynamic aggregation group to increase the link bandwidth.

Operating steps

Step 1 Create a VLAN and add the port to VLAN.
Create VLAN10 and VLAN20 and add port repectively. Switch B configuration is similar to switch A.

```
SwitchA(config)#vlan 10,20
SwitchA(config-if-vlan)#switchport ethernet 0/0/1 to ethernet 0/0/5
SwitchA(config-if-vlan)#exit
SwitchA(config)#interface range ethernet 0/0/1 to e 0/0/5
SwitchA(config-if-range)#switchport link-type trunk
SwitchA(config-if-range)#exit
```

Step 2 Member ports are added to the dynamic aggregation group on SwitchA and SwitchB.
#Configuration of switch A

```
SwitchA(config)#interface eth-trunk 1
SwitchA(config-if-eth-trunk-1)#link-aggregation members ethernet 0/0/1 to ethernet 0/0/3
SwitchA(config-if-eth-trunk-1)#link-aggregation mode dynamic
SwitchA(config-if-eth-trunk-1)#exit
```

#Switch B configuration:

```
SwitchB(config)#interface eth-trunk 1
SwitchB(config-if-eth-trunk-1)#link-aggregation members ethernet 0/0/1 to ethernet 0/0/3
```

SwitchB(config-if-eth-trunk-1)#link-aggregation mode dynamic
SwitchB(config-if-eth-trunk-1)#exit

Step 3 Verify configuration results
Execute the **show lacp** command under any view.
SwitchA(config)#show lacp local

eth-trunk ID: 1, load balance: dst-mac, status: dynamic

Port	State	A-Key	O-Key	Priority	Logic-port	Actor-state
GE0/0/1	bndl	2	2	128	1	10111100
GE0/0/2	bndl	2	2	128	1	10111100
GE0/0/3	bndl	2	2	128	1	10111100

actor-state: activity/timeout/aggregation/synchronization
collecting/distributing/defaulted/expired

Configuration file

The configuration file of switch A is the same as that of switch B.Here no longer say.
SwitchA(config)#show running-config

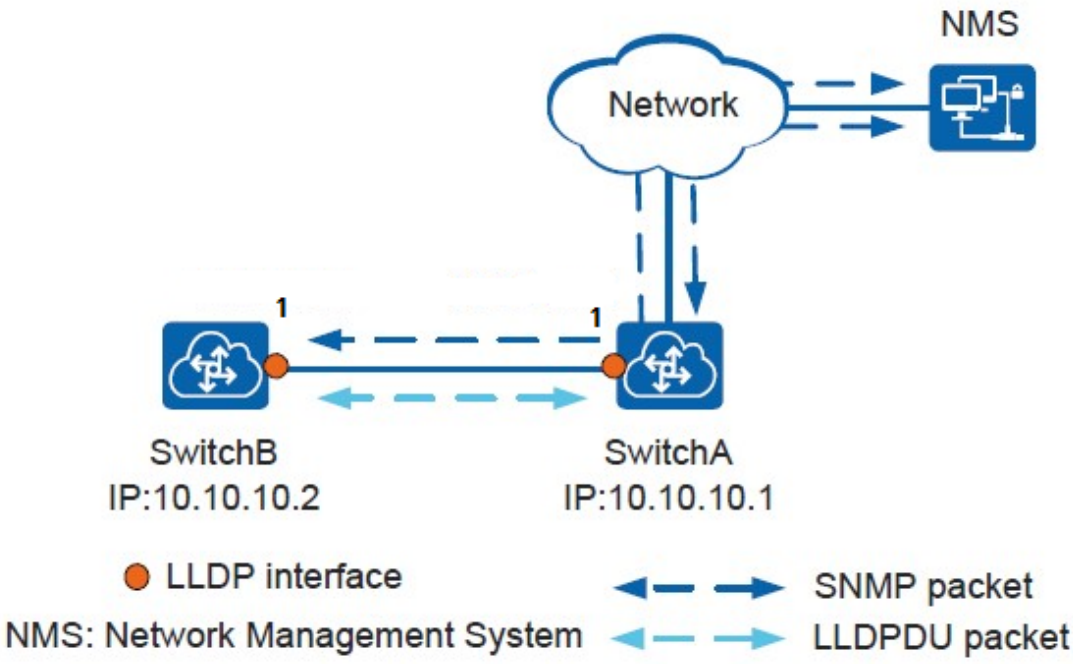
```
![VLAN]
vlan 10,20
exit
![LACP]
interface eth-trunk 1
link-aggregation mode dynamic
link-aggregation load-balance dst-mac
exit
interface ethernet 0/0/1
link-aggregation eth-trunk 1
exit
interface ethernet 0/0/2
link-aggregation eth-trunk 1
exit
interface ethernet 0/0/3
link-aggregation eth-trunk 1
exit
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
switchport trunk allowed vlan 10,20
```

```
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 10,20
exit
interface ethernet 0/0/3
switchport link-type trunk
switchport trunk allowed vlan 10,20
exit
interface ethernet 0/0/4
switchport link-type trunk
switchport trunk allowed vlan 10,20
exit
interface ethernet 0/0/5
switchport link-type trunk
switchport trunk allowed vlan 10,20
exit
```

29. Example for LLDP configuration

Networking requirements

As shown in the following figure, the SwitchA and SwitchB are directly connected, and the network management system NMS is reachable between SwitchA and SwitchB and the SNMP configuration has been completed.
The network administrator hopes to get the communication information between the SwitchA and SwitchB link and the alarm information of the device function change on NMS, which is used to understand the detailed topology of the network and determine whether there is configuration conflict in the network.



Configuration thinking

The network administrator hopes to get the communication between switch A and switch B on NMS, which can be realized by configuring the LLDP function. The configuration ideas are as follows:
1. Enable switch A and switch B global LLDP function.
2 Configure switch A and switch B management IP address is convenient for network management system to manage.

Operating steps

Step 1 Enable global LLDP function of SwitchA and SwitchB

Configure SwitchA

SwitchA(config)#lldp

Configure SwitchB

SwitchB(config)#lldp

Step 2 Configure the Management IP address of switch A and switch B

Configure SwitchA

SwitchA(config)#interface vlan-interface 1

SwitchA(config-if-vlanInterface-1)#ip address 10.10.10.1 255.255.255.0

SwitchA(config)#interface ethernet 0/0/24

SwitchA(config-if-ethernet-0/0/24)#lldp management-address vlan-interface 1

SwitchA(config-if-ethernet-0/0/24)#exit

Configure SwitchB

SwitchB(config)#interface vlan-interface 1

SwitchB(config-if-vlanInterface-1)#ip address 10.10.10.2 255.255.255.0

SwitchB(config)#interface ethernet 0/0/24

SwitchB(config-if-ethernet-0/0/24)#lldp management-address vlan-interface 1

SwitchB(config-if-ethernet-0/0/24)#exit

Step 3 Verify configuration results

View the neighbor information of SwitchA

SwitchA(config)#show lldp interface ethernet 0/0/24

System LLDP: enable

LLDP hello-time: 30(s) LLDP hold-times: 4 LLDP TTL: 120(s)

Interface e0/0/24

Port LLDP: rxtx Pkt Tx: 13 Pkt Rx: 1

Total neighbor count: 1

Local Management Address: main IP of vlan-interface 1

Neighbor (1):

TTL: 118(s)

Chassis ID: 00:0a:6a:00:03:ee

Port ID: port e0/0/24

System Name: SwitchB

System Description: Switch

Port Description: NULL
Management Address: 10.10.10.2
Port Vlan ID: 1
Port SetSpeed: auto
Port ActualSpeed: FULL-1000
Port Link Aggregation: support ,not in aggregation

Configuration file

Configuration file for SwitchA
SwitchA(config)#show running-config if lldp

```
![IF]
interface vlan-interface 1
ip address 10.10.10.1 255.255.255.0
exit
![LLDP]
lldp
interface ethernet 0/0/24
lldp management-address vlan-interface 1
exit
```

Configuration file for SwitchB
SwitchB(config)#show running-config if lldp

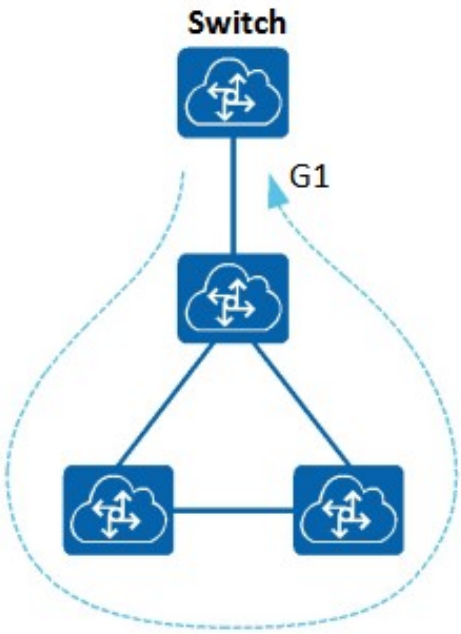
```
![IF]
interface vlan-interface 1
ip address 10.10.10.2 255.255.255.0
exit
![LLDP]
lldp
interface ethernet 0/0/24
lldp management-address vlan-interface 1
exit
```

30. Example for Loopback-detection configuration

Networking requirements

As shown in the following figure, if the network connected by the interface 10GE1/0/1 has a loop that leads to a broadcast storm, it may affect the communication of Switch and the entire network. Users hope to get loop detection in networks on the Switch, and by decreasing the loop of blocking downlink interface

The impact of other networks such as Switch and Switch can configure Loopback Detection function on Switch to detect whether the interface of the device has loopback, so as to determine whether there is a loop in the external network connected by the interface.



Configuration thinking

Configure the Loopback Detection function along the following lines:

1. Enable the global loopback-detection function, enable the Loopback detection function of the interface, realize the detection of the downlink network loop.
2. Configure the shutdown port when a loop is detected.

Operating steps

Step 1 Configure the shutdown port after it is not in the loop

Console(config)#loopback-detection action shutdown
Step 2 Enable loopback-detection function of port1
Console(config)#loopback-detection interface ethernet 0/0/1

Step 3 Verify configuration results
View the current status when disable in any view:
Console(config)#show loopback-detection
Loopback-detection action: Shutdown
Loopback-detection interval: 5s
Loopback-detection recover-time: 20s
Port Info:
PortId LB-Detect PortStatus
GE0/0/1 Enable Normal
GE0/0/2 Disable Normal
……

Configuration file

Switch configuration file;
Console(config)#show running-config stp

![STP]
loopback-detection interface ethernet 0/0/1
loopback-detection action shutdown

31. Example for Management configuration

Networking requirements

None

Configuration thinking

The DUT has a default superuser: Switch/Switch. Users can be configured as follows:
1. Configure the Guest permission user, user name: user_guest, password: guest.
2. Configure the User privilege user, username: User_user, password: user.
3. Configure the Operator permission user, user name: User_operator, password: operator.
4. Configure Manager rights user, user name: User_manager, password: manager.
5. Configure user User_operator to login only on the Console;
6. Configure user User_manager to log in for 5 consecutive times to enter the silence time;

Operating steps

Step1 Configure the Guest permission user, user name: user_guest, password: guest.
Console(config)# username user_guest privilege 0 password 0 guest
Console(config)#

Step2 Configure the User privilege user, username: User_user, password: user.
Console(config)# username User_user privilege 1 password 0 user
Console(config)#

Step3 Configure Operator permission user, username: User_operator, password: operator.
Console(config)# username User_operator privilege 2 password 0 operator
Console(config)#

Step4 Configure Manager privilege user, username: User_manager, password: manager.
Console(config)# username User_manager privilege 15 password 0 manager
Console(config)#

Step5 Configure user User_operator to login only on Console
Console(config)#username User_operator terminal console
Console(config)#

Step6 User User_manager is configured to log in for 5 consecutive times to enter the silent time;
Console(config)# username failmax User_manager 5
Console(config)#

Step7 Verify configuration results.
Console(config)# show username
display user information
Terminal type: C=Console, T=Telnet, S=SSH, W=Web
Global Failmax: n/a

User Name	level	Role	Terminal	FailMax	Fail	OnLineMax	OnLine
Switch	15	Manager	CTSW	n/a	0	n/a	1
user_guest	0	Guest	CTSW	n/a	0	n/a	0
User_user	1	User	CTSW	n/a	0	n/a	0
User_operator	2	Operator	CTSW	n/a	0	n/a	0
User_manager	15	Manager	CTSW	5	0	n/a	0

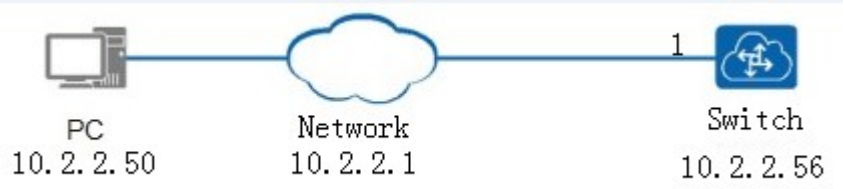
Configuration file

Configuration file for user management
Console#show running-config oam
![OAM]
username user_guest privilege 0 password 0 guest
username User_user privilege 1 password 0 user
username User_operator privilege 2 password 0 operator
username User_manager privilege 15 password 0 manager
username User_operator terminal console
username failmax User_manager 5

32. Example for Interface Management configuration

Networking requirements

As shown below, the switch connects to the host over the network, and the configure management interface 4094 through which the host can access the switch.



