

DCN

Switch Configuration Training

Contents

01 Introduction to O&M

02 Common Network

03 Common IP Service

04 Multicast

05 QinQ

01

Introduction to O&M

Introduction to O&M - VLAN

VLAN Basic Operation: Create VLAN 10-20,24. Set 1/0/24 interface trunk mode, set 1/0/23 interface to access VLAN 20, then delete VLAN 19

```
Switch(config)#vlan 10-20: 24
Switch(config-if-ethernet1/0/24)#switchport mode trunk
Switch(config-if-ethernet1/0/24)#switchport trunk allowed vlan 10-20: 24
Switch(config-if-ethernet1/0/23)#switchport mode access'
Switch(config-if-ethernet1/0/23)#switchport access vlan 20
Switch(config)#no vlan 19
Switch#show vlan
```

VLAN Name	Type	Media	Ports
10	VLAN0010	Static	ENET Ethernet1/0/24(T)
11	VLAN0011	Static	ENET Ethernet1/0/24(T)
12	VLAN0012	Static	ENET Ethernet1/0/24(T)
13	VLAN0013	Static	ENET Ethernet1/0/24(T)
14	VLAN0014	Static	ENET Ethernet1/0/24(T)
15	VLAN0015	Static	ENET Ethernet1/0/24(T)
16	VLAN0016	Static	ENET Ethernet1/0/24(T)
17	VLAN0017	Static	ENET Ethernet1/0/24(T)
18	VLAN0018	Static	ENET Ethernet1/0/24(T)
20	VLAN0020	Static	ENET Ethernet1/0/23 Ethernet1/0/24(T)
24	VLAN0024	Static	ENET Ethernet1/0/24(T)

Show VLAN:

show current VLAN created on the device and the relationship with interfaces

Show VLAN brief:

only show current VLAN on the device

Introduction to O&M - MAC & ARP

MAC+IP+ARP: Create static MAC entry, configure IP address for VLAN1 SVI interface. PC connected to the Eth15, PC ping switch, then check ARP table, delete static MAC.

```
Switch(config)#mac-address-table static address 00-00-00-00-00-01 vlan 1
interface ethernet 1/0/1
Switch#show mac-address-table
Read mac address table....
Vlan Mac Address                Type    Creator    Ports
-----
1    00-00-00-00-00-01            STATIC  User       Ethernet1/0/1
1    00-03-0f-92-79-3e            STATIC  System     CPU
1    38-f3-ab-89-89-20            DYNAMIC Hardware Ethernet1/0/15
Switch(config-if-vlan1)#ip add 150.1.1.254 255.255.255.0
Switch#show ip int b
Index    Interface    IP-Address    Protocol
1254     Ethernet0    unassigned    down
11001    Vlan1        150.1.1.254    up
17500    Loopback     127.0.0.1      up
Switch#show arp
ARP Unicast Items: 1, Valid: 1, Matched: 1, Verifying: 0, Incomplete: 0, Failed: 0, None: 0
Ethernet Manager Port ARP Items: 0
Address    Hardware Addr Interface    Port    Flag    Age-time(sec)  subvlanVID
150.1.1.1  38-f3-ab-89-89-20 Vlan1       Ethernet1/0/15 Dynamic 1199          1
Switch(config)#no mac-address-table static address 00-00-00-00-00-01 interface
ethernet 1/0/1
```

show mac-address-table:

to check current MAC address type and the corresponding interface

Show ip int brief:

to check L3 interface address and status (up/down)

Introduction to O&M - Static Routing

Static Routing: Create static route and default route, show route table, then delete static route

```
Switch(config)#ip route 155.1.1.0 255.255.255.0 150.1.1.1↵
Switch(config)#ip route 0.0.0.0 0.0.0.0 150.1.1.1 ↵
Switch(config)#show ip route ↵
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP↵
       O - OSPF, IA - OSPF inter area↵
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2↵
       E1 - OSPF external type 1, E2 - OSPF external type 2↵
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area↵
       * - candidate default↵
↵
Gateway of last resort is 150.1.1.1 to network 0.0.0.0↵
↵
S*      0.0.0.0/0 [1/0] via 150.1.1.1, Vlan1 tag:0↵
C       127.0.0.0/8 is directly connected, Loopback tag:0↵
C       150.1.1.0/24 is directly connected, Vlan1 tag:0↵
S       155.1.1.0/24 [1/0] via 150.1.1.1, Vlan1 tag:0↵
Total routes are : 4 item(s)↵
Switch(config)#no ip route 155.1.1.0 255.255.255.0 150.1.1.1↵
```

show ip route: show all routing entries that take effect on the current device

Show ip route static: show the static routing entries that take effect on the current device

Switch System Files

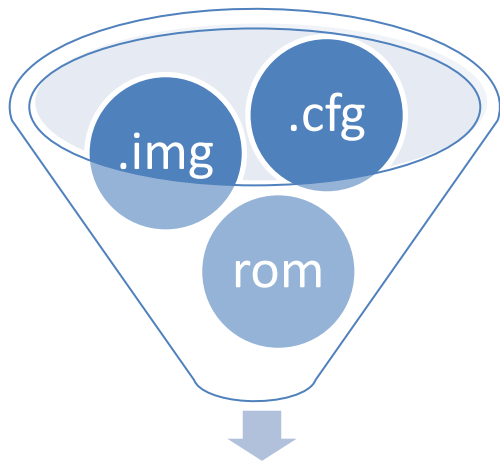
boot.rom

nos.img

Vendor.cfg

Switch software version upgrade is to update these three types of files. The method is to overwrite old files with new files.

Introduction to O&M - File System



Check if it exists nand flash:

```
Switch#dir all
-rw-      600.8K      ic.log
-rw-      1.8K       startup.cfg
-rw-      177        vsf.cfg
-rw-      2.1K       vsf_startup.cfg

Drive : flash:
Size:30.5M  Used:528.0K  Available:30.0M  Use:2%

-rw-      36.1M       nos.img

Drive : nandflash:
Size:113.8M  Used:36.2M  Available:72.8M  Use:33%
Switch#
```

To check and modify the boot item:

```
Switch#show boot-files
The primary img file at the next boot time:  nandflash:/nos.img
The backup img file at the next boot time:  nandflash:/backup.img
Current booted img file:                    nandflash:/nos.img

Repair primary img by backup img:           yes

The startup-config file at the next boot time:  flash:/vsf_startup.cfg
Current booted startup-config file:            flash:/vsf_startup.cfg
Switch#boot img nandflash:/nos.img primary
```


Img mode, single unit upgrade

Method 1: ftp upgrade

```
Switch#copy ftp: //usernamepassword@server ip/xxx nos.img nos.img
```

```
Switch#copy ftp: //usernamepassword@server ip/xxx nos.img nandflash: /nos.img
```

Method 2: tftp upgrade

```
Switch#copy tftp: //server ip/xxx nos.img nos.img
```

```
Switch#copy tftp: //server ip/xxx nos.img nandflash: /nos.img
```

Notes:

1. running tftp tool, package upload to tftp dir
2. PC could ping switch successfully
3. Disable Defender and virus software

VSF devices upgrade

Step 1. Master upgrade

```
Switch#copy tftp: //server ip/xxx nos.img nos.img
```

Step 2. Slave upgrade

```
Switch#copy tftp: //server ip/xxx nos.img member-2#nos.img
```

Step 3. Reboot

Introduction to O&M - Boot mode upgrade

Boot mode, single unit upgrade

Step 1. Press "Ctrl+b" when reboot to enter boot mode, set IP address

```
[Boot]: setconfig
Host IP Address: [10.1.1.1] 150.1.1.2
Server IP Address: [10.1.1.2] 150.1.1.1
[Boot]: ping 150.1.1.1
Using rtl8390#0 device
host 150.1.1.1 is alive
```

Step 2. Upgrade boot.rom, then run nos.img

```
[Boot]: load boot.rom
[Boot]: write boot.rom
[Boot]: run tftp:xxxx_nos.img
```

Step 3. In Img mode, upgrade nos.img

```
Switch#copy tftp: //server_ip/xxx_nos.img nos.img
```

Notes:

1. For 5750E series, some old model could directly write nos.img in boot mode.
2. Using MGMT interface (boot mode), using Ethernet port if there is no MGMT port.

Introduction to O&M - Xmodem Upgrade

Unable enter into boot mode, could try Xmode upgrade by console port, no need MGMT or Ethernet port

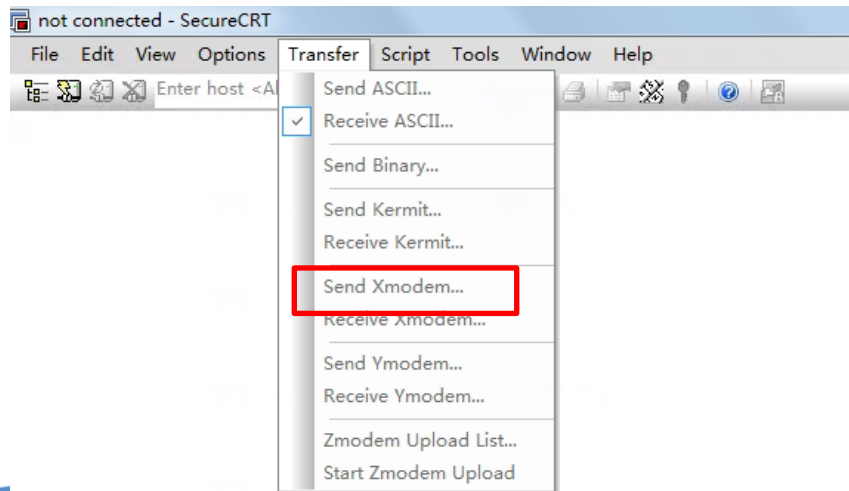
1. Set baudrate and enter xmode

```
[Boot]: baudrate 115200
```

```
[Boot]: xmode
```

2. Transfer version file by secure

3. Write boot.rom and reboot

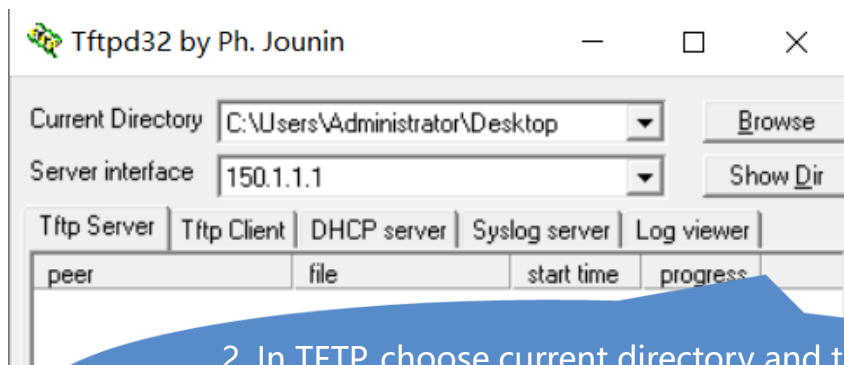
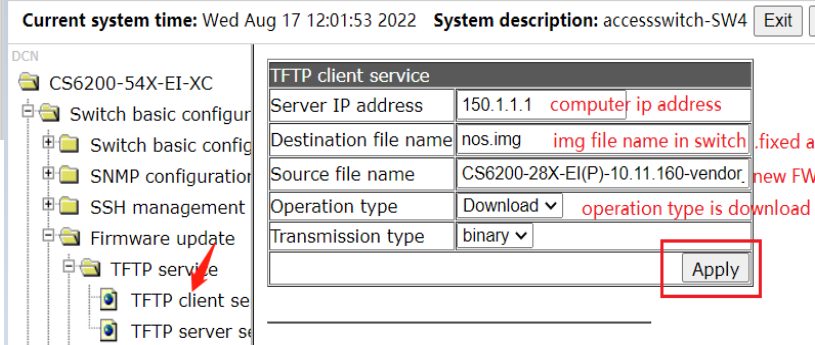
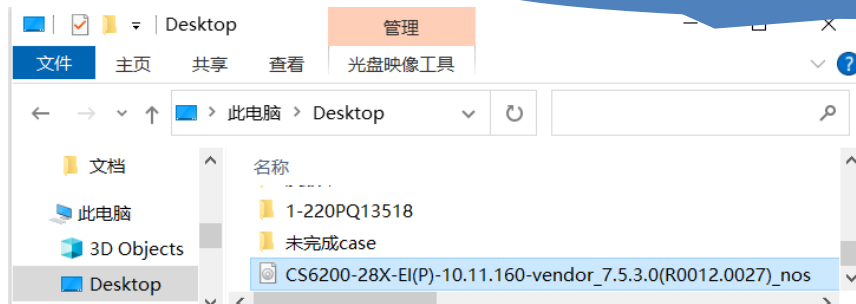


Notes:

Need to reconnect after change the baudrate

Introduction to O&M - WEB Upgrade

1. Download file to local directory



2. In TFTP, choose current directory and the server interface(wired network adapter address)

3. Login switch on Web, fill in the corresponding parameters according to the picture, then apply and reboot

Introduction to O&M - X86 Switch Upgrade

X86 switch upgrade in onie mode

Step 1. When restarting the device select the down arrow to enter the ONIE menu

GNU GRUB version 2.02~beta2+e4a1fe391

```
+-----+  
|nos.img|  
|* ONIE |  
|       |  
|       |  
|       |  
|       |  
+-----+
```

Introduction to O&M - X86 Switch Upgrade

Step 2. Choose "Install OS"

```
GNU GRUB  version 2.02~beta2+e4a1fe391↵
+-----+↵
|*ONIE: Install OS          |↵
| ONIE: Rescue              |↵
| ONIE: Uninstall OS       |↵
| ONIE: Update ONIE        |↵
| ONIE: Embed ONIE         |↵
|                           |↵
|                           |↵
|                           |↵
|                           |↵
+-----+↵
```

Introduction to O&M - X86 Switch Upgrade

Step 3. Upgrade and reboot

```
ONIE: / # onie-discovery-stop  
ONIE: / # ifconfig eth0 192.168.1.2  
ONIE: / # ping 192.168.1.1ePING 172.17.3.200 (172.17.3.200): 56 data bytes  
64 bvtes from 172.17.3.200: seg=0 ttl=64 time=3.184 ms  
64 bytes from 172.17.3.200: seg=1 ttl=64 time=1.044 ms  
ONE: / # onie-nos-install tfp: //172.17.3.220/Switch-10.14.178-vendor 7.3.3.0R0006.0116))  
nos.onic
```

X86 switch will generate two version files after
compiling: nos.img & nos.onie

Introduction to O&M - Upgrade trouble shooting

Copy is ok, error occurred when write, or shows timeout:

The possible reason is flash memory, delete some contents or directly upgrade it in nand flash to check it again.

```
#####
File transfer complete.
Recv total 17594702 bytes

Begin to write local file, please wait...
Write file "flash:/S5750E.img" error(Error:ERROR)!
close tftp client.
show version
S5750E-16F-SI-R Device, Compiled on Apr 30 15:33:17 2020
sysLocation China
CPU Mac 00:03:0f:d2:2a:76
Vlan MAC 00:03:0f:d2:2a:75
SoftWare Package Version 7.5.3.2(R0004.0256)
BootRom Version 7.5.25
HardWare Version 1.0.1
CPLD Version 1.04
Serial No.:SW074510JC14000071
Copyright (C) 2001-2020 by DC YunKe Networks Co.,Ltd.
All rights reserved
Last reboot is cold reset.
Uptime is 0 weeks, 0 days, 0 hours, 15 minutes
RC-core-1E-229#f
```

Introduction to O&M - Upgrade trouble shooting

It shows "recv signal 11,tid 34" when booting the switch, the switch cannot boot successfully

Plz help try " [Boot]: format flash: /" to resolve it.

```
Bytes transferred = 13790886 (d26ea6 hex)
## Booting kernel from Legacy Image at 81000100 ...
Image Name:
Created:      2022-02-14   1:08:32 UTC
Image Type:   MIPS Linux Kernel Image (gzip compressed)
Data Size:    13745207 Bytes = 13.1 MiB
Load Address: 80000000
Entry Point:  80003710
Verifying Checksum ... OK
Uncompressing Kernel Image ... OK
```

```
Starting kernel ...
recv signal 11, tid 34
```

Introduction to O&M - Upgrade trouble shooting

It shows “flash/filed: no such device” when upgrade the device
This is because the flash loading failed, the revised new device has replaced flash, and the old version cannot be recognized by flash.
That is to say, do not use the old version for new equipment.

```
omount: mounting /dev/mtdblock3 on /mnt/flash/ failed: No such device
mount: mounting /dev/mtdblock2 on /mnt/flash1/ failed: No such device
open /dev/mtd1 faiopen /dev/mtd1 fai
gpio init fail: -1!Can't get device type!!!
```

Introduction to O&M - Multi .cfg files management

1. Copy "startup.cfg" into new file "backup.cfg"

```
sw4#dir
-rw-      2.1K      backup.cfg
-rw-      1.0M      boot1.rom
-rw-     21.7M      nos.img
-rw-      2.1K      startup.cfg

Drive : flash:
Size:29.0M  Used:23.1M  Available:5.9M  Use:80%
sw4#rename backup.cfg rebackup.cfg
Rename backup.cfg to rebackup.cfg ok!
sw4#dir
-rw-      1.0M      boot1.rom
-rw-     21.7M      nos.img
-rw-      2.1K      rebackup.cfg
-rw-      2.1K      startup.cfg

Drive : flash:
Size:29.0M  Used:23.1M  Available:5.9M  Use:80%
sw4#
```

```
sw4#dir
-rw-      1.0M      boot1.rom
-rw-     21.7M      nos.img
-rw-      2.1K      startup.cfg

Drive : flash:
Size:29.0M  Used:23.1M  Available:5.9M  Use:80%
sw4#copy startup.cfg backup.cfg
Write ok.
sw4#dir
-rw-      2.1K      backup.cfg
-rw-      1.0M      boot1.rom
-rw-     21.7M      nos.img
-rw-      2.1K      startup.cfg

Drive : flash:
Size:29.0M  Used:23.1M  Available:5.9M  Use:80%
sw4#
```

2. Rename file: backup.cfg
-> rebackup.cfg

Introduction to O&M - Multi .cfg files management

```
sw4#dir all
-rw-      1.0M      boot1.rom
-rw-     21.7M      nos.img
-rw-      2.1K      rebackup.cfg
-rw-      2.1K      startup.cfg
Drive : flash:
Size:29.0M  Used:23.1M  Available:5.9M  Use:80%
-rw-      21.8M      AVPro.img
-rw-      21.7M      DCN-CS6200-8G24S2Q-EI.img
-rw-      4.5K      startup_b.cfg
-rw-      1.3M      sys.log
Drive : nandflash:
Size:110.1M  Used:42.5M  Available:62.8M  Use:40%
```

```
sw4#pwd
flash:/
sw4#
```

```
sw4(config)#no load running-config
sw4(config)#load running-config from tftp://150.1.1.3/quad.cfg
sw4(config)#Begin to receive file, please wait...

File transfer complete.
Loading running-config ...
Loading running-config end

sw4(config)#
```

cd nandflash: /

Change the current directory
to "nandflash: /" !

sw4#cd flash: /

Change the current directory to
"flash: /" ! (default is flash)

Introduction to O&M - Multi .cfg files management

sw4#show boot-files

The primary img file at the next boot time: flash:/nos.img

The backup img file at the next boot time: flash:/nos.img

Current booted img file: flash:/nos.img hootoe

The startup-config file at the next boot time: flash:/startup.cfg

Current booted startup-config file: flash://startup.cfg

sw4#boot img DCN_CS6200_8G24S2Q-El.img primary

nandflash/DCN_CS6200_8G24S2Q-El.img will be used as the primary img file at the next time!

sw4#boot img DCN.img backup

nandFlash./DCN.img will be used as the backup mg le at the next time!

sw4#boot startup-config rebackup.cfg

rebackup.cfg is not existing

sw4#boot startup-config flash:/rebackup.cfg

flash:/rebackup.cfg will be used as the startup-config file at the next time!

sw4#show boot-files

The primary img file at the next boot time: nandflash://CN-CS6200-8G24S2Q-El.img

The backup img g file at the next boot time: nandflash:/DCN.img

Current booted img file: flash:/nos.img

The startup-config file at the next boot time: flash:/rebackup.cfg

Current booted startup-config file: flash:/startup.cfg

Change the boot item: boot img/startup.cfg filename

Switch could store 2 img files as start file, one is primary while the other is backup.

There is only one configuration file can be used as starting configurations.

The first parameter of the user level is for the mode. If you want to control the command line level under a certain mode, you must first upgrade the commands in this mode to level 15.

Step 1. Upgrade the mode level to 15, such as config, exec mode.

Step 2. Configure the command level under the certain mode.