Configuration thinking

The configuration thinking are as follows:
1. Create vlan 4094 and add PC to vlan 4094 through the network connection port.
2. Configure management interface vlan 4094, configure management IP 10.2.2.56 and 2001: 1. 1

Operating steps

Step 1 Add port 1 to vlan 4094.
SwitchA(config)#vlan 4094
SwitchA(config-if-vlan)#switchport ethernet 0/0/1
SwitchA(config-if-vlan)#exit

Step2 Configure Management interface vlan 4094.

Configure Management IP address as 10.2.2.56 / 24 and 2001: 1 / 64.
SwitchA(config)#interface vlan-interface 4094
SwitchA(config-if-vlanInterface-4094)#ip address 10.2.2.56 255.255.255.0
SwitchA(config-if-vlanInterface-1)#ipv6 address 2000::1/64
SwitchA(config-if-vlanInterface-4094)#exit
SwitchA(config)#interface ethernet 0/0/1
SwitchA(config-if-ethernet-0/0/1)#switchport pvid 4094
SwitchA(config-if-ethernet-0/0/1)#exit

Step3 Verify configuration results.

```
SwitchA(config)#show ip interface vlan-interface 4094
Show informations of interface
The mac-address of interface is 00:0a:6a:00:02:bb
Interface name          : VLAN-IF4094
Primary ipaddress     : 10.2.2.56/255.255.255.0
Secondary ipaddress : None
VLAN                        : 4094
Address-range           : None
Interface status       : Up

Total entries: 1 interface.
SwitchA(config)#show ipv6 interface vlan-interface 4094
Show informations of ipv6 interface

VLAN-IF4094:
sw1        Link type:Ethernet    HWaddr 00:0a:6a:00:02:bb    Queue:none
           IPv6 forwarding is disabled
           inet6 unicast 2000::1    prefixlen 64
           inet6 unicast FE80::20A:6AFF:FE00:3BB%sw1    prefixlen 64    automatic
           inet6 multicast FF02::1%sw1    prefixlen 16    automatic
           inet6 multicast FF02::1:FF00:3BB%sw1    prefixlen 16
           inet6 multicast FF02::1:FF00:1%sw1    prefixlen 16
           UP RUNNING SIMPLEX BROADCAST MULTICAST PROMISC
           MTU:1500    metric:1    VR:0    ifindex:3
           RX packets:0 mcast:0 errors:0 dropped:0
           TX packets:8 mcast:6 errors:0
           collisions:0 unsupported proto:0
           RX bytes:0    TX bytes:600

Total entries: 1 interface.
```

Configuration file

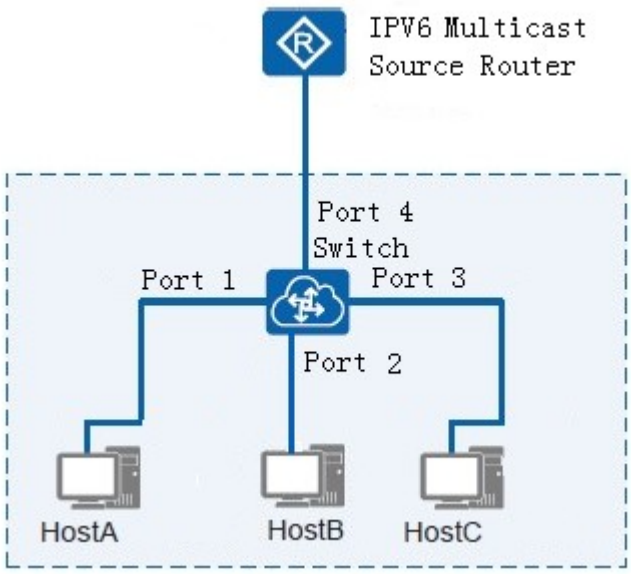
Configuration file for Switch

```
SwitchA(config)#show running-config if

![IF]
interface vlan-interface 4094
ip address 10.2.2.56 255.255.255.0
ipv6 address 2000::1/64
exit
```

33. Example for Multicast Listener Discovery Snooping configuration

Networking requirements

In the network shown below, the hosts of Host-A, Host-B, and Host-C are VLAN2, VLAN3, and VLAN4, respectively. The configuration allows 3 hosts to receive group addresses of FF02:: 0101 to FF02:: 0103 of multicast group data.



Configuration thinking

The configuration of MLD-snooping is as follows:
Enable mld-snooping switch, others use default configuration.

Operating steps

Step 1 Configure mld snooping

Console(config)#mld-snooping

Step 2 Verify configuration results

```
Console(config)#show mld-snooping
Enable MLD-Snooping
The max response time is 10 second(s)
The host port timeout is 300 second(s).
```

Disable MLD-Snooping route-port forward
The Router port timeout is 300 second(s), Currently aging is running
Denied VLAN
Black list:
NULL
White list:
NULL
Default group policy is permit
MLD-Snooping Querier : OFF
Querier vlan : 1
Querier Source IPv6 FE80::20A:6BFF:FE00:3BB
Max Respond Time 10 sec | Query interval 60 sec
Port Information:

port	groups-limit	fast-leave	mcast-vlan
GE0/0/1	1020	disabled	disabled
GE0/0/2	1020	disabled	disabled
GE0/0/3	1020	disabled	disabled
GE0/0/4	1020	disabled	disabled

……

When Host-A, Host-B and Host-C send MLD report messages to Switch, Switch will learn the corresponding multicast group table entries; View multicast groups learned by switches.

Console(config)#show multicast mld-snooping
show multicast table information
Time interval of multicast proxy is 10s

MAC Address : 33:33:00:00:01:01
VLAN ID : 1
Static port list :
MLD port list : GE0/0/4.

MAC Address : 33:33:00:00:01:02
VLAN ID : 1
Static port list :
MLD port list : GE0/0/4.

MAC Address : 33:33:00:00:01:03
VLAN ID : 1
Static port list :
MLD port list : GE0/0/4.

Total entries: 3 .

Configuration file

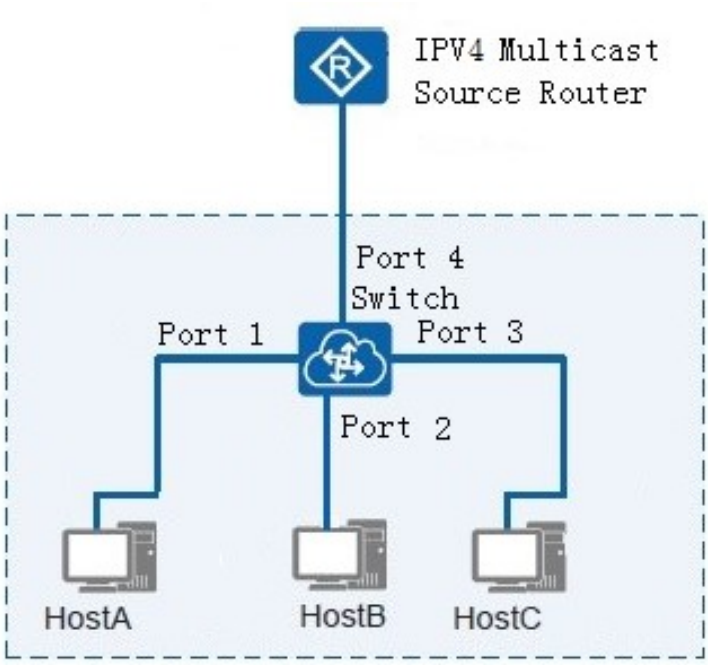
Switch configuration file
Console(config)#show running-config mld_snooping
![MLD_SNOOPING]
mld-snooping

34. Example for Multicast configuration

34.1 Example for configuration IGMP Snooping

Networking requirements

As shown below, in the multicast network, the router connects to the user network through a Layer 2 switch. The network has three receivers HostA, HostB, and HostC. As required by the service, Host-A, Host-B, and Host-C each want to receive multicast service data flows whose group addresses are 225.1.1.1 to 225.1.1.3.



Configuration thinking

The configuration thinking are as follows:

1. Enable igmp-snooping
2. The host sends a report message to the switch. The switch learns the multicast group.
3. The multicast source router sends a query packet to the switch. The switch learns route port entries.
4. The multicast source router sends multicast service traffic to the switch. The switch distributes the traffic to the host accordingly.

Operating steps

Step1 Configure IGMP Snooping function.

Global enable IGMP Snooping

Console(config)#igmp-snooping

Step2 Verify configuration results.

use the show ip igmp snooping command to view the global IGMP Snooping configuration

Console(config)#show igmp-snooping
Enable IGMP-Snooping
Disable IGMP-Snooping report-suppression
The max response time is 10 second(s)
The host aging time is 300 second(s).
Disable IGMP-Snooping route-port forward
The Router port timeout is 300 second(s), Currently aging is running
Denied VLAN:
Black list:
NULL
White list:
NULL
Default group policy is permit
IGMP-Snooping Querier : OFF
Querier vlan : 1
Querier Source IP 0.0.0.0 | Query interval 60 sec | Special query interval 1 s
ec | Robust count 2 | IGMP version 2
Port Information:

port	limit	action	fast-leave	mcast-vlan	igmp-profile	drop-type
e0/0/1	1020	drop	disabled	disabled	disabled	null
e0/0/2	1020	drop	disabled	disabled	disabled	null
e0/0/3	1020	drop	disabled	disabled	disabled	null

……

When Host-A, Host-B, and Host-C send igmp report packets to the switch, the switch learns the corresponding multicast group entries. When the multicast source router sends igmp query packets to the switch, the switch Learned the corresponding route port entry.

Use the show multicast igmp-snooping interface command to view the ports learning multicast.

Console(config)#show multicast igmp-snooping interface
show igmp-snooping multicast table information

Groups	Ports	VLAN	Exptime(s)	GrpMac	IGMPVer
225.1.1.1	GE0/0/1	1	288	01:00:5e:01:01:01	v2
225.1.1.2	GE0/0/2	1	270	01:00:5e:01:01:02	v2
225.1.1.3	GE0/0/3	1	280	01:00:5e:01:01:03	v2

Total Record: 3

Use the show igmp-snooping router-dynamic command to view the routing port.

```
Console(config)#show igmp-snooping router-dynamic
   Port            VID       Age          Type
GE0/0/4            1       290            { QUERY }
Total Record: 0
```

When Multicast Source Router sends multicast service data 225.1.1.1 to 225.1.1.3, Switch1 will distribute it to Host-A, Host-B, and Host-C accordingly.

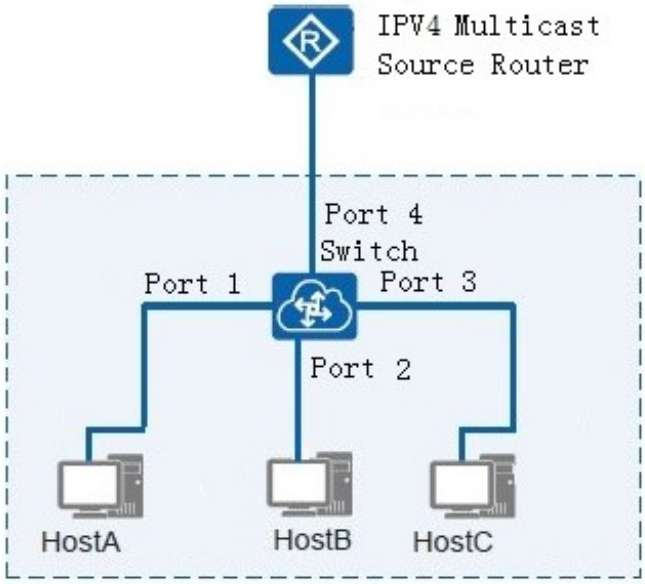
Configuration file

```
# Configuration file for switch
Console(config)#show running-config igmp_snooping
![IGMP_SNOOPING]
igmp-snooping
```

34.2 Example for Configuration Static Multicast

Networking requirements

As shown below, in a multicast network, routers connect to user networks through Layer 2 switches. The network has three receivers: HostA, HostB, and HostC. As required by the service, HostA and HostC want to receive packets with the destination address 01:00:5e:01:01:01, 01:00:5e:01:01:02, but HostB cannot receive them.



Configuration thinking

Configure static multicast MAC addresses on Layer 2 switches to meet this requirement:

1. Configure static multicast MAC address 01:00:5e:01:01:01,01:00:5e:01:01:02 on interfaces Gi1 and Gi3.

Operating Steps

Step1 Configure static multicast MAC address

```
Console(config)#multicast mac-address 01:00:5e:01:01:01 vlan 1 interface ether
net 0/0/1
Console(config)#multicast mac-address 01:00:5e:01:01:02 vlan 1 interface ether
net 0/0/2
```

Step2 Verify configuration results.