Introduction to O&M - Multi user level

Application 1: Only above Level 3 users could use OSPF

Command:

```
!  
privilege exec level 15 all  
privilege config level 15 all  
privilege exec level 3 configure  
privilege config level 3 router ospf  
!
```

To check vty 3 level
user login info

```
150.1.1.253  
login:test  
Password:****  
CS6200-8G24S2Q-EI>?  
Exec commands:  
  configure  Enter configuration mode  
  enable    Turn on privileged mode command  
  exit      End current mode and down to previous mode  
  help      Description of the interactive help system  
  
CS6200-8G24S2Q-EI>configure  
The CONFIG mode is locked by other user, now only one user can login!  
CS6200-8G24S2Q-EI>configure  
CS6200-8G24S2Q-EI(config)>?  
Configure commands:  
  end      End current mode and change to EXEC mode  
  exit     End current mode and down to previous mode  
  help     Description of the interactive help system  
  router   Enable a routing process  
  
CS6200-8G24S2Q-EI(config)>router ?  
  ospf    Open Shortest Path First (OSPF)  
  
CS6200-8G24S2Q-EI(config)>router ospf ?  
  <cr>  
  
CS6200-8G24S2Q-EI(config)>router ospf  
CS6200-8G24S2Q-EI(config-router)>■
```


Introduction to O&M - Multi user level

Application 2: Only above Level 13 users could enter enable

Command:

privilege exec level 15 all

privilege exec level 13 enable

Level 3 user-test, login switch

```
150.1.1.253
login:test
Password:****
CS6200-8G24S2Q-EI>?
Exec commands:
  exit  结束当前模式并返回上一次模式
  help  交互系统描述
CS6200-8G24S2Q-EI>
```

Level 14 user-test1, login switch

```
login:test1
Password:*****
CS6200-8G24S2Q-EI>?
Exec commands:
  enable  打开特权模式命令
  exit    结束当前模式并返回上一次模式
  help    交互系统描述
CS6200-8G24S2Q-EI>
```

Introduction to O&M - Log introduction

The system log is to record the changes of the system in real time

Switch Log
example



```
76 %Jan 01 19:10:29:241 2006 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin login successfully from 150.1.1.3:65067.
75 %Jan 01 19:10:23:152 2006 <warnings> DEFAULT[tIPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP
74 %Jan 01 19:10:22:156 2006 <warnings> MODULE_PORT[tphyDaemon]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1, changed state to UP
73 %Jan 01 04:34:24:659 2006 <warnings> DEFAULT[tIPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to DOWN
72 %Jan 01 04:34:23:659 2006 <warnings> MODULE_PORT[tphyDaemon]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1, changed state to DOWN
71 %Jan 01 04:08:50:619 2006 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin logout from 150.1.1.3:54365.
70 %Jan 01 03:45:12:098 2006 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin login successfully from 150.1.1.3:54365.
69 %Jan 01 02:39:45:458 2006 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin logout from 150.1.1.3:53279.
68 %Jan 01 02:29:37:336 2006 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin login successfully from 150.1.1.3:53279.
67 %Jan 01 02:04:14:675 2006 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin logout from 150.1.1.3:52735.
66 %Jan 01 01:51:25:277 2006 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin login successfully from 150.1.1.3:52735.
65 %Jan 01 00:20:28:709 2006 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin logout from 150.1.1.3:51287.
```

Introduction to O&M - Log introduction

There are two methods to achieve log feature:

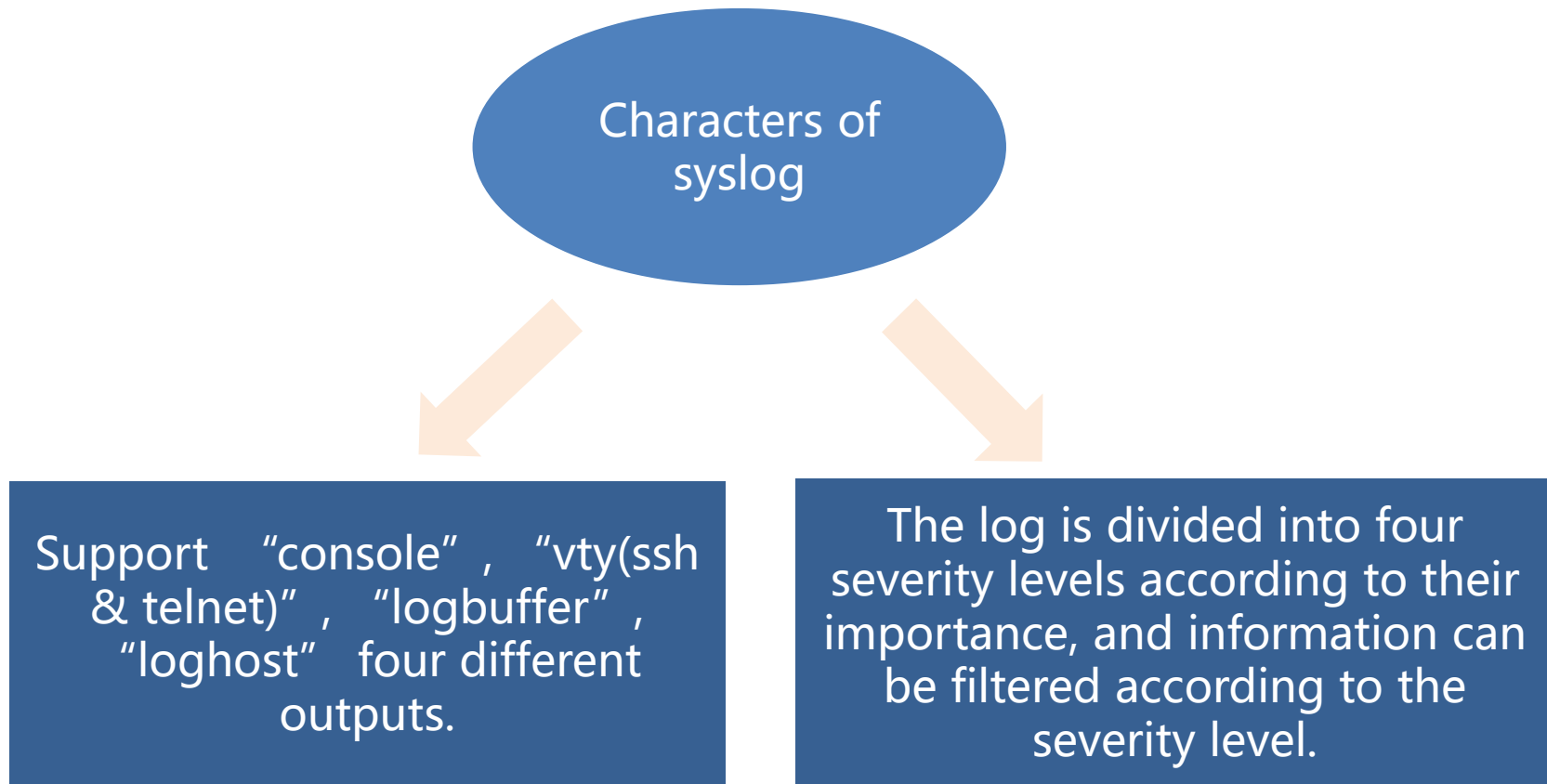
Syslog :

Model: S4600/S5750E-26X-SI/CS6200-8G24S2Q-EI

Command: show logging buffered level warnings

Info-center :

Model: S4600-28X-SI/S5750EV2/CS6200V2/CS65 series



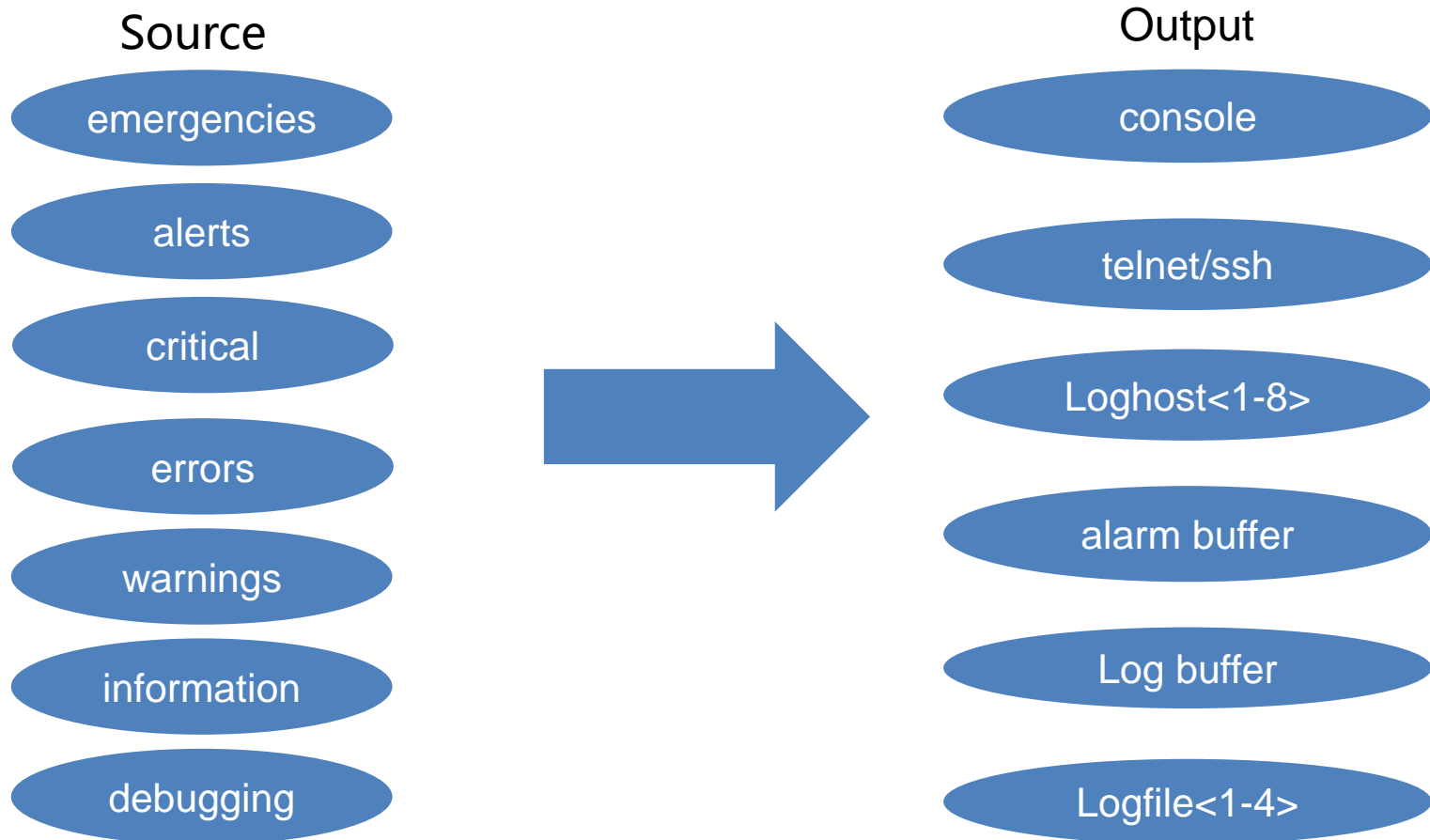
There are four different severity log info:

- Device reboot, task error and so on are "critical 2" .
- Interface up/down switchover, change of topology, trunk port state change...belong to "warning 4" .
- The Output info which is generated by entering commands in CLI is "informational 6" .
- The level of information output by the CLI configuration command debug switch is "debugging 7" .