Use show multicast command to view static multicast MAC configuration.

```
Console(config)#show multicast
show multicast table information
Time interval of multicast proxy is 10s
MAC Address            : 01:00:5e:01:01:01
VLAN ID                : 1
Static port list    : e0/0/1.
IGMP port list       :
Dynamic port list :
Proxy port list     :

MAC Address            : 01:00:5e:01:01:02
VLAN ID                : 1
Static port list    : e0/0/2.
IGMP port list       :
Dynamic port list :
Proxy port list     :

Total entries: 2 .
```

Configuration file

Configuration file for switch

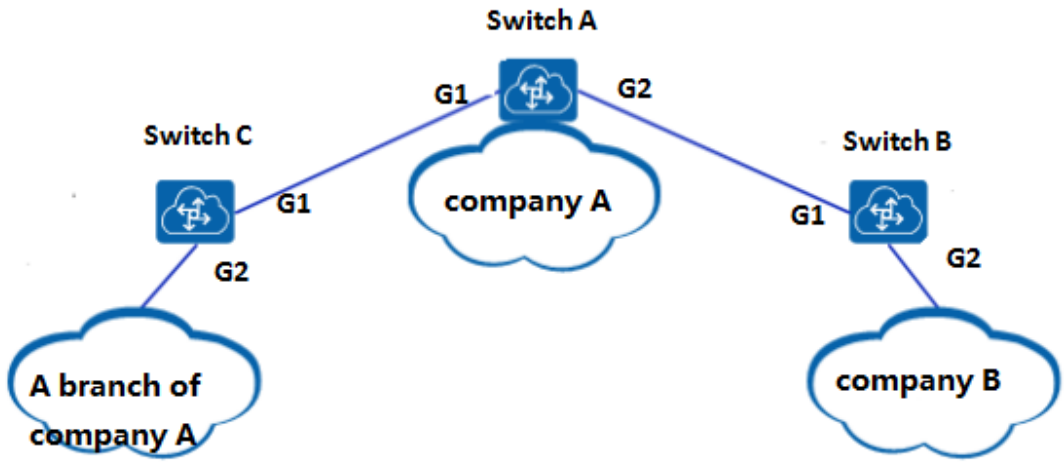
```
Console(config)#show running-config garp

![GARP]
```

multicast mac-address 01:00:5e:01:01:01 vlan 1 interface ethernet 0/0/1
multicast mac-address 01:00:5e:01:01:02 vlan 1 interface ethernet 0/0/2

34.3 Example for configure GMRP

Networking requirements

As shown below, Static multicast exists on SwitchC and SwitchB: 01:00:5e:01:01:01 VLAN1 contains both G1/G2 members. You need to learn GMRP on SwitchA. 01:00:5e;01:01:01 Vlan 1 multicast, and let G1 and G2 join;



Configuration thinking

The configuration thinking are as follows:
1. Configure static multicast and configure GMRP on Switch C.
2. Configure static multicast and configure GMRP on Switch B.
3. Configure GMRP related functions on Switch A.

Operating Steps

Step1 Configure the SwitchC;
SwitchC(config)#multicast mac-address 01:00:5e:01:01:01 vlan 1 interface ethernet 0/0/1 ethernet 0/0/2
SwitchC(config)#garp permit multicast mac-address 01:00:5e:01:01:01 vlan 1
SwitchC(config)#interface range ethernet 0/0/1 ethernet 0/0/2
SwitchC(config-if-range)#switchport link-type trunk
SwitchC(config-if-range)#gmrp
SwitchC(config-if-range)#exit
SwitchC(config)#gmrp

Step2 Configure the SwitchB;

```
SwitchB(config)#multicast mac-address 01:00:5e:01:01:01 vlan 1 interface ethernet 0/0/1 ethernet 0/0/2
SwitchB(config)#garp permit multicast mac-address 01:00:5e:01:01:01 vlan 1
SwitchB(config)#interface range ethernet 0/0/1 ethernet 0/0/2
SwitchB(config-if-range)#switchport link-type trunk
SwitchB(config-if-range)#gmrp
SwitchB(config-if-range)#exit
SwitchB(config)#gmrp
```

Step3 Configure the SwitchA;

```
SwitchA(config)#interface range ethernet 0/0/1 ethernet 0/0/2
SwitchA(config-if-range)#switchport link-type trunk
SwitchA(config-if-range)#gmrp
SwitchA(config-if-range)#exit
SwitchA(config)#gmrp
```

Step4 Verify configuration results.

View Switch A to learn multicast;

```
SwitchA(config)#show multicast
show multicast table information
Time interval of multicast proxy is 10s
MAC Address            : 01:00:5e:01:01:01
VLAN ID                : 1
Static port list   :
IGMP port list     :
Dynamic port list : e0/0/1-e0/0/2.
Proxy port list    :

Total entries: 1 .
```

View the SwitchC configuration

```
SwitchC(config)#show gmrp
GMRP status : enable
SwitchC(config)#show gmrp interface ethernet 0/0/1 ethernet 0/0/2
port      GMRP status
e0/0/1    enable
e0/0/2    enable

Total entries: 2.
```

Configuration file

Configuration file for Switch A;
SwitchA(config)#show running-config garp device

```
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
exit
interface ethernet 0/0/2
switchport link-type trunk
exit
![GARP]
gmrp
interface ethernet 0/0/1
gmrp
exit
interface ethernet 0/0/2
gmrp
exit
```

Configuration file for Switch B;
SwitchB(config)#show running-config garp device

```
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
exit
interface ethernet 0/0/2
switchport link-type trunk
exit
![GARP]
multicast mac-address 01:00:5e:01:01:01 vlan 1 interface ethernet 0/0/1 to ethernet 0/0/2
garp permit multicast mac-address 01:00:5e:01:01:01 vlan 1
gmrp
interface ethernet 0/0/1
gmrp
exit
interface ethernet 0/0/2
gmrp
```

exit

Configuration file for Switch C;
SwitchC(config)#show running-config garp device

```
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
exit
interface ethernet 0/0/2
switchport link-type trunk
exit
![GARP]
multicast mac-address 01:00:5e:01:01:01 vlan 1 interface ethernet 0/0/1 to ethernet 0/0/2
garp permit multicast mac-address 01:00:5e:01:01:01 vlan 1
gmrp
interface ethernet 0/0/1
gmrp
exit
interface ethernet 0/0/2
gmrp
exit
```

35. Example for PPPoE configuration

Networking requirements

Configure PPPoE-related function on switch as shown in the following figure:
Configure pppoE-related functionality on switch as shown in the following figure:
PC ----------(G1)Switch (G2)----------PPPoe-server

Configuration thinking

1. Configure client port to open PPPoE function on Switch.
2. The port connected to the server is configured on the switch to enable the trust function;
3. Configure custom circuit/remote-id content on switch;

Operating steps

Step 1 Enable the pppoe plus function of the port connected to the client PC;
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#pppoeplus

Step 2 The port connected to the server is configured as a pppoe plus trust port;
Console(config-if-ethernet-0/0/1)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#pppoeplus trust
Console(config-if-ethernet-0/0/2)#exit

Step 3 configure use custom types and configure the corresponding circuit-id and remote-id content
Console(config)#pppoeplus type self-defined circuit-id test_pppoe
Console(config)#pppoeplus type self-defined remote-id test_remote_id

Step 4 Verify the results
View configuration
Console(config)#show pppoeplus interface ethernet 0/0/1
PPPoE plus type : self-defined
circuit ID : "test_pppoe"
remote ID : "test_remote_id"
PPPoE plus format : binary
PPPoE plus content delimiter : space

```
GE0/0/1:
  Pppoe plus is enabled, port mode is untrust.
  The strategy of the port is replace.
  Drop padi and padr packet of the port is disabled.
  Drop pado and pads packet of the port is disabled.
  No user defined circuit ID.

Console(config)#show pppoeplus interface ethernet 0/0/2
PPPoE plus type : self-defined
  circuit ID : "test_pppoe"
  remote ID : "test_remote_id"
PPPoE plus format : binary
PPPoE plus content delimiter : space
---------------------------------
GE0/0/2:
  Pppoe plus is disabled, port mode is trust.
  The strategy of the port is replace.
  Drop padi and padr packet of the port is disabled.
  Drop pado and pads packet of the port is disabled.
  No user defined circuit ID.
```

Configuration file

Switch configuration file;

```
Console(config)#show running-config pppoeplus

![PPPOEPLUS]
pppoeplus type self-defined circuit-id "test_pppoe"
pppoeplus type self-defined remote-id "test_remote_id"
interface ethernet 0/0/1
pppoeplus
exit
interface ethernet 0/0/2
pppoeplus trust
exit
```

36. Example for RMON configuration

Networking requirements

As shown in the following figure, it is required to monitor the devices connected by the interface 2 of the switch, including:

1. Real time and historical statistics for traffic and the number of various types of packages.
2. The log is recorded when the per minute traffic exceeds the set value.
3. Monitor the subnet broadcast and multicast traffic, when exceeds a set value, take the initiative to report the alarm information to the NMS.

Configuration thinking

By configuring RMON statistical functions, real-time and historical statistical information can be monitored and monitored for the quantity of traffic and various types of packets. Configuring the RMON alarm function can record the log and report the alarm information to the NMS actively when the traffic exceeds the set value.

The following ideas are used to configure RMON:

1. Configuring the IP address of the switch interface and the network management end route can be reached.

2. Configuration allows Trap messages to be sent to NMS.

3. It can make statistics function and configure statistics table and history control table to realize RMON statistical function.

4. Configure event table and alarm table to realize RMON alarm function.

Operating steps

Step 1 Configure the IP address of the switch interface

```
Console(config)#interface vlan-interface 1
Console(config-if-vlanInterface-1)#ip address 10.2.2.5 255.255.255.0
Console(config-if-vlanInterface-1)#exit
```

Step 2 Configure allows Trap messages to be sent to NMS

```
Console(config)#snmp-server host 10.2.2.55 version 2 test
Console(config)#snmp-server community test rw permit
```

Step 3 Configure statistical function

```
# Configuration statistics
Console(config)#interface ethernet 0/0/2
Console(config-if-ethernet-0/0/2)#rmon statistics 1
```

Configure the history control table, set RMON sample traffic information in the subnet, sample intervals is 30 seconds, and save the recent 3 times of data

```
Console(config-if-ethernet-0/0/2)#rmon history 1 buckets 3 interval 30
```

Step 4 Configure alarm function

Configure the event table and set RMON's No.1 event handling mode to log and send Trap messages to network management stations.

```
Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.5.1 10 absolute rising 102400 1 falling 10240 1
Console(config)#rmon event 1 log-trap test
```

Step 5 Check configuration results

```
# View alarm configuration
Console(config)#show rmon alarm
AlarmEntry 1:
   Variable      : 1.3.6.1.2.1.16.1.1.5.1
   Interval      : 10
   Type          : absolute
   Rising        : threshold 102400 event index 1
   Falling       : threshold 10240 event index 1
   Last value    : 0
   Owner         : NULL
```

```
# View event configuration
Console(config)#show rmon eventlog
LogEntry 1, no logs
```

View statistics information
Console(config)#show rmon statistics interface ethernet 0/0/2
EtherStatsEntry 1:
  Interface : GE0/0/2
  Owner : NULL
  Octets : 17280, Pkts : 270, BroadcastPkts : 2
  MulticastPkts : 268, CRCAlignErrors : 0, UndersizePkts : 0
  OversizePkts : 0, Fragments : 0, Jabbers : 0
  Collisions : 0, DropEvents : 0, Pkts64 : 270
  Pkts65to127 : 0, Pkts128to255 : 0, Pkts256to511 : 0
  Pkts512to1023 : 0, Pkts1024to1518 : 0

View history statistics
Console(config)#show rmon history interface ethernet 0/0/2
HistoryControlEntry 1:
  Interface : GE0/0/2
  Owner : NULL
  Interval : 30
  Buckets : 3
  History record 1: 0 days 0 hours 6 minutes 35 seconds
    DropEvents : 0, Octets : 1024, Pkts : 16
    BroadcastPkts : 0, MulticastPkts : 16, CRCAlignErrors : 0
    UndersizePkts : 0, OversizePkts : 0, Fragments : 0
    Jabbers : 0, Collisions : 0, Utilization : 0
  History record 2: 0 days 0 hours 7 minutes 3 seconds
    DropEvents : 0, Octets : 960, Pkts : 15
    BroadcastPkts : 0, MulticastPkts : 15, CRCAlignErrors : 0
    UndersizePkts : 0, OversizePkts : 0, Fragments : 0
    Jabbers : 0, Collisions : 0, Utilization : 0
  History record 3: 0 days 0 hours 7 minutes 31 seconds
    DropEvents : 0, Octets : 1024, Pkts : 16
    BroadcastPkts : 0, MulticastPkts : 16, CRCAlignErrors : 0
    UndersizePkts : 0, OversizePkts : 0, Fragments : 0
    Jabbers : 0, Collisions : 0, Utilization : 0

Configuration file

Switch configuration file
  Console(config)#show running-config if snmp rmon

  ![SNMP]

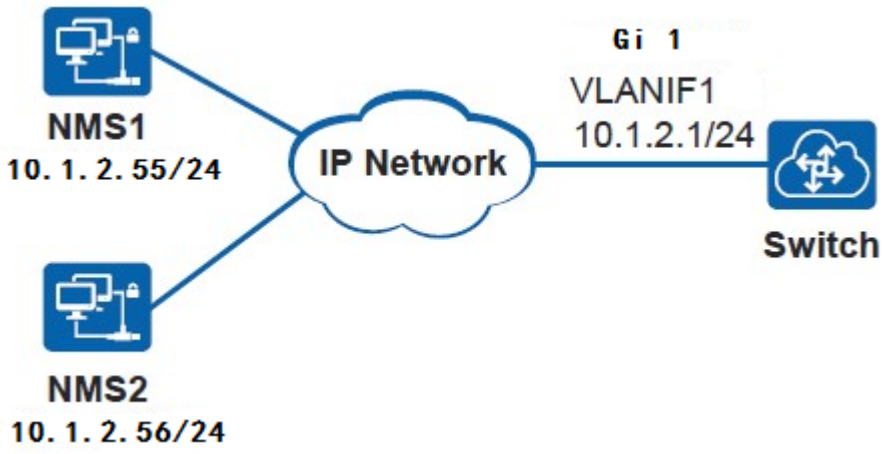
```
snmp-server community test rw permit view iso
snmp-server host 10.2.2.55 version 2c test udp-port 162 notify-type bridge gbn gbnsavecfg
interfaces rmon snmp
![IF]
interface vlan-interface 1
ip address 10.2.2.5 255.255.255.0
exit
![RMON]
interface ethernet 0/0/2
rmon statistics 1
exit
interface ethernet 0/0/2
rmon history 1 buckets 3 interval 30
exit
rmon event 1 log-trap test
rmon alarm 1 1.3.6.1.2.1.16.1.1.5.1 10 absolute rising 102400 1 falling 10240 1
```

37 Example for SNMP configuration

37.1 Configure device to use SNMPv1 to communicate with network management example

Networking requirements

As shown in the following figure, the network management NMS1 and NMS2 in the existing network supervise the equipment in the network. Because of the smaller network size and higher security factors, the configuration device uses the SNMPv1 version to communicate with the network management in the planning. Now, because of the need for expansion, a new switch is added and supervised by the network management. Users want to monitor the switches by using existing network resources, and can quickly locate and exclude failures in the event of failure.