Introduction to O&M - Different log severity


Severity	Value	Description
emergencies	0	System is unusable
alerts	1	Action must be taken immediately
critical	2	Critical conditions
errors	3	Error conditions
warnings	4	Warning conditions
notifications	5	Normal but significant condition
informational	6	Informational messages
debugging	7	Debug-level messages

Introduction to O&M - info-center



Introduction to O&M - Different log severity

```
S5750E-52F-SI-R#show info-center config
info-center enable
info-center sync enable
info-center console output-enable
info-center monitor output-enable
info-center trapbuffer output-enable
info-center logbuffer output-enable
info-center logfile 4 config count 40960 flash logfile.log
info-center logfile 4 output-enable
info-center console match level debugging
info-center console prefix on
info-center monitor match level debugging
info-center monitor prefix on
info-center trapbuffer prefix on
info-center logbuffer match level warnings
info-center logbuffer prefix on
info-center loghost 1 prefix on
info-center loghost 2 prefix on
info-center loghost 3 prefix on
info-center loghost 4 prefix on
info-center loghost 5 prefix on
info-center loghost 6 prefix on
info-center loghost 7 prefix on
info-center loghost 8 prefix on
info-center logfile 1 prefix on
info-center logfile 2 prefix on
info-center logfile 3 prefix on
info-center logfile 4 match level warnings
info-center logfile 4 prefix on
```



show info-center config:
shows default switch info-center configuration, we could add configuration according to our need based on the default configuration.

Introduction to O&M - Syslog configuration

Configuring to output "debugging" level log and upload it to syslog server

Command:

```
S4600-28P-SI(config)#logging 150.1.1.3 facility local0 level debugging
```

```
S4600-28P-SI(config)#logging loghost sequence-number
```

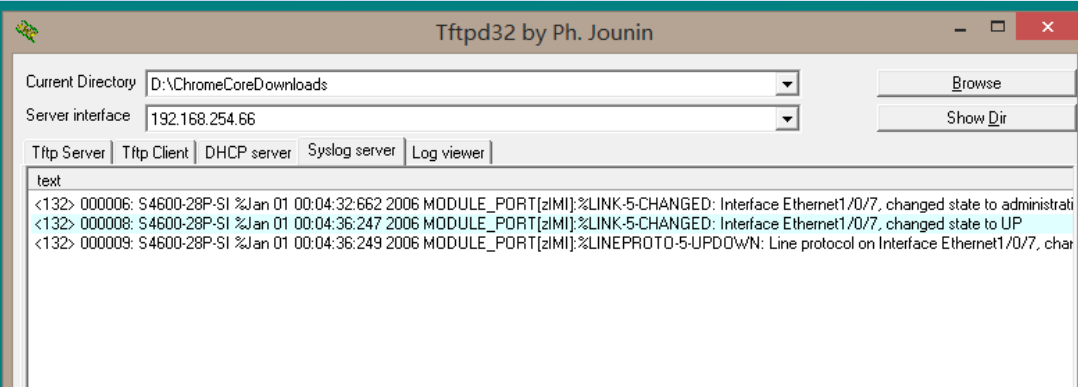
(This command adds a sequence number to the logs sent to the log host)

Tftp as syslog server

Result:

```
% Unrecognized command
S4600-28P-SI(config-if-ethernet1/0/5)#exi
S4600-28P-SI(config)#logging 150.1.1.3 facility local0 level ?
critical          critical level(2)
debugging         debugging level(7)
informational     informational level(6)
warnings          warnings level(4)

S4600-28P-SI(config)#logging 150.1.1.3 facility local0 level debugging
S4600-28P-SI(config)#log
logging          login
S4600-28P-SI(config)#
S4600-28P-SI(config)#
S4600-28P-SI(config)#
S4600-28P-SI(config)#
S4600-28P-SI(config)#logging 150.1.1.3 facility local0 level debugging
S4600-28P-SI(config)#logging loghost sequence-number
S4600-28P-SI(config)#int ethernet 1/0/7
S4600-28P-SI(config-if-ethernet1/0/7)#shutdown
S4600-28P-SI(config-if-ethernet1/0/7)#no shutdown
S4600-28P-SI(config-if-ethernet1/0/7)#
```



Introduction to O&M – Syslog configuration

View the logs of the logging buffer on the switch and configure different log levels


Command:

logging flash level critical

The configured level is 2, "show logging buffer" only shows logs with level 2, but the total entries in SDRAM are 3

Notes: If no level configured, default is critical level(2)

Result:



```
s4600-28P-SI(config)#show logging buffered
Current messages in SDRAM:3

s4600-28P-SI(config)#show logging buffered level warnings
Current messages in SDRAM:3

3 %Jan 01 00:50:01:619 2006 <warnings> MODULE_PORT[zIMI]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/2, changed state
2 %Jan 01 00:50:01:617 2006 <warnings> MODULE_PORT[zIMI]:%LINK-5-CHANGED: Interface Ethernet1/0/2, changed state to UP
1 %Jan 01 00:49:59:131 2006 <warnings> MODULE_PORT[zIMI]:%LINK-5-CHANGED: Interface Ethernet1/0/2, changed state to administratively D
s4600-28P-SI(config)#show logging buffered level critical
Current messages in SDRAM:3
```

Introduction to O&M – Syslog configuration

Recording user commands to syslog on the switch or log host

Command:

```
S4600-28P-SI(config)#logging executed-commands enable (disable)
```

```
S4600-28P-SI(config)#logging 150.1.1.3 facility local0 level warnings
```

```
S4600-28P-SI(config)#logging 150.1.1.3 transport udp port <1-65535>
```

Result:

```
S4600-28P-SI#show logging buffered
Current messages in SDRAM:24
24 %Jan 01 01:05:57:698 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, show running-config
22 %Jan 01 01:05:54:463 2006 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 2093: FS_DEV_UNLOCK slot: 1 dev_name:flash: file_name:flash:/startup.cfg
21 %Jan 01 01:05:54:405 2006 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 2075: FS_DEV_LOCK_NO_WAIT slot: 1 dev_name:flash: file_name:flash:/startup.cfg
20 %Jan 01 01:05:52:363 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, write
19 %Jan 01 01:05:41:124 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, exit
18 %Jan 01 01:05:18:561 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, logging 150.1.1.3 facility local0 level critical
17 %Jan 01 01:03:51:166 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, conf
16 %Jan 01 01:02:55:347 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, exit
15 %Jan 01 01:02:49:276 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, logging 150.1.1.3 facility local0 level warnings
14 %Jan 01 01:02:14:539 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, conf
13 %Jan 01 01:00:33:330 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, show logging buffered
12 %Jan 01 01:00:25:218 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, logging flash level critical
11 %Jan 01 01:00:17:261 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, conf
10 %Jan 01 00:59:49:438 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, show running-config
```

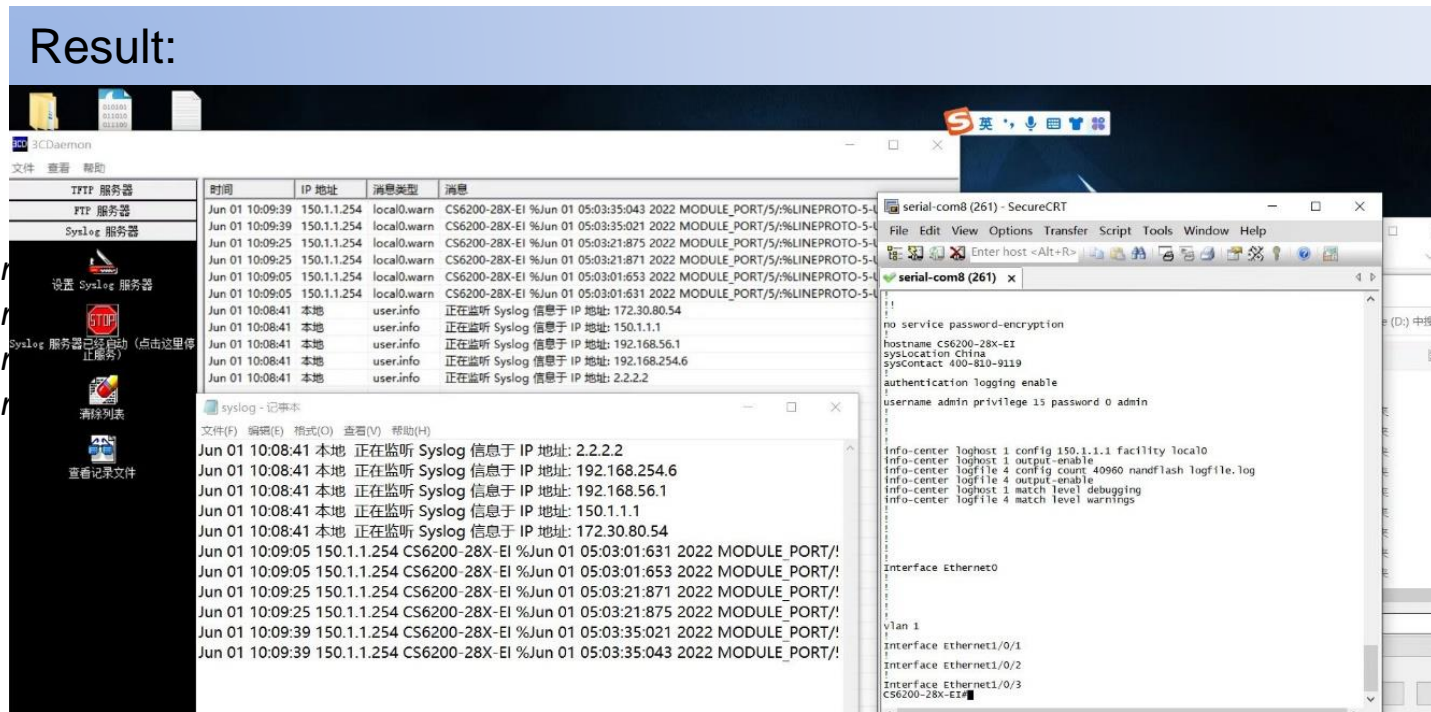
Introduction to O&M - info-center configuration

Configure the log output level as debugging to be uploaded to the syslog server

Result:

Command:

`Switch(config)#info-center`
`Switch(config)#info-center`
`Switch(config)#info-center`
`Switch(config)#info-center`



Introduction to O&M - info-center configuration

Recording user commands to syslog on the switch or log host

Command:

Switch(config)#info-center logbuffer output-enable

Switch(config)#info-center logbuffer record-cmd

```
S4600-28P-SI#show logging buffered  
Current messages in SDRAM:24
```

```
24 %Jan 01 01:05:57:698 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, show running-config  
22 %Jan 01 01:05:54:463 2006 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 2093: FS_DEV_UNLOCK slot: 1 dev_name:flash: file_name:flash:/s1  
21 %Jan 01 01:05:54:405 2006 <critical> MODULE_UTILS_FILESYSTEM[zIMI]:fs_write_file 2075: FS_DEV_LOCK_NO_WAIT slot: 1 dev_name:flash: file_name:flash:/startup.c  
20 %Jan 01 01:05:52:363 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, write  
19 %Jan 01 01:05:41:124 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, exit  
18 %Jan 01 01:05:18:561 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, logging 150.1.1.3 facility local0 level critical  
17 %Jan 01 01:03:51:166 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, conf  
16 %Jan 01 01:02:55:347 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, exit  
15 %Jan 01 01:02:49:276 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, logging 150.1.1.3 facility local0 level warnings  
14 %Jan 01 01:02:14:539 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, conf  
13 %Jan 01 01:00:33:330 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, show logging buffered  
12 %Jan 01 01:00:25:218 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, logging flash level critical  
11 %Jan 01 01:00:17:261 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, conf  
10 %Jan 01 00:59:49:438 2006 <critical> DEFAULT[zIMI]:[Telnet/SSH] admin@150.1.1.3:64696, show running-config
```

```
S4600-28X-SI(config)#info-center loghost 1 config 1.1.1.1 facility local0 transport udp port ?  
<1-65535> <1-65535> Port number
```

```
S4600-28X-SI(config)#info-center loghost 1 config 1.1.1.1 facility local0 transport udp port
```

Introduction to O&M - ACL

Standard ACL

```
switch(config)#access-list ?
<1-99> IP standard access list <1-99>
<100-199> IP extended access list <100-199>
<1100-1199> MAC extended access list <1100-1199>
<200-299> IP extended access list(support discontinuous ip address mask)<200-299>
<3100-3199> MAC-IP extended access list <3100-3199>
<3200-3299> MAC-IP extended access list(support discontinuous ip address
mask) <3200-3299>
<5000-5099> Multicast source control access list <5000-5099>
<6000-7999> Multicast destination control access list <6000-7999>
<700-799> MAC standard access list <700-799>
```

IP-ACL

```
switch(config)#ip access-list ?
extended Extended Access List
standard Standard Access List
```

```
switch(config-ip-ext-nacl-test)#permit ?
<0-255> An IP protocol number <0-255>
eigrp Cisco's EIGRP routing protocol
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
igmp Internet Group Management Protocol
igrp Cisco's IGRP routing protocol
ip Any Internet Protocol
ipinip IP in IP tunneling
ospf OSPF routing protocol
tcp Transfer Control Protocol
udp User Datagram Protocol
```

VLAN-ACL

Use the commands of Standard and IP ACL to match the traffic, apply it to VLAN, and apply traditional ACL to ports

```
ip access-list extended test
permit ip any-source host-destination 1.1.1.1
exit
!
vACL ip access-group test in vlan 1
```

User defined ACL

Used when matching message fields exactly

```
switch2(config)#userdefined-access-list standard offset ?
window1 Specify window1(2bytes)
window10 Specify window10(2bytes)
window11 Specify window11(2bytes)
window12 Specify window12(2bytes)
window2 Specify window2(2bytes)
window3 Specify window3(2bytes)
window4 Specify window4(2bytes)
window5 Specify window5(2bytes)
window6 Specify window6(2bytes)
window7 Specify window7(2bytes)
window8 Specify window8(2bytes)
window9 Specify window9(2bytes)
```

Introduction to O&M - Application scenario of ACL

Case1:

Requirement: The MAC address of the network segment connected to port 10 of the switch is 00-12-11-23-XX-XX, and the IP is 10.0.0.0/24 network segment. The administrator does not want users to use ftp, nor allow external networks to ping this any host on the network segment.

1. Traffic matching

```
access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac tcp  
p 10.0.0.0 0.0.0.255 any-destination d-port 21  
access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp an  
y-source 10.0.0.0 0.0.0.255
```

2. Applying it on the port

```
Interface Ethernet1/0/1  
mac-ip access-group 3110 in
```

3. Check the rules

```
switch(config-if-ethernet1/0/1)#show access-lists  
userdefined-access-list standard 1200(used 0 time(s)) 1 rule(s)  
rule id 1: deny window1 3 ffff
```

```
access-list 3110(used 1 time(s)) 2 rule(s)
```

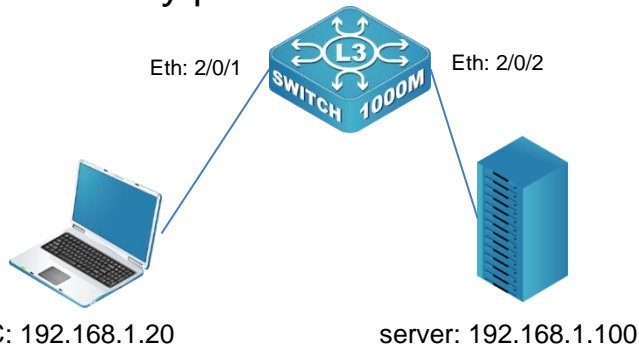
```
rule ID 1: deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac tcp 1  
0.0.0.0 0.0.0.255 any-destination d-port 21
```

```
rule ID 2: deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255
```

Notes: The rules are matched sequentially, if the first one matches, stop matching, if there is no match, continue until it matches

Introduction to O&M - Application scenario of ACL

Case2: Only permit 192.168.1.0 net access 21 port on the server and ping successfully



Command:

```
ip access-list extended test
 permit icmp 192.168.1.0 0.0.0.255 host-destination 192.168.1.100
 permit tcp 192.168.1.0 0.0.0.255 any-destination d-port 21
 deny ip any-source any-destination
 exit
!
Interface Ethernet2/0/1
 switchport access vlan 500
!
Interface Ethernet2/0/2
 ip access-group test out traffic-statistic
```

Some model cloud apply ACL on the output port to do the statistics

Result:

```
CS6200-54X-EI-XC(config-if-ethernet2/0/2)#show access-lists test
The total number of rules created is 3.
ip access-list extended test(used 1 time(s)) 3 rule(s)
 rule ID 2: permit icmp 192.168.1.0 0.0.0.255 host-destination 192.168.1.100
 rule ID 3: permit tcp 192.168.1.0 0.0.0.255 any-destination d-port 21
 rule ID 4: deny ip any-source any-destination
```

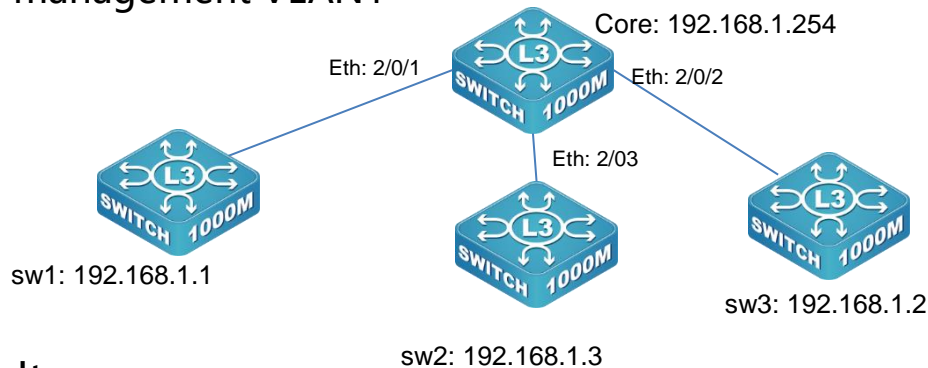
Notes: When using the permit statement, add "deny any any" to the last rule

```
CS6200-54X-EI-XC(config-if-ethernet2/0/2)#show access-group
interface name:Ethernet2/0/2
 IP Egress access-list used is test, packet(s) number is 0
 Rule ID 2 packet(s) number is 0.
 Rule ID 3 packet(s) number is 0.
 Rule ID 4 packet(s) number is 0.
CS6200-54X-EI-XC(config-if-ethernet2/0/2)#
```

Statistics: When hitting a packet, the 0 here would be changed into 1, which is usually used to judge the sending and receiving of a specific packet by the interface

Introduction to O&M - Application scenario of ACL

Case3: Only SNMP and telnet packets are allowed to pass through the core switch management VLAN1



Command:

```
ip access-list extended aaa
 permit udp any-source host-destination 192.168.1.254 d-port range 161 162
 permit tcp any-source host-destination 192.168.1.254 d-port 23
 deny ip any-source any-destination
 exit

vACL ip access-group aaa in vlan 1
```

Result:

```
ip access-list extended aaa(used 1 time(s)) 3 rule(s)
 rule ID 1: permit udp any-source host-destination 192.168.1.254 d-port range 161 162
 rule ID 2: permit tcp any-source host-destination 192.168.1.254 d-port 23
 rule ID 3: deny ip any-source any-destination
```

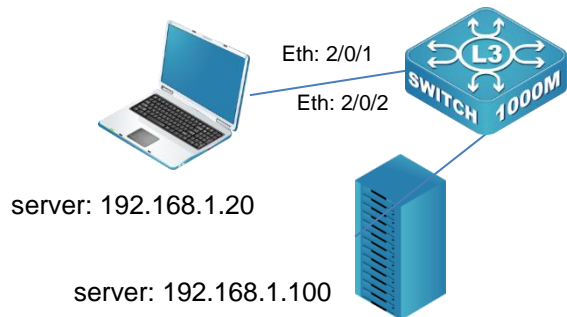
Notes: When using the permit statement, add "deny any any" to the last rule

```
CS6200-54X-EI-XC(config)#show vACL in vlan 1
VLAN 1:
IP Ingress access-list used is aaa, traffic-statistics Disable.
CS6200-54X-EI-XC(config)#
```

Ingress acting on the incoming direction
Traffic disable, that's why cannot see statistics

Introduction to O&M - Application scenario of ACL

Case4: The 2/0/2 port of the switch is not allowed to receive data packets whose first two bytes are 0xffff and TLV is 64.



Command & Result:

```
userdefined-access-list standard offset window1 12start 0 window2 13start 2
userdefined-access-list standard 1200 deny window1 ffff ffff window2 4000 ff00
```

```
Interface Ethernet2/0/2
in access-group test out traffic-statistic
userdefined access-group 1200 in
```

only support
incoming direction

✓ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 78
Identification: 0x3570 (13680)
> Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0xfd41 [validation disabled]

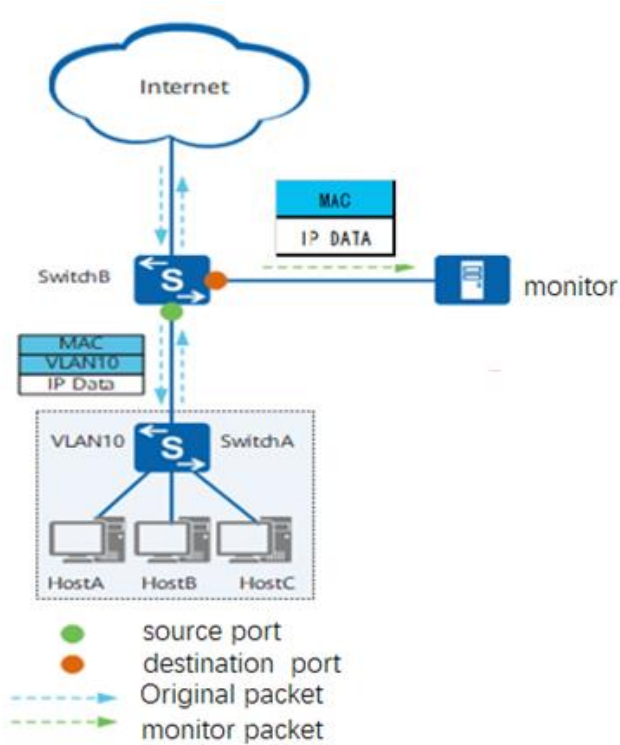
L3 head

```
000 ff ff ff ff ff e8 9a 8f 08 62 25 08 00 45 00 ..... b%..E.
010 00 4e 35 70 00 00 40 11 fd 41 0a 68 19 1f 0a 08 N5p... A.h...h
020 19 ff 00 89 00 89 00 3a 3c 0a ee ee 01 10 00 01 ..... : <.....
030 00 00 00 00 00 00 20 46 45 46 44 46 44 43 4f 46 ..... F EFDFCOF
040 46 46 41 45 45 46 43 46 47 43 4f 45 44 45 50 45 FFAEEFCF GCOEDEPE
050 4e 43 41 43 41 41 41 00 00 20 00 01 NCACAAA.. ..
```

Set offset, l3start 2 indicates offset 8 byte,
each model has different unit, the nos. of
used window also are different.

```
CS6200-54X-EI-XC(config)#userdefined-access-list standard offset
window1 Specify window1(4bytes)
window2 Specify window2(4bytes)
window3 Specify window3(4bytes)
window4 Specify window4(4bytes)
<cr>
```

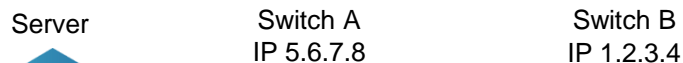
Introduction to O&M - Port mirroring



- Port mirroring refers to copying the packets received or sent by the mirroring source port to the mirroring destination port
- Different port mirroring:
 - Port mirroring
 - CPU mirroring
 - Flow mirroring

Introduction to O&M - Port mirroring configuration

The user needs to monitor the data frames received by port 7 and the data frames sent by port 9 on port 1, and also monitor the data frames received and sent by the CPU. Port 15 complies with rule 120 (source IP is 1.2.3.4, destination IP is 5.6.7.8) The data frame of the entrance is realized by configuring the mirror.