Configuration thinking

In view of the high security of the network and the smaller network size, the new devices still use the SNMPv1 version. In order to reduce the burden of the network management station, NMS2 is selected to supervise the switch, and NMS1 does not supervise the switch. The following configuration ideas are used:

1. Set the SNMP version of the configuration switch is SNMPv1.
2. Configure access permissions to enable NMS2 to manage switches.
3. Configure the alarm host so that the alarm generated by the switch can be sent to NMS2. In order to locate the alarm information conveniently and avoid too many useless alerts, it will cause interference to the processing problem, and only allow the default open module to send the alarm.
4. Configure the network management station (only NMS2).

Operating steps

Step 1 Configure the interface IP address of the switch

Console(config)#interface vlan-interface 1
Console(config-if-vlanInterface-1)#ip address 10.1.2.1 255.255.255.0
Console(config-if-vlanInterface-1)#exit

Step 2 Configure access privilege

Configure ACL and only allow NMS2 to manage switches.
Console(config)#no login-access-list snmp all
Console(config)#login-access-list snmp 10.1.2.56 0.0.0.0

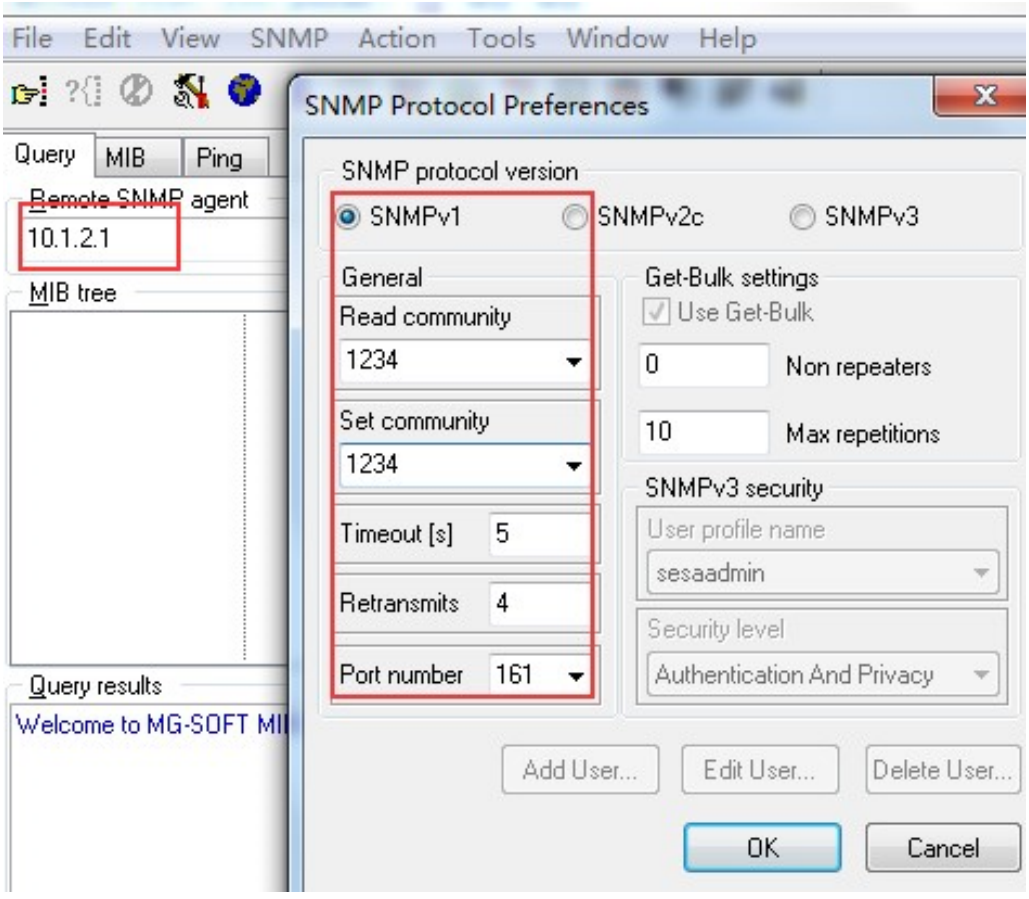
Configure read and write group names and enable the SNMP function
Console(config)#snmp-server community 1234 rw permit

Step 3 Configure the host server

Console(config)#snmp-server host 10.1.2.56 version 1 1234
Console(config)#snmp-server enable traps

Step 4 Configure the NMS2

#Install the MIB brower software and open it to connect.



Step 5 Verify configuration results

View snmp community
Console(config)#show snmp community
Show snmp community information
Encryption status: OFF

index	community	priority	state	view-name
1	1234	rw	permit	iso

Check the alarm host
Console(config)#show snmp host
Show SNMP trap host information

SNMP host ip	security	version
10.1.2.56	1234	1

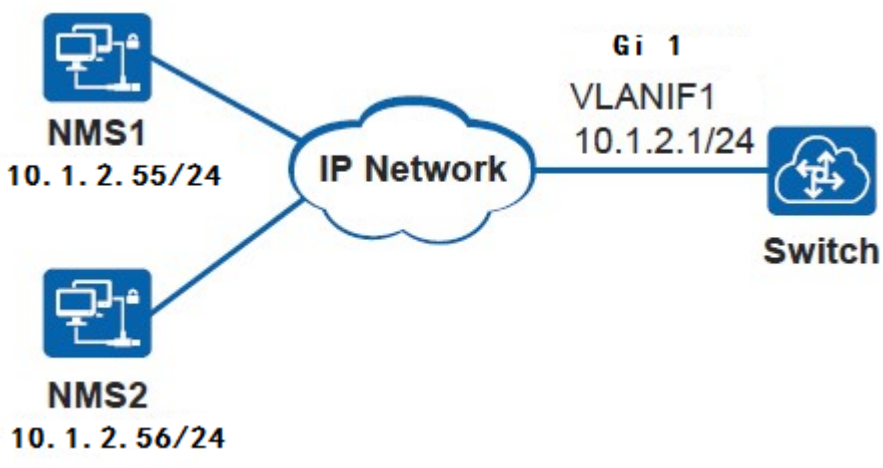
Configuration file

Configuration file of switch
Console(config)#show ru if snmp
![SNMP]
snmp-server name Switch
snmp-server community 1234 rw permit view iso
snmp-server host 10.1.2.56 version 1 1234 udp-port 162 notify-type bridge gbn gbnsavecfg interfaces rmon snmp
snmp-server enable traps bridge gbn gbnsavecfg interfaces rmon snmp
![IF]
interface vlan-interface 1
ip address 10.1.2.1 255.255.255.0
exit

37.2 Configure devices use SNMPv2 and network management communication examples

Networking requirements

As shown in the following figure, the network management NMS1 and NMS2 in the existing network supervise the equipment in the network. Because of the smaller network size and higher security factors, the configuration device uses the SNMPv1 version to communicate with the network management in the planning.
Now, because of the need for expansion, a new switch is added and supervised by the network management. Users want to monitor the switches by using existing network resources, and can quickly locate and exclude failures in the event of failure.



Configuration thinking

In view of the high security of the network and the smaller network size, the new devices still use the SNMPv1 version. In order to reduce the burden of the network management station, NMS2 is selected to supervise the switch, and NMS1 does not supervise the switch.
The following configuration ideas are used:
1. Configure the SNMP version as SNMPv1.
2. Configure access permissions to enable NMS2 to manage switches.
3. Configure the alarm host so that the alarm generated by the switch can be sent to NMS2. In order to locate the alarm information conveniently, avoid too many useless alarms to interfere with the problem of processing, only the module which is open by default can send alarm.
4. Configuration network management station (NMS2 only).

Operating steps

Step 1 Configure the interface IP address of the switch
Console(config)#interface vlan-interface 1

Console(config-if-vlanInterface-1)#ip address 10.1.2.1 255.255.255.0
Console(config-if-vlanInterface-1)#exit

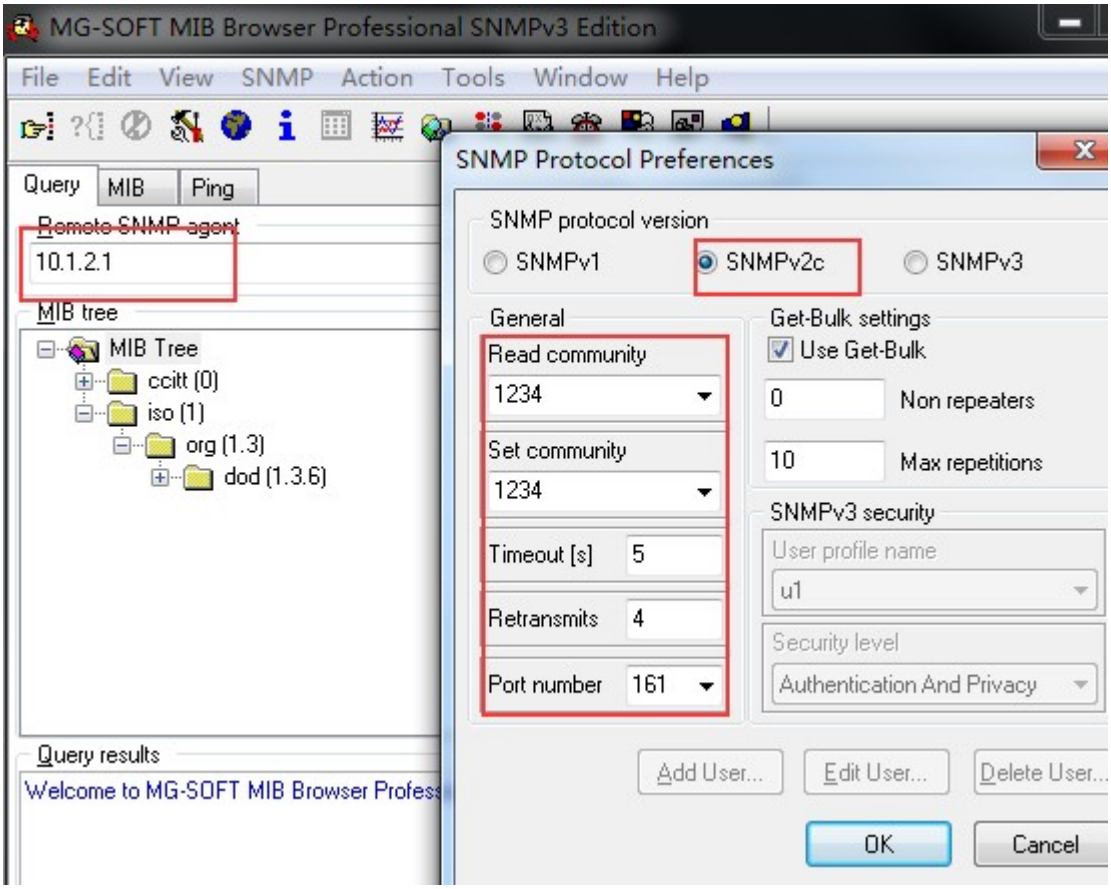
Step 2 Configure access authority
Configure ACLs to allow only NMS2 to manage switches.
Console(config)#no login-access-list snmp all
Console(config)#login-access-list snmp 10.1.2.56 0.0.0.0

Configure readable writable group names and enable snmp function
Console(config)# Console(config)#snmp-server community 1234 rw permit
Console(config)# snmp-server enable

Step 3 Configure trap host

Console(config)#snmp-server host 10.1.2.56 version 2c 1234

Step 4 Configuration network management station（NMS2）
#Install the MIB brower software and open it to connect



Step 5 Verify the configuration results
view snmp community
Console(config)#show snmp community

Show snmp community information
Encryption status: OFF
index community priority state view-name
1 1234 rw permit iso

Check the alarm host
Console(config)#show snmp host
Show SNMP trap host information
SNMP host ip security version
10.1.2.56 1234 2c

Configuration file

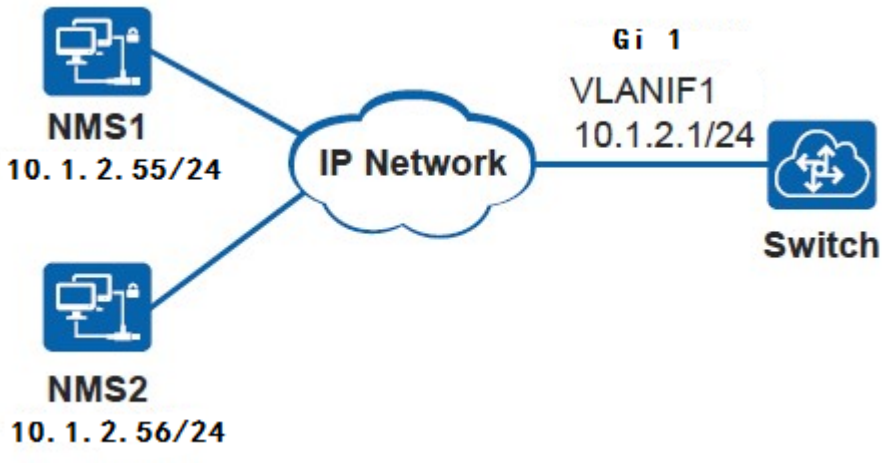
Switch configuration file

```
Console(config)#show ru snmp
![SNMP]
snmp-server community 1234 rw permit view iso
snmp-server host 10.1.2.56 version 2c 1234 udp-port 162 notify-type bridge gbn gbnsavecfg
interfaces rmon snmp
```

37.3 Configuration devices use SNMPv3 and network management communication examples (USM users)

Networking requirements

As shown in the following figure, the network management NMS1 and NMS2 in the existing network supervise the equipment in the network. Due to the large scale and low security of the network, the SNMPv3 configuration is used to communicate with the network management at the time of planning, and the authentication and encryption function is configured to ensure the security. Now, because of the need for expansion, a new switch is added and supervised by the network management.
Users want to supervise switches by using existing network resources and quickly locate and exclude failures in the event of failure.