Notes:

1. Flow mirroring can take effect only when the specified rule is permit
2. A session has one and only one destination port
3. The throughput of the mirror destination port should be greater than the sum of the throughput of the mirror source ports

```
Switch-A#show monitor
No monitor in session 1
-----
No monitor in session 2
-----
No monitor in session 3
-----
monitor session 4:
Destination Ethernet1/0/1

source ports:
  RX port: 7 CPU
  TX port: 9 CPU
Flow monitor source:
  ACL Name:120
  RX port: 15
-----
```

```
access-list 120 permit tcp 1.2.3.0 0.0.0.255 5.6.7.0 0.0.0.255!
monitor session 4 source cpu tx
monitor session 4 source cpu rx
monitor session 4 source interface Ethernet1/0/9 tx
monitor session 4 source interface Ethernet1/0/7 rx
monitor session 4 source interface Ethernet1/0/15 access-list 120 rx
monitor session 4 destination interface Ethernet1/0/1
```

Introduction to O&M - Port mirroring Q&A

Q: Protocol packets such as OSPF and BGP cannot be mirrored to the destination port through TX port mirroring?

A: The protocol packets sent by the CPU cannot be mirrored to the destination port through port mirroring tx. This is not a problem. It is a characteristic of DCN equipment. The CPU does not go through the export process when sending packets, so it will not go to the mirroring process at the egress port. If you want to view cpu packets, please configure CPU mirroring.

Q: What are the usage scenarios of port mirroring and aggregated ports?

A: The aggregated port that cannot be used as the mirroring source port and destination port, when using mirroring, please use all the physical ports included in the aggregated port.

Q: Scenarios for using port mirroring on box switches?

A: A box switch can only be configured with one session

Q: VLAN of the mirroring source port?

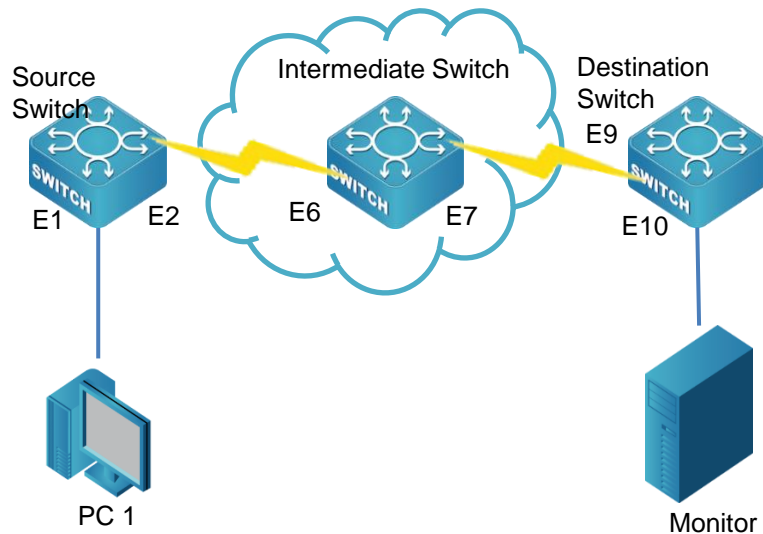
A: Multiple mirroring source ports can be in the same VLAN or in different VLANs



www.dcnglobal.com

Introduction to O&M - RSPAN configuration

- The user needs to detect the traffic received by the E1 port of the Source Switch on the Destination Switch



```
Source-Switch#  
vlan 5  
remote-span  
Interface Ethernet1/0/2  
switchport mode trunk  
!  
Interface Ethernet1/0/3  
switchport mode trunk  
monitor session 1 source interface Ethernet1/0/1 rx  
monitor session 1 reflector-port interface Ethernet1/0/3  
monitor session 1 remote vlan 5
```

```
Intermediate-Switch#  
vlan 5  
remote-span  
Interface Ethernet1/0/6  
switchport mode trunk  
!  
Interface Ethernet1/0/7  
switchport mode trunk
```

```
Destination-Switch#  
vlan 5  
remote-span  
Interface Ethernet1/0/9  
switchport mode trunk  
!  
Interface Ethernet1/0/10  
switchport mode trunk
```

Notes:

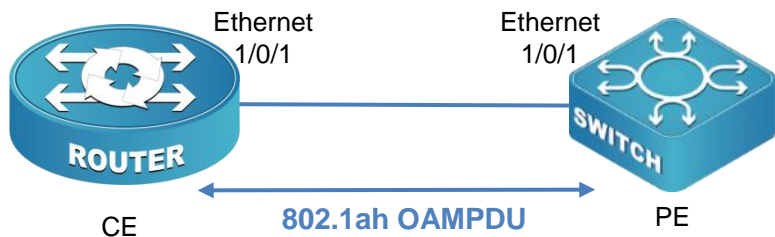
1. The destination port must have access remote VLAN
2. The reflection port is not wired
3. Remote VLAN is used to forward RSPAN data packets, and cannot carry user services in this VLAN

1. Layer 3 interfaces cannot be set up on the RSPAN VLAN on all devices, otherwise the mirrored packets may be discarded and cannot reach the destination port.
2. In the RSPAN data transmission link between the source switch and the intermediate switch, the native VLAN of the Trunk port in the output direction of the switch cannot be set to RSPAN VLAN, otherwise the RSPAN tag will be stripped when it does not reach the destination switch, resulting in RSPAN failure .
3. When the source switch adopts the reflection port mirroring method, the mirrored source port cannot be configured as a member port of the RSPAN VLAN in access or trunk mode.
4. When using remote mirroring, it is necessary to pay attention to the bandwidth of the link to meet the needs of business flow and mirroring traffic.

Introduction to O&M - EFM & OAM configuration

Case:

Enable the EFM OAM function on the CE and PE devices of the point-to-point link to monitor the performance of the "last mile" link. When an error event occurs, the log will be recorded and reported to the network management system; when necessary, the remote The end loopback function detects the link.



Command on CE device:

```
CE(config)#interface ethernet 1/0/1
CE (config-if-ethernet1/0/1)#ethernet-oam mode passive
CE (config-if-ethernet1/0/1)#ethernet-oam
CE (config-if-ethernet1/0/1)#ethernet-oam remote-loopback
supported
```

Notes:

Could use "ethernet-oam remote-loopback" to check the link status. Should disable remote-loopback after checking

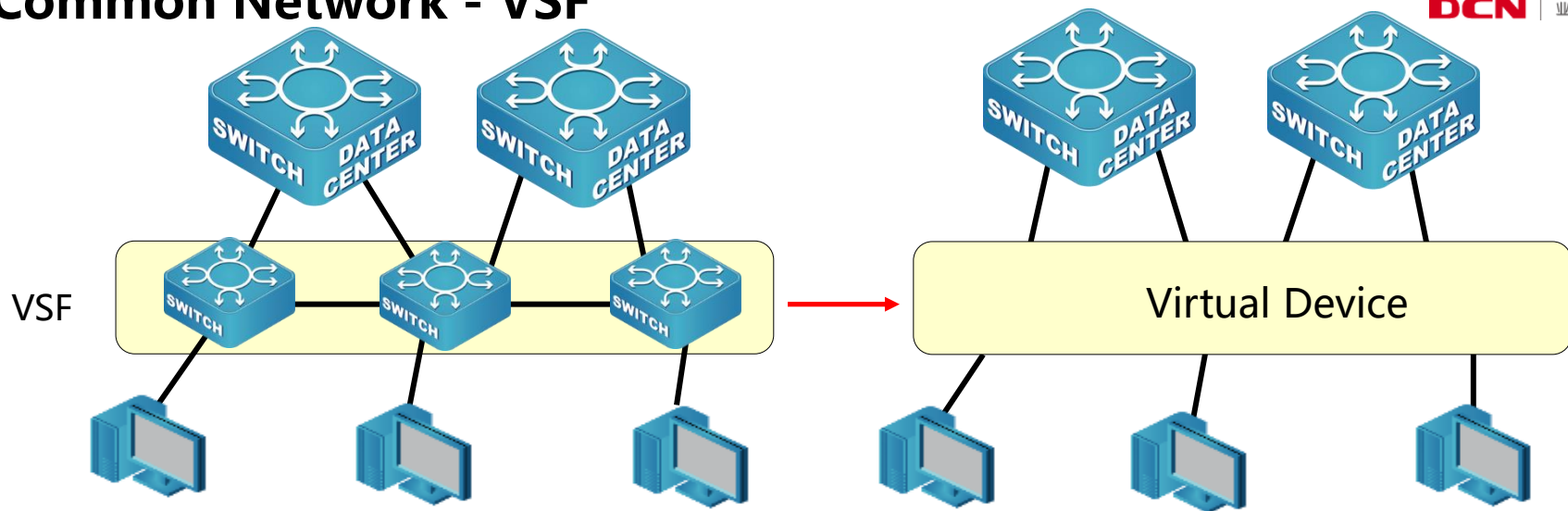
Command on PE device:

```
PE(config)#interface ethernet 1/0/1
PE (config-if-ethernet1/0/1)#ethernet-oam
Other parameters are default
```