Configuration thinking

In view of the high security of the network and the smaller network size, the new devices still use the SNMPv1 version. In order to reduce the burden of the network management station, NMS2 is selected to supervise the switch, and NMS1 does not supervise the switch.
The following configuration ideas are used:
1. Configure access permissions to enable NMS2 to manage switches.
2. Configure user groups and users, NMS2 establishes a connection to the device through the user group and the user.
3. Configure the snmp host so that the alarm generated by the switch can be sent to NMS2. In order to locate the alarm information conveniently and avoid too many useless alerts, it will cause interference to the processing problem, and only allow the default open module to send the alarm.
4. Configuration network management station（NMS2 Only）。

Operating steps

Step 1 Configure IP address of the interface of the switch

Console(config)#interface vlan-interface 1

Console(config-if-vlanInterface-1)#ip address 10.1.2.1 255.255.255.0

Console(config-if-vlanInterface-1)#exit

Step 2 Configure access list

Configure ACL, Only allow NMS2 to manage the switch.

Console(config)#no login-access-list snmp all

Console(config)#login-access-list snmp 10.1.2.56 0.0.0.0

Configure SNMP function enable

Console(config)# snmp-server enable

Step 3 Configure users and groups

Console(config)#snmp-server group g1 3 priv read iso write iso notify iso

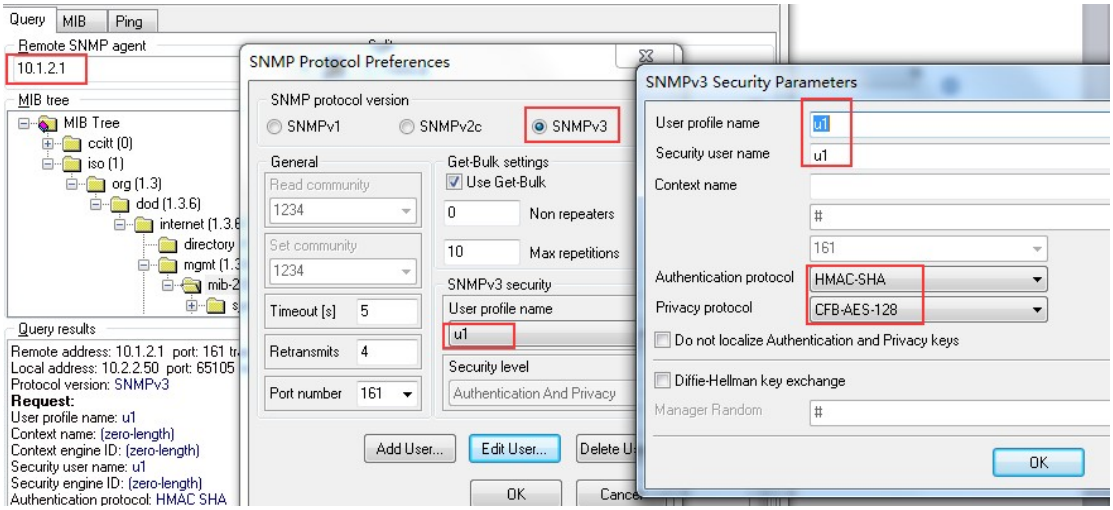
Console(config)#snmp-server user u1 g1 auth md5 auth-password 12345678 priv des priv-password 12345678

Step 4 Configure alarm host

snmp-server host 10.1.2.56 version 3 priv u1

Step 5 Configure network management station（NMS2）

#Install the MIB brower software and open it to connect.



Step 6 Verify configuration results

View users and groups

Console(config)#show snmp user u1

User name: u1

Engine ID: 138680000000000000000000

Authentication Protocol: HMACMD5AuthProtocol
Group-name: g1
Validation: valid

Console(config)#show snmp group g1
groupname: g1
securitymodel: 3 priv
readview: iso
writeview: iso
notifyview: iso
context: default value(NULL)

View view
Console(config)#show snmp view
View Name Type Subtree
iso Include 1
sysview Include 1.3.6.1.2.1.1
internet Include 1.3.6.1

view number:3
Check the alarm host
Console(config)#show snmp host
Show SNMP trap host information
SNMP host ip security version
10.1.2.56 u1 3

Configuration file

Switch configuration file
Console(config)#show running-config if snmp

![SNMP]
snmp-server user u1 g1 auth md5 auth-password encrypt-authpassword
82dfdb18864b9d57374fa1208e52c273 priv des priv-password encrypt-privpassword
82dfdb18864b9d57374fa1208e52c273
snmp-server group g1 3 priv write iso notify iso
snmp-server host 10.1.2.56 version 3 priv u1 udp-port 162 notify-type bridge gbn gbnsavecfg
interfaces rmon snmp
![IF]
interface vlan-interface 1
ip address 10.1.2.1 255.255.255.0
exit

38. Example for SNTP configuration

Networking requirements

As shown in the following figure, the switch needs time synchronization, and SNTP server and switch are reachable.

Configuration thinking

The configuration of SNTP is as follows:

On Switch, the SNTP server address is set to 192.168.2.66.

Operating steps

Step 1 Enable sntp.

Console(config)#sntp client

Step 2 Configure the IP address of the sntp server as 192.168.2.66.

Console(config)#sntp client valid-server 192.168.2.66 0.0.0.0

Step 3 Configure IP address of the interface VLANIF.

Console(config)#interface vlan-interface 1

Console(config-if-vlanInterface-1)#ip address 192.168.2.1 255.255.255.0

Console(config-if-vlanInterface-1)#exit

Step 4 Verify the Configure settings

Console(config)#show sntp client

```
 Clock state    : synchronized      Current mode      : broadcast
 Use server     : 192.168.2.66      State             : idle
 Server state : synchronized        Server stratum    : 1
 Authenticate : disable             Bcast delay       : 3ms
 Last synchronized time: WED JAN 31 11:14:09 2016
```

Summer-time is not set.
Valid server list:
Server address:192.168.2.66 wildcard:0.0.0.0

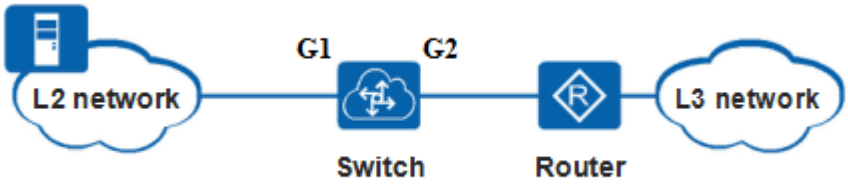
Configuring file

Switch configuration file
Console(config)#show ru if sntpc
![IF]
interface vlan-interface 1
ip address 10.2.2.56 255.255.255.0
exit
![SNTPC]
sntp client
sntp client valid-server 192.168.0.59 0.0.0.0

39. Example for Storm-suppression configuration

Networking requirement

As shown below, Switch A is the join point of the layer two network to the layer three router. It needs to limit the broadcast, multicast or unknown unicast message generated by the layer two network to generate the broadcast storm.



Configuration thinking

The following ideas are used to configure the Storm-suppression function：

1.Configure the units of storm-suppression;

2.Configure port broadcast storm, multicast storm, unknown unicast storm rate;

Operating steps

Step 1 Configure Global Storm Control Unit as byte

Console(config)#storm-suppression mode byte

Step 2 Configure port broadcast storm, multicast storm, unknown unicast storm rate;

Console(config)#interface ethernet 0/0/1

Console(config-if-ethernet-0/0/1)#storm-suppression broadcast kbps 1024

Console(config-if-ethernet-0/0/1)#storm-suppression multicast kbps 2048

Console(config-if-ethernet-0/0/1)#storm-suppression unicast kbps 5120

Step 3 Verify configurating result

Console(config)#show storm-suppression ethernet 0/0/1

Port number : e0/0/1

Broadcast storm suppression target rate is 1024 kbps

Multicast storm suppression target rate is 2048 kbps

Unicast storm suppression target rate is 5120 kbps
Total entries: 1.

Configuration file

The configuration file of the Switch
Console(config)#show running-config

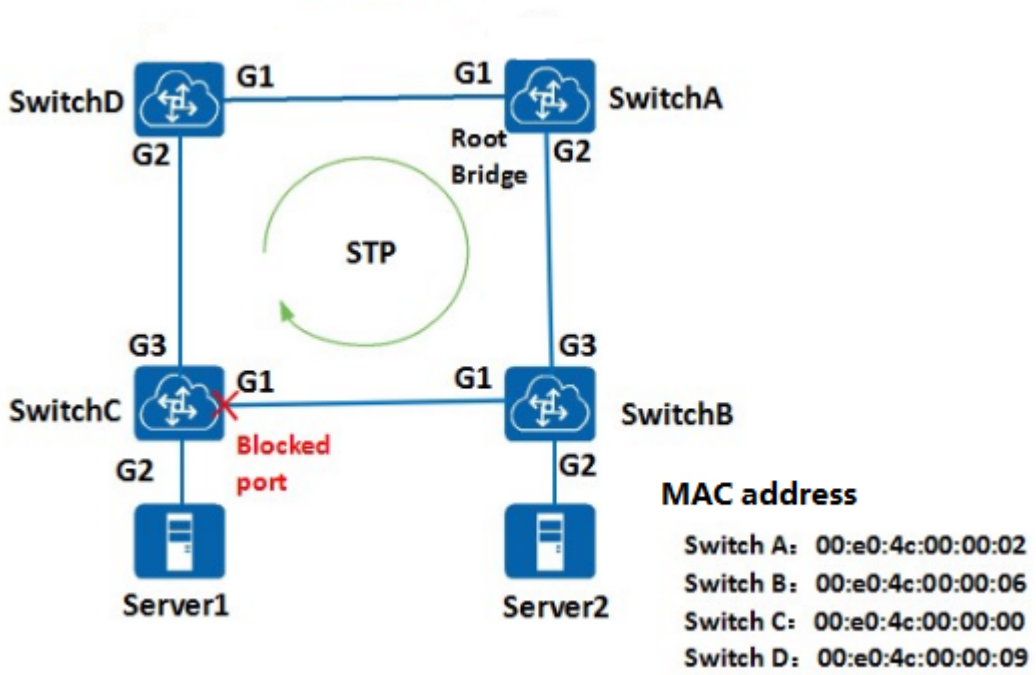
![DEVICE]
storm-suppression mode byte
interface ethernet 0/0/1
storm-suppression broadcast kbps 1024
storm-suppression unicast kbps 5120
storm-suppression multicast kbps 2048
exit

40. Example for Loop configuration

40.1 STP Configuration

Networking requirement

In a complex network, network planners tend to deploy multiple physical links between devices because of the need of redundant backup, one of which is to use main link and other links to backup. This will inevitably form a ring network. If there is a loop in the network, the broadcast storm and the MAC bridge item can be destroyed. After network planners plan the network, the STP protocol prevention loop can be deployed in the network. When there is a loop in the network, STP is blocked by a port to achieve the goal of breaking the loop.
As shown below, there are loops in the network, SwitchA, SwitchB, SwitchC and SwitchD are running STP, interact with each other through the information found in the loop networks, and have the option of a port is blocked, will eventually cut into a ring network structure network structure tree network loop, thereby preventing the message in a ring network in the continuous proliferation and infinite loop, avoid the equipment due to duplication of receiving the same message caused decline in processing capacity.



Configuration thinking

Tips for configuring STP：

1.Configure the spanning tree protocol of device in the ring network to work in STP mode;

2.Confirm root device；

3.Configure the DUT priority to block the port;

4.The port connected to the Server does not take part in STP computing, and it is 5.recommended to enable STP;
6.Verify the configuration results;

Operating Steps

Step 1 Configuration of switch A and switch B:
SwitchA(config)#stp mode stp
SwitchA(config)#stp priority 0
SwitchA(config)#stp

Step 2 Configure SwitchD：
SwitchB(config)#stp mode stp
SwitchB(config)#stp priority 4096
SwitchB(config)#stp

Step 3 ConfigureSwitch B:
SwitchC(config)#stp mode stp
SwitchC(config)#stp priority 8192
SwitchC(config)#stp

Step 4 Configure SwitchC:
SwitchC(config)#stp mode stp
SwitchC(config)#stp priority 12288　//It also could use default value 32665
SwitchC(config)#stp

Step 5 Disable the spanning tree function of the port connected to Server so that it does not participate in the STP calculation;
SwitchB(config)#interface ethernet 0/0/2
SwitchB(config-if-ethernet-0/0/2)#no stp
SwitchB(config-if-ethernet-0/0/2)#exit

SwitchC(config)#interface ethernet 0/0/2
SwitchC(config-if-ethernet-0/0/2)#no stp
SwitchC(config-if-ethernet-0/0/2)#exit

Step 6　Verify configuration results
View configuration：
SwitchA(config)#show stp interface brief
Spanning-tree protocol: Enabled, spanning-tree mode: STP

Port Protect: R-RootGuard, L-LoopGuard, B-BpduGuard, F-BpduFilter

---

Port	Cost	Priority	Protect	Role	State
GE0/0/1	20000	128	N/A	Designated	Forwarding
GE0/0/2	20000	128	N/A	Designated	Forwarding

Configuration file

Configuration file of switch A;

SwitchA(config)#show running-config stp

![STP]

stp priority 0

stp mode stp

Configuration file of switch B;

SwitchB(config)#show running-config stp

![STP]

stp priority 8192

stp mode stp

interface ethernet 0/0/2

no stp

exit

Configuration file of switch C;

SwitchC(config)#show running-config stp

![STP]

stp priority 12288

stp mode stp

interface ethernet 0/0/2

no stp

exit

Configuration file of switch D;

SwitchD(config)#show running-config stp

![STP]

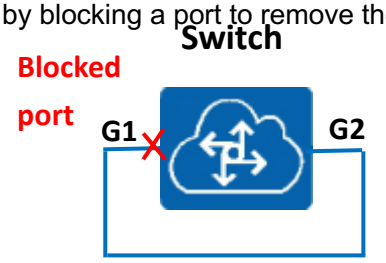
stp priority 4096

stp mode stp

40.2 Configure STP

Networking requirement

As shown in the following figure, the Switch two port forms a self ring, and the STP is transported in the Switch, and the loop is blocked by blocking a port to remove the loop.



Configuration thinking

Tips for STP function configuration:
Configure Switch's spanning-tree mode as STP;
View the election status of the spanning tree;
Configure port priority, achieved expected elections;
Verify the configuring result;

Operating Steps

Step 1 open the spanning tree function of Switch A, set the mode to STP;
SwitchA(config)# stp
SwitchA(config)# stp mode stp

Step 2 Check the election Status;
SwitchA(config)#show stp interface brief
Spanning-tree protocol: Enabled, spanning-tree mode: STP

Port Protect: R-RootGuard, L-LoopGuard, B-BpduGuard, F-BpduFilter

---

Port	Cost	Priority	Protect	Role	State
GE0/0/1	20000	128	N/A	Designated	Forwarding
GE0/0/2	20000	128	N/A	BackupPort	Discarding

PortID	config-status	cost	priority	role	forward-status
e0/0/1	enabled	20000	128	DesignatedPort	Forwarding
e0/0/2	enabled	20000	128	BackupPort	Discarding

From the above information, you can see that port 2 was selected as backup port and blocked;

Step 3 Configure port 1's port priority as 160;

SwitchA(config)#interface eth 0/0/1

SwitchA(config-if-ethernet-0/0/1)#stp port-priority 160

Step 4 Verify configuration results

SwitchA(config)#show stp interface brief

Spanning-tree protocol: Enabled, spanning-tree mode: STP

Port Protect: R-RootGuard, L-LoopGuard, B-BpduGuard, F-BpduFilter

---

Port	Cost	Priority	Protect	Role	State
GE0/0/1	20000	160	N/A	BackupPort	Discarding
GE0/0/2	20000	128	N/A	Designated	Forwarding

From the above information, you can see that port 1 is a backup port, which is blocked;

Configuration file

Configuration file of switch A; ;

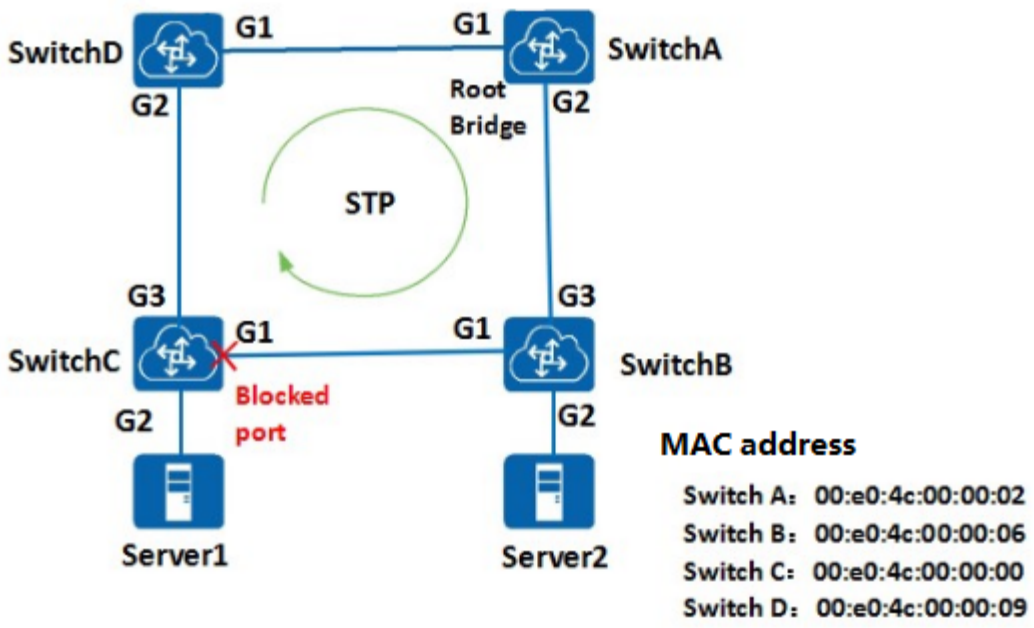
SwitchA(config)#show running-config stp

```
![STP]
stp priority 0
stp mode stp
interface ethernet 0/0/1
stp port-priority 160
exit
```

40.3 RSTP Configuration

Networking requirement

In a complex network, network planners tend to deploy multiple physical links between devices because of the need of redundant backup, one of which is to use main link and other links to backup. This will inevitably form a ring network. If there is a loop in the network, the broadcast storm and the MAC bridge item can be destroyed. After network planners plan a good network, the RSTP protocol can be deployed in the middle of the network to prevent the loop. When there is a loop in the network, RSTP is blocked by a port to achieve the goal of breaking the loop. As shown in Figure 9-18, there are loops in the network, Switch A, Switch B, Switch C and Switch D are running RSTP, interact with each other through the information found in the loop networks, and have the option of a port is blocked, will eventually cut into a ring network structure network structure tree network loop, thereby preventing the message in the ring in the network constantly proliferation and infinite loop, avoid the equipment due to repeated receiving the same message caused by the decline in processing capacity.



Configuration thinking

Tips for RSTP configuration:

1.Enable RSTP;

2.Confirm root device;

3.Configure the port's path overhead value to block the port;

Operation steps

Step 1 Configuration of witch A and switch B:

SwitchA(config)#stp mode rstp

SwitchA(config)#stp priority 0

SwitchA(config)#stp

Step 2 Configure switch D:
SwitchB(config)#stp mode rstp
SwitchB(config)#stp priority 4096
SwitchB(config)#stp

Step 3 Configure Switch B:
SwitchC(config)#stp mode rstp
SwitchC(config)#stp priority 8192
SwitchC(config)#stp

Step 4 Configure switch C:
SwitchC(config)#stp mode rstp
SwitchC(config)#stp priority 12288 // It also could use default value 32665
SwitchC(config)#stp

Step 5 Enable the spanning tree function of the port connected to Server so that it does not participate in the STP calculation;
SwitchB(config)#interface ethernet 0/0/2
SwitchB(config-if-ethernet-0/0/2)#no stp
SwitchB(config-if-ethernet-0/0/2)#exit

SwitchC(config)#interface ethernet 0/0/2
SwitchC(config-if-ethernet-0/0/2)#no stp
SwitchC(config-if-ethernet-0/0/2)#exit

Step 6 Verify configuration results
View configuration:
SwitchA(config)#show stp interface brief
Spanning-tree protocol: Enabled, spanning-tree mode: RSTP

Port Protect: R-RootGuard, L-LoopGuard, B-BpduGuard, F-BpduFilter
---

Port	Cost	Priority	Protect	Role	State
GE0/0/1	20000	128	N/A	Designated	Forwarding
GE0/0/2	20000	128	N/A	Designated	Forwarding

Configuration file

Configuration file of switch A;
SwitchA(config)#show running-config stp

```
![STP]
stp priority 0
```

Configuration file of switch B;

```
SwitchB(config)#show running-config stp

![STP]
stp priority 8192
interface ethernet 0/0/2
no stp
exit
```

Configuration file of switch C;

```
SwitchC(config)#show running-config stp

![STP]
stp priority 12288
interface ethernet 0/0/2
no stp
exit
```

Configuration file of switch D;

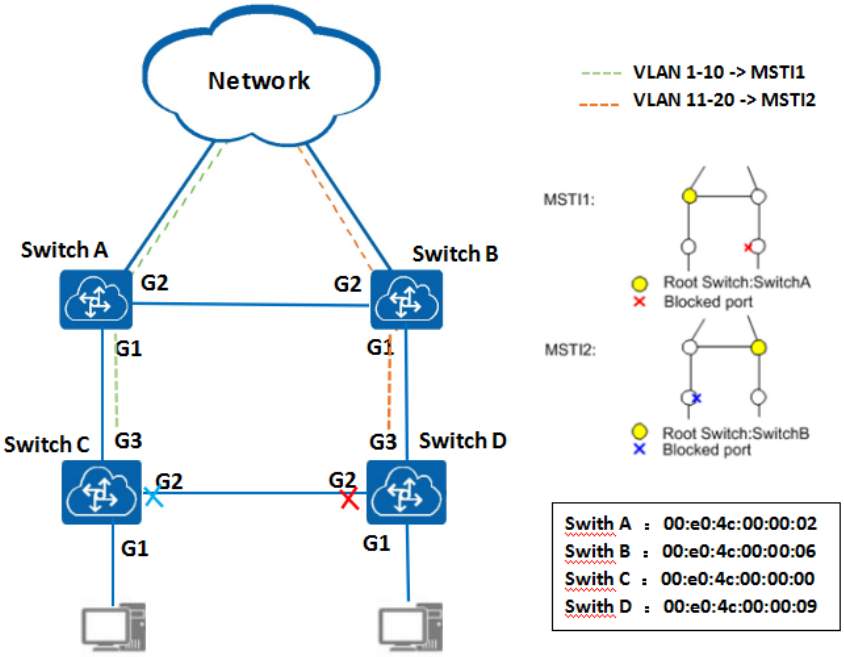
```
SwitchD(config)#show running-config stp

![STP]
stp priority 4096
```

40.4 MSTP Configuration

Networking requirement

In a complex network, due to the need of redundant backup, network planners tend to deploy multiple physical links between devices, one of which is used as a main link and others as a backup link. This will inevitably lead to a loop, if there is a loop in the network, it may cause a broadcast storm and MAC table items to be destroyed. To this end, the MSTP protocol prevention loop can be deployed in the middle of the network. MSTP can block redundant links in two layers of network, prune the network into a tree, and achieve the purpose of eliminating the loop.

As shown in the following figure, SwitchA, SwitchB, SwitchC, and SwitchD all run MSTP. They are connected to each other to form a ring network, because there is a redundant link between the SwitchA and the SwitchB, and between the SwitchC and the SwitchD. In order to share the traffic load of VLAN1 to VLAN10 and VLAN11 to VLAN20, this example uses the MSTP protocol to configure two MSTI, namely MSTI1 and MSTI2.



Configuration thinking

Tips for MSTP configuration:

1. Create VLAN;
2. Enable MSTP；
3. Configuring the domain name of the switch, the revision level, the instance VLAN mapping relationship;
4. confirm the total root, domain root equipment;
5. Configure the port's path overhead value to block the port;
6. Configure the port connected to Server as an edge port；
7. Verify the configure result;

Operating steps

Step 1 Switch A configuration:

```
Admin(config)#hostname SwitchA
SwitchA(config)#vlan 1-20
SwitchA(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/2
SwitchA(config-if-vlan)#exit
SwitchA(config)#interface range ethernet 0/0/1 t e 0/0/2
SwitchA(config-if-range)#switchport link-type trunk
SwitchA(config-if-range)#exit

SwitchA(config)#stp mode mstp
SwitchA(config)#mstp instance 1 vlan 1-10
SwitchA(config)#mstp instance 2 vlan 11-20
SwitchA(config)#mstp instance 1 priority 0
SwitchA(config)#mstp instance 2 priority 4096
SwitchA(config)#mstp region-name MSTP_Test
SwitchA(config)#STP
```

Step 2 Switch B configuration

```
Admin(config)#hostname SwitchB
SwitchB(config)#vlan 1-20
SwitchB(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/2
SwitchB(config-if-vlan)#exit
SwitchB(config)#interface range ethernet 0/0/1 t e 0/0/2
SwitchB(config-if-range)#switchport link-type trunk
SwitchB(config-if-range)#exit

SwitchB(config)#stp mode mstp
SwitchB(config)#mstp instance 1 vlan 1-10
SwitchB(config)#mstp instance 2 vlan 11-20
SwitchB(config)#mstp instance 1 priority 4096
SwitchB(config)#mstp instance 2 priority 0
SwitchB(config)#mstp region-name MSTP_Test
SwitchB(config)#STP
```

Step 3 SwitchC Configuration：

```
Admin(config)#hostname SwitchB
SwitchC(config)#vlan 1-20
SwitchC(config-if-vlan)#switchport ethernet 0/0/2 ethernet 0/0/3
SwitchC(config-if-vlan)#exit
```

SwitchC(config)#interface range ethernet 0/0/2 t e 0/0/3
SwitchC(config-if-range)#switchport link-type trunk
SwitchC(config-if-range)#exit

SwitchC(config)#stp mode mstp
SwitchC(config)#mstp instance 1 vlan 1-10
SwitchC(config)#mstp instance 2 vlan 11-20
SwitchC(config)#mstp instance 1 priority 8192
SwitchC(config)#mstp instance 2 priority 12288
SwitchC(config)#mstp region-name MSTP_Test
SwitchC(config)#STP

Step 4 Switch D configuration:
Admin(config)#hostname SwitchD
SwitchD(config)#vlan 1-20
SwitchD(config-if-vlan)#switchport ethernet 0/0/2 ethernet 0/0/3
SwitchD(config-if-vlan)#exit
SwitchD(config)#interface range ethernet 0/0/2 t e 0/0/3
SwitchD(config-if-range)#switchport link-type trunk
SwitchD(config-if-range)#exit

SwitchD(config)#stp mode mstp
SwitchD(config)#mstp instance 1 vlan 1-10
SwitchD(config)#mstp instance 2 vlan 11-20
SwitchD(config)#mstp instance 1 priority 12288
SwitchD(config)#mstp instance 2 priority 8192
SwitchD(config)#mstp region-name MSTP_Test
SwitchD(config)#STP

Step 5 Verification result
SwitchA(config)#show mstp instance brief
Current spanning tree protocol is MSTP
  Spanning tree protocol is enable
  Received information time factor is 3
  TC protection is enable, interval is 10, threshold is 6
  Flap guard is disable, max count 5, detect perid 10 s, recovery period 30 s

  MSTP Instance 0 vlans mapped:21-4094
  Bridge ID 32768-00e0.4c00.0000
  CIST root 32768-00e0.4c00.0000
  Region root 32768-00e0.4c00.0000

Bridge time HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20
Cist Root time HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20
External rpc: 0, Internal rpc: 0

PortID	Role	Sts	ExternalCost	InternalCost	Prio.Nbr	Type
GE0/0/1	Design	FWD	20000	20000	128.1	P2P
GE0/0/2	Design	FWD	20000	20000	128.2	P2P

MSTP Instance 1 vlans mapped:1-10
Bridge ID 0-00e0.4c00.0002
CIST root 32768-00e0.4c00.0000
Region root 0-00e0.4c00.0002
Bridge time HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20
Cist Root time HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20
External rpc: 0, Internal rpc: 0

PortID	Role	Sts	ExternalCost	InternalCost	Prio.Nbr	Type
GE0/0/1	Design	FWD	20000	20000	128.1	P2P
GE0/0/2	Design	FWD	20000	20000	128.2	P2P

MSTP Instance 2 vlans mapped:11-20
Bridge ID 4096-00e0.4c00.0002
CIST root 32768-00e0.4c00.0000
Region root 0-00e0.4c00.0006
Bridge time HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20
Cist Root time HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20
External rpc: 0, Internal rpc: 0

PortID	Role	Sts	ExternalCost	InternalCost	Prio.Nbr	Type
GE0/0/1	Design	FWD	20000	20000	128.1	P2P
GE0/0/2	Design	FWD	20000	20000	128.2	P2P

Configuration file

Configuration file of switch A;
SwitchA(config)#show running-config stp mstp vlan device

![VLAN]
vlan 2-20
exit

```
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
switchport trunk allowed vlan 2-20
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 2-20
exit
![STP]
stp mode mstp
![MSTP]
mstp region-name MSTP_Test
mstp instance 1 priority 0
mstp instance 1 vlan 1-10
mstp instance 2 priority 4096
mstp instance 2 vlan 11-20
```

Configuration file of switch B;

```
SwitchB(config)#show running-config stp mstp vlan device

![VLAN]
vlan 2-20
exit
![DEVICE]
interface ethernet 0/0/1
switchport link-type trunk
switchport trunk allowed vlan 2-20
exit
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 2-20
exit
![STP]
stp mode mstp
![MSTP]
mstp region-name MSTP_Test
mstp instance 1 priority 4096
mstp instance 1 vlan 1-10
mstp instance 2 priority 0
mstp instance 2 vlan 11-20
```

Configuration file of switch C;
SwitchC(config)#show running-config stp mstp vlan device

```
![VLAN]
vlan 2-20
exit
![DEVICE]
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 2-20
exit
interface ethernet 0/0/3
switchport link-type trunk
switchport trunk allowed vlan 2-20
exit
![STP]
stp mode mstp
![MSTP]
mstp region-name MSTP_Test
mstp instance 1 priority 8192
mstp instance 1 vlan 1-10
mstp instance 2 priority 12288
mstp instance 2 vlan 11-20
```

Configuration file of switch D;
SwitchD(config)#show running-config stp mstp vlan device

```
![VLAN]
vlan 2-20
exit
![DEVICE]
interface ethernet 0/0/2
switchport link-type trunk
switchport trunk allowed vlan 2-20
exit
interface ethernet 0/0/3
switchport link-type trunk
switchport trunk allowed vlan 2-20
exit
![STP]
```

stp mode mstp

![MSTP]

mstp region-name MSTP_Test

mstp instance 1 priority 12288

mstp instance 1 vlan 1-10

mstp instance 2 priority 8192

mstp instance 2 vlan 11-20

41. Example for switch information configuration

Networking requirements

As shown in the following figure, configure switch host name as Switch-123, phone number as 07234343120, location as china and the system time as 12:12 on December 12th 2016.

Configuration thinking

The basic information of the system is configured as follows:

1.Configure contact information.

2.Configure location

3.Configure system time.

4.Configure host name.

5.Configure welcome message.

Operating steps

Step1 Configure the contact information of switch .

Console(config)#snmp-server contact 0731-23250172-8600

Console(config)#

Step2 Configure location of the switch.

Console(config)#snmp-server location changsha.China

Console(config)#

Step3 Configure host name as Switch

Console(config)#hostname Switch

Console(config)#

Step4 The system time:

Console(config)#end

Console#clock set 8:8:8 2015/8/8

Set clock successfully.

Clock will be reset to 2004/01/01 00:00:00 after system rebooting because there is no realtime clock chip.

Console#

Step5 Start welcome message:

Console(config)#banner

Step6 Verify configuration results.

Console(config)#show clock

Sat 2015/08/08 08:09:41 CCT 08:00

Configuration file

Configuration file for Switch

Console(config)#show running-config snmp oam

![OAM]

banner

hostname Switch

![SNMP]

snmp-server contact 0731-23250172-8600

snmp-server location changsha.China

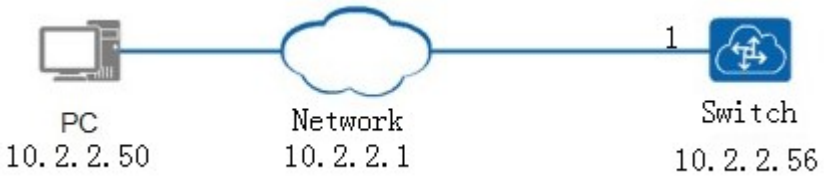
snmp-server name Switch

42. Example for System debugging configuration

42.1 Example for ping/traceroute

Networking requirements

As the following figure shows, the switch needs to know whether a host can reach and pass through the route;



Configuration thinking

The configuration thinking are as follows:

Set switch and network to share a network segment.

1.DUT ping pc;

2.DUT tracert pc;

Operating steps

Step1 Configure management interface ip .

Console(config)#interface vlan-interface 1

Console(config-if-vlanInterface-1)#ip address 192.150.100.1 255.255.255.0

This ipaddress will be the primary ipaddress of the interface.

Set successfully.

Console(config-if-vlanInterface-1)#exit

Step2 DUT ping PC。

Console(config)#ping 192.150.100.12

Pinging 192.150.100.12 (192.150.100.12) with 40 bytes of data:

Reply from 192.150.100.12 bytes=40 time=9ms ttl=128

Reply from 192.150.100.12 bytes=40 time=9ms ttl=128
Reply from 192.150.100.12 bytes=40 time=9ms ttl=128
Reply from 192.150.100.12 bytes=40 time=9ms ttl=128
Reply from 192.150.100.12 bytes=40 time=9ms ttl=128

--- 192.150.100.12 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4050 ms
rtt min/avg/max = 9/9/9 ms

Step3 DUT tracert PC
Console(config)#tracert 192.150.100.12
Tracing route to 192.150.100.12 [192.150.100.12]
over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 192.150.100.12

tracert complete.

Configuration file

Configuration file for Switch
Console(config)#show running-config if
![IF]
interface vlan-interface 1
ip address 192.150.100.1 255.255.255.0
exit

42.2 Example for Switch restart automatically

Networking requirements

As shown below, the switch restarts automatically at 08:00 every Friday night;

Configuration thinking

The configuration thinking are as follows:
Set switch automatic restart time and save configuration.

Operating steps

Step1 Configure switch automatic restart time at 08:00 on Friday evening

Console(config)#auto-reboot at 20:00:00 daily

Enable auto-reboot successfully.

Step2 Save configuration

Console(config)#exit

Console#copy running-config startup-config

Startup config in flash will be updated, are you sure(y/n)? [n]y

Building, please wait...

Update startup config successfully.

Step3 Verify configuration

Console#show auto-reboot

Auto-reboot setting

Type: durational

Time: 20:00:00 daily

Auto-reboot in 19 hours, 24 minutes and 32 seconds.

Configuration file

Configuration file for Switch

Console#show running-config oam

![OAM]

hostname Switch

exit

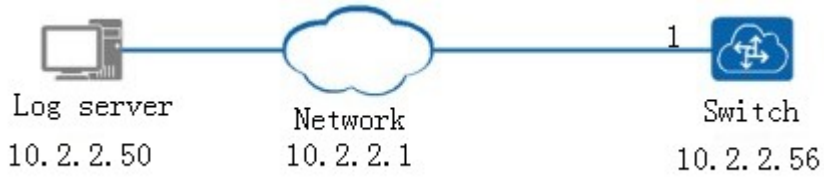
configure terminal

auto-reboot at 20:00:00 daily

42.3 Example for system log configuration

Networking requirements

As shown in the following figure, the IPv4 address of the switch log uploaded to the remote log server is 10.2.2.50.



Configuration thinking

The system log configuration thinking are as follows:

1.Configure management ip of switch.

2.Upload the configuration log to the log server;

Operating Steps

Step1 Configure management IP

Console(config)#interface vlan-interface 1

Console(config-if-vlanInterface-1)#ip address 10.2.2.56 255.255.255.0

Console(config-if-vlanInterface-1)#exit

Step2 Configure log server

Console(config)#logging 10.2.2.50

Console(config)#logging host 10.2.2.50

Step3 Verify configuration

Console(config)#show logging

state: on;

logging sequence-numbers: off;

logging timestamps: rfc5424;

logging language: english;

logging flash msg-number 100;

logging flash interval 30

logging monitor:

Console: state: off; display: on; 0 logged; 0 lost; 0 overflow.

logging buffered: state: on; 89 logged; 0 lost; 0 overflow.

logging flash: state: off; 0 logged; 0 lost; 0 overflow.

logging loghost:
logging facility: localuse7;logging source: off
192.150.100.13(514): state: on; 2 logged; 0 lost; 0 overflow.
logging SNMP Agent: state: off; 0 logged; 0 lost; 0 overflow.

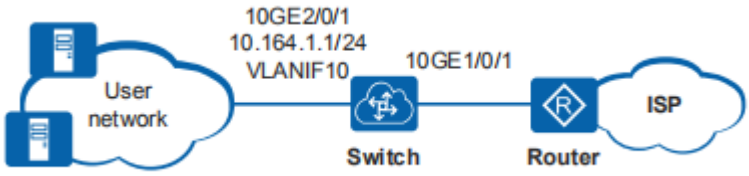
Configuration file

Console(config)#show running-config if syslog
![IF]
interface vlan-interface 1
ip address 192.150.100.1 255.255.255.0
exit
![SYSLOG]
logging 192.150.100.13

43. Example for URPF configuration

Networking requirement

As shown in the figure, the Switch is connected to the Internet Service Provider (ISP) router through 10GE1/0/1 and connected to the user network through 10GE2/0/1. An administrator wants the Switch to defend against source address spoofing attacks to prevent illegal users from using legitimate service requests and occupying too many service resources. As a result, legitimate users cannot receive service responses and cannot communicate normally.



Configuration thinking

Configure 10GE2/0/1 on the user side of the Switch to be added to a VLAN (Virtual Local Area Network) and configure URPF on the VLANIF interface so that the device can defend against user-side source address spoofing attacks.

Operating Steps

Step1 Configure the URPF check mode on the interface

```
Console(config)#interface vlan-interface 1
Console(config-if-vlanInterface-1)#ip address 10.164.1.1 255.255.255.0
Console(config-if-vlanInterface-1)#urpf strict
Console(config-if-vlanInterface-1)#exit
```

Step2 Verify configuration results

```
Console(config)#show urpf
Interface                URPF Status
VLAN-IF1                   Strict Mode
```

Configuration file

The configuration file of the Switch;
Console(config)#show running-config if urpf

```
![IF]
interface vlan-interface 1
ip address 10.164.1.1 255.255.255.0
exit
![URPF]
interface vlan-interface 1
urpf strict
exit
```

44. Example for User login configuration

44.1 Example of basic configuration after first login

Networking requirements

As shown below, after the terminal logs in to the switch for the first time, basic configuration of the switch is performed.

Configuration thinking

1.Log in to the switch through the command line terminal (console/ssh/telnet).
2.Basic configuration of the switch.

Operating steps

Step1 Login the switch.
Username(1-32 chars):admin
Password(1-16 chars):*****

Admin>enable

Note: The default user password for the neutral version is admin.

Step2 Basic configuration of the switch.
Set the date and time of the system
Admin#clock set 11:11:11 2018/05/05
Set clock successfully.
Clock will be reset to 2004/01/01 00:00:00 after system rebooting because there is no realtime clock chip.

#The configuration terminal does not time out.
Console#no timeout
Set the switch name
Admin#configure terminal

Admin(config)#hostname Switch
Set the maximum number of characters for a single line
Console(config)#line width 100

Set unsplit-screen display
Console(config)#no screen-rows per-page

Open display welcome message
Console(config)#banner

Do not allow the switch to be managed via the web
Console(config)#http disable
HTTP server is stopping...

HTTP server stopped successfully!

Step4 Verify configuration results.
Console(config)#show clock

Sat 2018/05/05 11:12:48 CCT 08:00

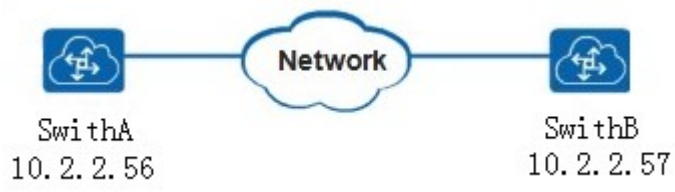
Configuration file

Configuration file for Switch
Console(config)#show running-config oam
![OAM]
banner
line width 100
hostname Switch
http enable
exit
no timeout
configure terminal

44.2 Example for Configuration Telnet login

Networking requirements

As shown below, two switches are connected through the network. SwitchB needs to be managed by SwitchA.



Configuration thinking

The configuration thinking are as follows:
Configure the Telnet-server function on SwitchB. SwitchA and SwitchB are on the same network segment.

Operating Steps

Step1 Check SwitchB Telnet-server function;
SwitchB(config)#show telnet
Telnet service port is 23, using port is 23, user limit is 5, current is 0.

#Set telnet client number is 2;
SwitchB(config)#telnet limit 2

#Set telnet client does not time out;
SwitchB(config)#no telnetclient timeout

Configuration the management IP address of SwitchB;
SwitchB(config)# interface vlan 1
SwitchB(config-if-vlanInterface-1)#ip address 10.2.2.57 255.255.255.0
This ipaddress will be the primary ipaddress of the interface.
Set successfully.

SwitchB(config-if-vlanInterface-1)#exit

Step2 Configure SwitchA

Configuration the management IP address of SwitchA;

SwitchA(config)# interface vlan 1
SwitchA(config-if-vlanInterface-1)#ip address 10.2.2.56 255.255.255.0
This ipaddress will be the primary ipaddress of the interface.
Set successfully.

SwitchA(config-if-vlanInterface-1)#exit

Step3 Verify configuration results.

Use the telnet command on SwitchA to telnet SwitchB.
SwitchA#telnet 10.2.2.57
Trying to connect to 10.2.2.57 ...
Connected to 10.2.2.57 successfully."Ctr+]" to exit.

Username(1-32 chars):

Note: 1. Use the quit command to return to the SwitchA command line.
2. The configuration of the telnet client does not need to be configured on the DUT. Default open, no close command.

Configuration file

Configuration file for SwitchA
SwitchA#show running-config if
![IF]
interface vlan-interface 1
ip address 10.2.2.56 255.255.255.0
exit

Configuration file for SwitchB
SwitchB(config)#show running-config oam
![OAM]
telnet limit 2
exit
configure terminal
no telnetclient timeout
![IF]
interface vlan-interface 1
ip address 10.2.2.57 255.255.255.0
exit

44.3 Example for configuration the SSH login

Networking requirements

As shown below, PC2 is connected to the Switch through the network, and the Switch needs to be managed through PC2 SSH, with a configured timeout of 120 minutes.

Configuration thinking

The configuration thinking are as follows:
Enable SSH server function on Switch, configure device management IP in the same network segment as PC2.

Operating steps

Step1 Open the Switch SSH function and configure a timeout of 120 minutes
#Activate using the default key
Console#crypto key generate rsa
Generate default SSH key successfully.
Console#crypto key refresh
Refresh SSH key successfully.
Console#configure terminal

#Open the SSH server function
Console(config)#ssh
Config SSH state successfully.

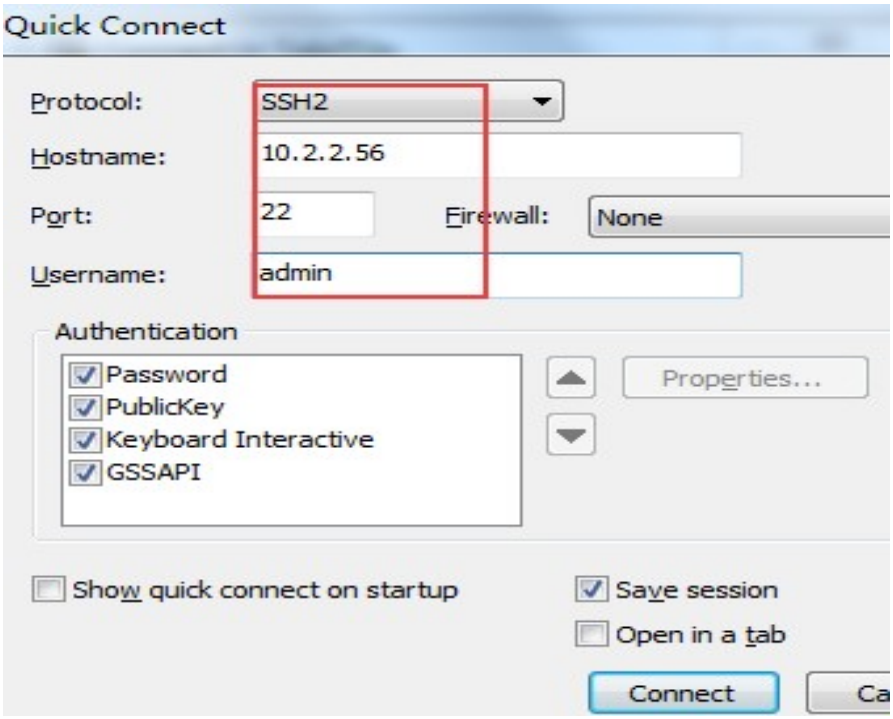
Step2 Configure management IP on Switch

#Configure Switch
Console(config)# interface vlan 1
Console(config-if-vlan1)# ip address 10.2.2.56 255.255.255.0
Console(config-if-vlan1)# exit

Step3 Verify configuration results.
#Check SSH server status
Console(config)#show ssh

ssh version : 2.0
ssh state : on
ssh key file : available

PC2 logs in to Switch using ssh on the CRT tool.



Configuration file

Configuration file for Switch
Console(config)#show running-config ssh

![SSH]
ssh

44.4 Example for the Console user interface Configuration

Networking requirements

The user needs to manage the DUT through the Console and modify the baud rate as needed. 115200 is used by default, and all users can use the console to manage the DUT by default.

Configuration thinking

Adapt Configure thinking as follows to the login device:
1. Configure the console baud rate is 9600;
2. Configure the user user_console to log in to the DUT through the console.

Operating Steps

Step1 Configure the console baud rate is 9600
Console#baud speed 9600
set console baud rate success, need to reboot taking effect !
#Check the console baud rate configuration
Console#show baud
current console baud rate is 115200, the setted speed is 9600 !

Step2
#Configure user user_console can’ t log in to the DUT through the console
Console(config)#username user_console terminal web telnet ssh

Configuration file

Configuration file for Switch
Console(config)#show running-config oam
![OAM]
username user_console privilege 0 password 0 guest
username user_console terminal web telnet ssh

Note: Baud configuration will not enter decompilation, write flash directly, no delete command, use baud speed 115200 to restore the default value;

44.5 Example for configure WEB login

Networking requirements

None

Configuration thinking

Adapt Configure thinking as follows to the login device:
1.Enable the http function so that the DUT can be managed via the web.

Operating Steps

Step1 Turn on http features
Console(config)#http enable
HTTP server is starting...

HTTP server started successfully!

Step2 Verify configuration results

Console(config)#show http

HTTP server information:
Current status: enable, TCP port: 80 (Default status: disable, TCP port: 80)

Configuration file

Configuration file for Switch
Console(config)#show running-config oam
![OAM]
http enable
exit

45. Example for User management configuration

Networking requirements

None

Configuration thinking

DUT has the default super user: switch / switch, which can be configured as follows:
1.Configure Guest priority user, username:user_guest, password:guest.
2.Configure Guest priority user, username:user_guest, password:user.
3.Configure Operator priority user, username:user_operator, password:operator.
4.Configure Manager priority user, username: User_manager. password: manager.
5.Configure user User_operator only login in console.
6. Configure user User_manager login error 5 times to enter silent time;

Operating steps

Step 1 Configure Guest priority user, username:user_guest, password:guest.
Console(config)# username user_guest privilege 0 password 0 guest
Console(config)#

Step 2 Configure Guest priority user, username:user_guest, password:user.
Console(config)# username User_user privilege 1 password 0 user
Console(config)#

Step 3 Configure Operator priority user, username:user_operator, password:operator.
Console(config)# username User_operator privilege 2 password 0 operator
Console(config)#

Step 4 Configure Manager priority user, username: User_manager. password: manager.
Console(config)# username User_manager privilege 15 password 0 manager
Console(config)#

Step 5 Configure user User_operator only login in console.
Console(config)#username User_operator terminal console
Console(config)#

Step 6 Configure user User_manager login error 5 times to enter silent time
Console(config)# username failmax User_manager 5
Console(config)#

Step 7 Verify configuration results.
Console(config)# show username
display user information
Terminal type: C=Console, T=Telnet, S=SSH, W=Web
Global Failmax: n/a

User Name	level	Role	Terminal	FailMax	Fail	OnLineMax	OnLine
Switch	15	Manager	CTSW	n/a	0	n/a	1
user_guest	0	Guest	CTSW	n/a	0	n/a	0
User_user	1	User	CTSW	n/a	0	n/a	0
User_operator	2	Operator	C	n/a	0	n/a	0
User_manager	15	Manager	CTSW	5	0	n/a	0

Configuration file

User managed profile:
Console#show running-config oam
![OAM]
username user_guest privilege 0 password 0 guest
username User_user privilege 1 password 0 user
username User_operator privilege 2 password 0 operator
username User_manager privilege 15 password 0 manager
username User_operator terminal console
username failmax User_manager 5

46. Example for VCT detection configuration

Networking requirement

The cable detection uses the virtual cable to detect the VCT technology, and uses the time domain reflection TDR (Time Domain Reflectometry) to detect the cable state. When the pulse signal is transmitted in the cable, some energy will be reflected if it meets the end of the cable or other fault points. This phenomenon is called time domain reflection. The VCT algorithm measures the time of the pulse transmission in the cable, the fault point and the return time, and converts the measured time to the distance.
As shown in the following figure, disconnect the Switch B port 1 network line and use VCT on Switch A

Configuration thinking

Tips to configure VCT function:
1. Disconnect the Switch B port 1 network
2. VCT detection on port 1 of Switch A
3. Connect the network line of Switch B port 1
4. VCT detection on port 1 of Switch A

Operating steps

Step 1 Disconnect the Switch B's port 1 net;

Step 2 VCT detection at port 1 of Switch A;
Console(config)#interface ethernet 0/0/1
Console(config-if-ethernet-0/0/1)#vct run

Port ethernet 0/0/1 VCT result :

	pair1	pair2	pair3	pair4
status :	OPEN	OPEN	OPEN	OPEN
locate :	0	0	0	0

From the above information, we can see that the link of Switch A is disconnected,

Step 3 Connect the Switch B port 1 network line;

Step 4 VCT detection on port 1 of Switch A;

```
Console(config-if-ethernet-0/0/1)#vct run
Port ethernet 0/0/1 VCT result :
                    pair1          pair2          pair3          pair4
status    :       NORMAL         NORMAL         NORMAL         NORMAL
locate    :          _              _              _              _
```

As you can see from the information above, the link of the Switch A works normally.

Configuration file

Configuring file of the Switch.
The commands detected by the VCT do not exist in the decompile.