02

Common Network

Common Network - VSF

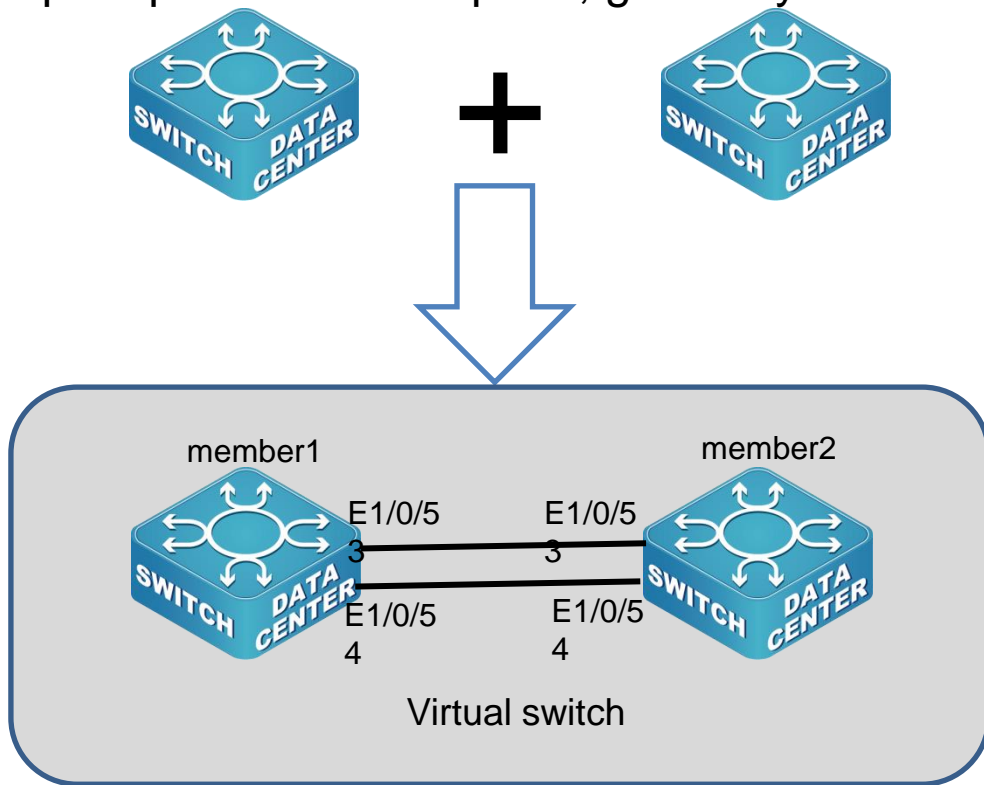


VSF(Virtual Switch Framework): It is to connect multiple devices to form a virtual logical device. The user manages this virtual device to realize the management of all physical devices in the virtual device.

The master completes the control of the VSF system, and all member devices can forward and process traffic locally

Common Network - VSF

In this scenario(2 units in stacking), a chain stack is used, and one vsf-port is used. Each vsf-port can put up to 8 member ports, generally use 2 member ports.



Common Network - VSF typical scenario

Member1 configuration:

```
switch convert mode vsf
vsf member 1
vsf priority 32
vsf port-group 1
vsf port-group Interface Ethernet1/0/53
vsf port-group Interface Ethernet1/0/54
```

Member2 configuration:

```
switch convert mode vsf
vsf member 2
vsf port-group 1
vsf port-group Interface Ethernet1/0/53
vsf port-group Interface Ethernet1/0/54
```

Checking vsf status

```
CS6200-54X-EI-XC#show vsf topology
Switch      VSF-Port1      Neighbor      VSF-Port2
1           Neighbor
1           Ethernet1/0/53  2             --
           --
           Ethernet1/0/54
2           Ethernet2/0/53  1             --
           --
           Ethernet2/0/54
```

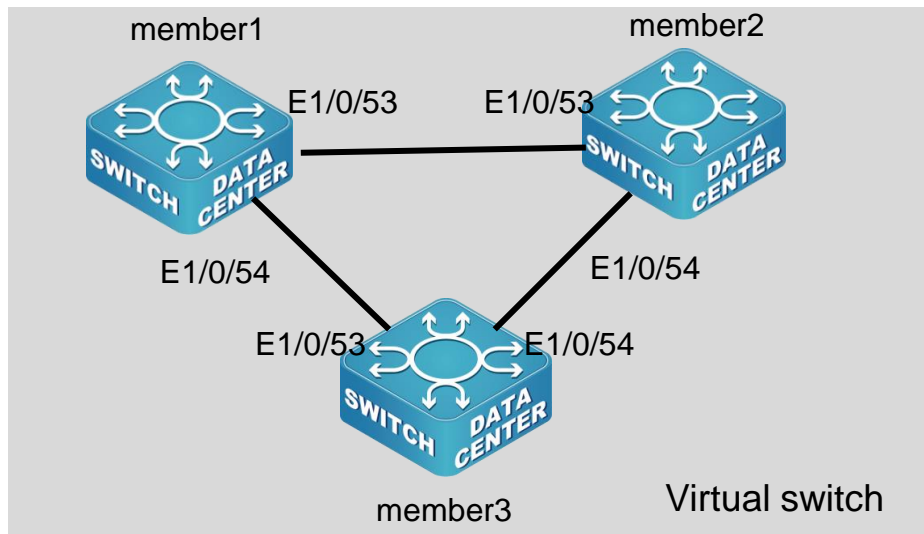
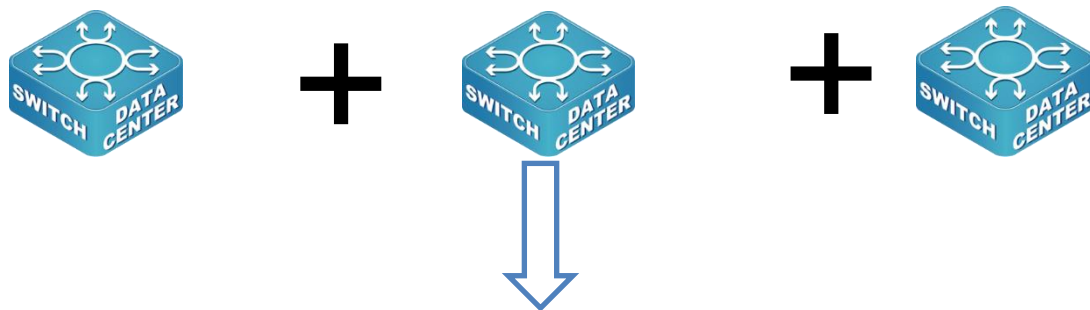
Member1 ports:
53,54

Member2 ports:
53,54

Notes: 2 units in stacking, in usual, recommend to use one vsf-port to put 2 physical ports, and the traffic here is in load balance mode. If two vsf-ports are used, one set of ports is in the backup state, and the ports that do not forward traffic are blocked.

Which scenario will use 2 vsf-ports?

Common Network - VSF



Multiple switches (up to 4) stacking scenario uses ring stacking, need to use 2 VSF-ports

Common Network - VSF configuration

Ring stacking configurations:

member1:

```
switch convert mode vsf
vsf member 1
vsf priority 32
vsf port-group 1
vsf port-group Interface Ethernet1/0/53
vsf port-group 2
vsf port-group Interface Ethernet1/0/54
```

member2:

```
switch convert mode vsf
vsf member 2
vsf port-group 1
vsf port-group Interface Ethernet1/0/53
vsf port-group 2
vsf port-group Interface Ethernet1/0/54
```

member3:

```
switch convert mode vsf
vsf member 2
vsf port-group 1
vsf port-group Interface Ethernet1/0/53
vsf port-group 2
vsf port-group Interface Ethernet1/0/54
```

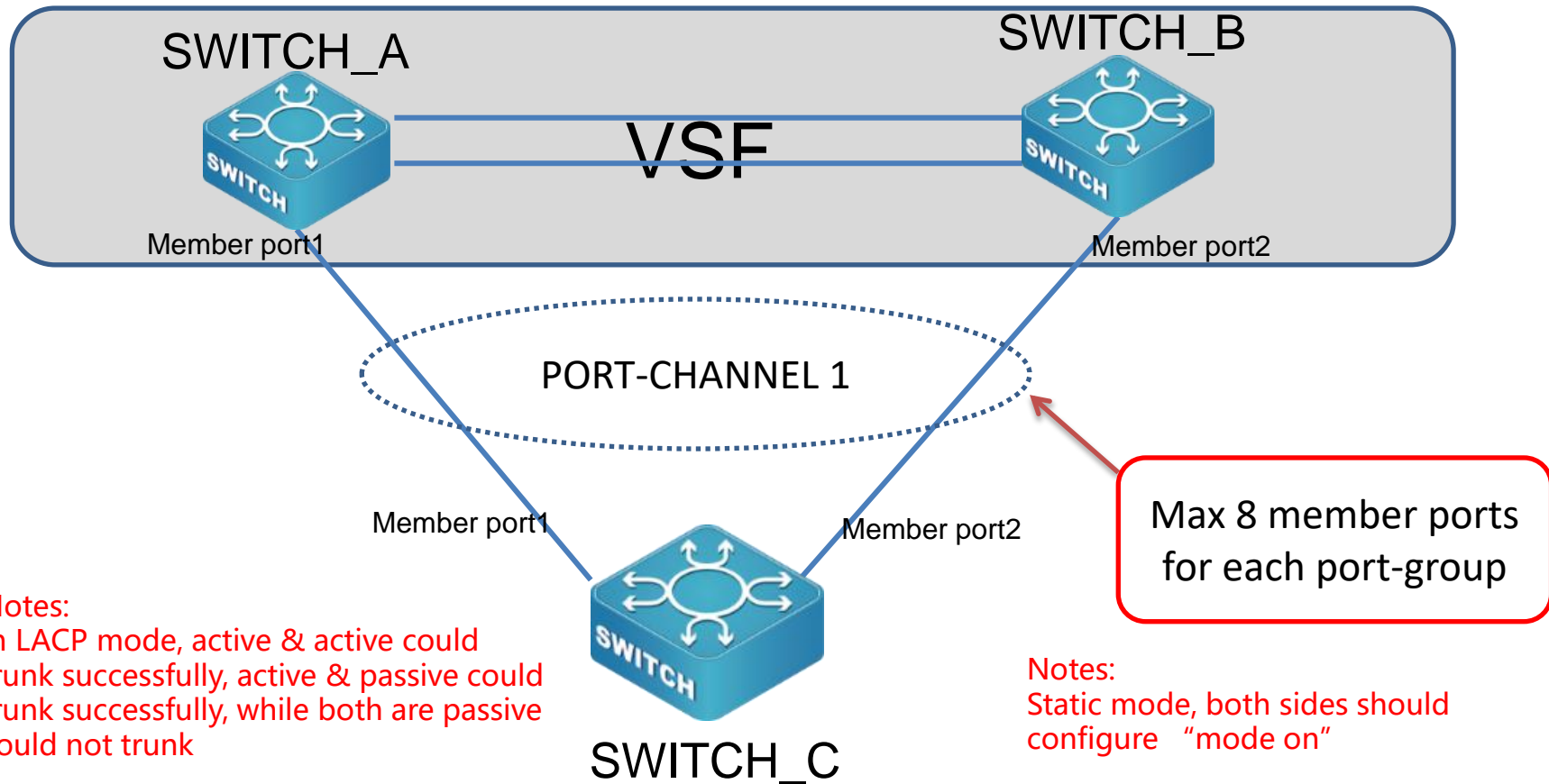
Notes:

After slave device reboot, need to config "vsf auto-merge enable" to achieve auto-merge

Common Network - VSF switchover mechanism

SW1 Pri32, SW2 Pri32	VSF mac-address persistent	Master Reboot	Slave Reboot	Master Device switchover
Master Reboot	Y	Y	N	Y
Slave Reboot	Y	N	Y	N
VSF Division(Cable disconnected)	Y	N	Y	Dual home
VSF Merge(Cable connected)	Y	N	Y	Elect SW1 as master according to priority
Master Reboot	N	Y	Y	Elect SW1 as master according to priority
Slave Reboot	N	N	Y	N
VSF Division(Cable disconnected)	N	N	Y	Dual home
VSF Merge(Cable connected)	N	N	Y	Elect SW1 as master according to priority

Common Network - Port-group



Common Network - Port-group

```
Switch(config)#show port-group 1 detail
Flags: A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

```
Port-group number: 1, Mode: , Load-balance: dst-src-mac
```

```
Port-group detail information:
```

```
System ID: 0x8000,00-03-0f-92-79-3f
```

```
Local:
```

Port	Status	Priority	Oper-Key	Flag
Ethernet1/0/9	Selected	32768	1	{ACDEF}
Ethernet1/0/10	Selected	32768	1	{ACDEF}
Ethernet1/0/11	Selected	32768	1	{ACG}

```
Remote:
```

Actor	Partner	Priority	Oper-Key	SystemID	Flag
Ethernet1/0/9	1	32768	1	0x8000,00-03-0f-d4-1c-8b	{ACDEF}
Ethernet1/0/10	65	32768	1	0x8000,00-03-0f-d4-1c-8b	{ACDEF}

A-active mode
CDEF-trunk successfully
CG-trunk failed

3 ports: 9-11
Selected-member ports
11 shows "ACG", because port 11 not
connected to opposite side

Common Network - Port-gruop

```
Switch(config)#show interface port-channel 1
Interface brief:
Port-Channel1 is down, line protocol is down
Port-Channel1 is layer 2 port, alias name is (null), index is 1025
Port-Channel1 is LAG port, member is :
    Hardware is EtherChannel, address is 00-03-0f-92-79-3f
PVID is 1
MTU 1500 bytes, BW 20000 Kbit
Time since last status change: 0w-4d-4h-34m-57s (362097 seconds)
Encapsulation ARPA, Loopback not set
Force half-duplex, Auto-speed
FlwControl is off, MDI type is auto
Statistics:
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
The last 5 second input rate 0 bits/sec, 0 packets/sec
The last 5 second output rate 0 bits/sec, 0 packets/sec
Input packets statistics:
```

After trunking, we could see port bandwidth changed into 2G by "show int port-channel 1"

Common Network - Port-group

```
CS6200-54X-EI-XC(config-if-ethernet1/0/1)#port-group 1 mode active  
Error: The VLAN property on port Ethernet1/0/1 is different from port-group 1!
```

Aggregated member port attributes are inconsistent

Method of load balance:

Based on flow, one flow can only choose one side.

dst-mac: based on the destination MAC

dst-src-ip: based on the source and destination IP address

dst-src-mac: based on the source and destination MAC address

src-ip: based on the source IP address

src-mac: based on the source MAC address

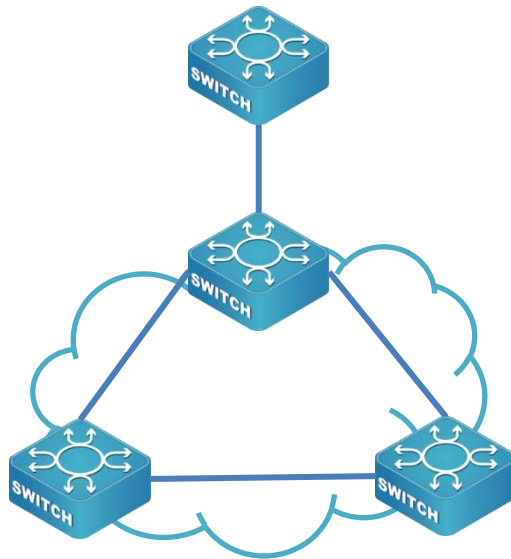
default: based on the source MAC address

Common Q&A

1. Load balance
2. Packet loss---Checking trunk port status, try to down one port to test

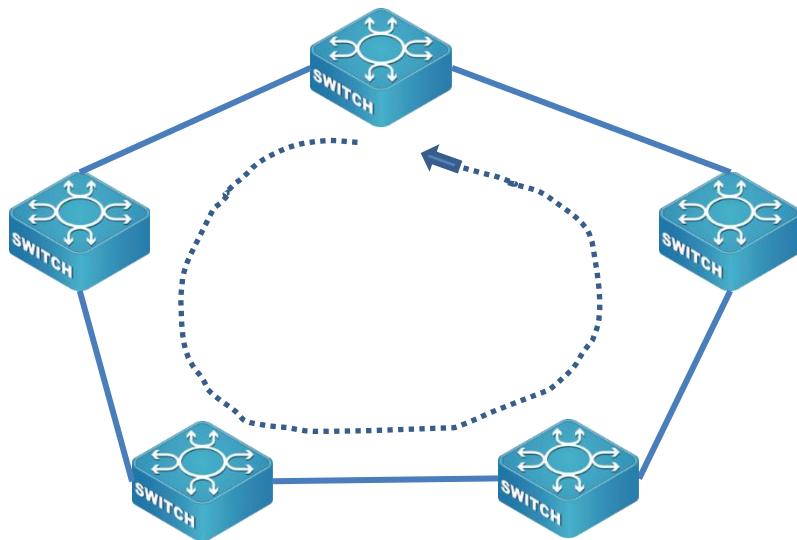
Common Network - Loop detection

Case1: Single-port loop detection, a loop occurs in the network connected to the Switch, so that the packets sent from the interface are looped back to the interface after passing through the external network.

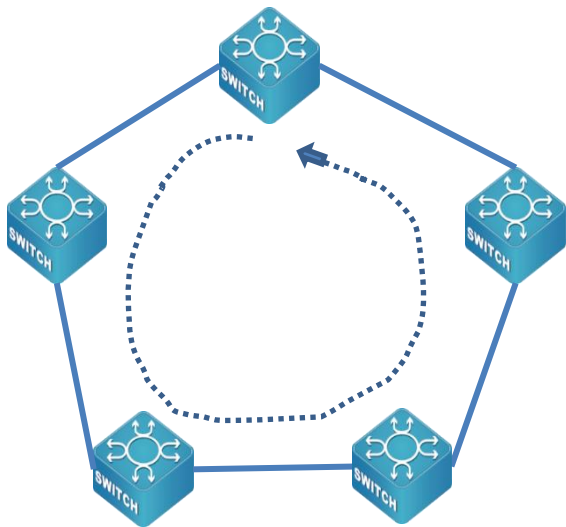


Common Network - Loop detection

Case2: Dual-arm loopback means that after the detection message is sent from the port S1P1, the detection message passes through the downstream switch and then loops back to the switch from another port S1P2 of the device.



Common Network - Port loop detection command



Main Command:

1. loopback-detection specified-VLAN <VLAN-list>
2. loopback-detection control {**shutdown** | **block** | **learning**}

```
!
Interface Ethernet1/0/9
 loopback-detection specified-vlan 1
 loopback-detection control shutdown
!
```

Common Network - Port Loop Detection

Only one port needs to be configured for single-port environment detection, and both ports need to be configured for dual-arm

```
CS6200-28X-E1#show loopback-detection
Loopback Detection Global Information
Transmit Interval : 5s(loopback mode), 3s(no loopback mode)
Control Recover Time : 0
Loopback Detection Port Information
PortName      Loopback Detection      Control Mode  Is Controlled
Happen times
Ethernet1/0/1  Disable                No            No
0
Ethernet1/0/2  Disable                No            No
0
Ethernet1/0/3  Disable                No            No
0
Ethernet1/0/4  Disable                No            No
0
Ethernet1/0/5  Disable                No            No
0
Ethernet1/0/6  Disable                No            No
0
Ethernet1/0/7  Disable                No            No
0
Ethernet1/0/8  Disable                No            No
0
Ethernet1/0/9  Enable                 Shutdown      Yes
0
Ethernet1/0/10 Disable                No            No
0
```

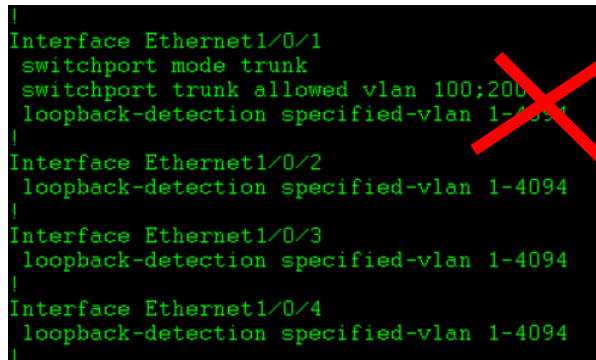
Single port loop

```
Ethernet1/0/5  Enable                 Shutdown      No
30
Ethernet1/0/6  Disable                No            No
0
Ethernet1/0/7  Disable                No            No
0
Ethernet1/0/8  Disable                No            No
0
Ethernet1/0/9  Enable                 Shutdown      Yes
4
Ethernet1/0/10 Disable                No            No
```

dual arm loop

Common Network - FAQ of Loopback detection

1. By sending the detection packets, if there were a large number of ports and VLANs, the burden on the system CPU will be increased. It is recommended to only configure the VLAN used by the port.

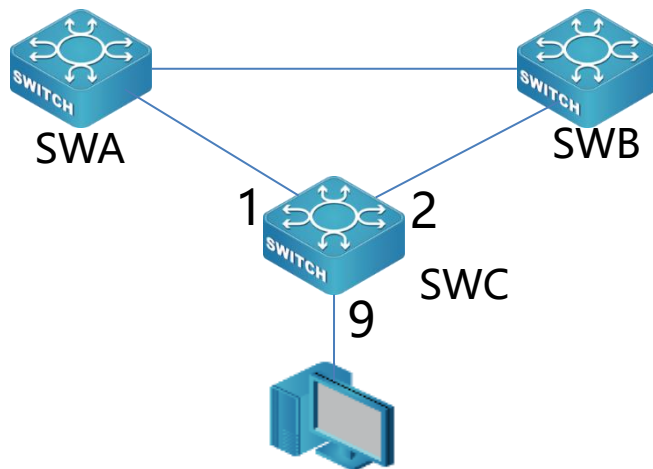


```
Interface Ethernet1/0/1
 switchport mode trunk
 switchport trunk allowed vlan 100;200
 loopback-detection specified-vlan 1-4094
|
Interface Ethernet1/0/2
 loopback-detection specified-vlan 1-4094
|
Interface Ethernet1/0/3
 loopback-detection specified-vlan 1-4094
|
Interface Ethernet1/0/4
 loopback-detection specified-vlan 1-4094
|
```

2. The detection of downlink network loops does not support QinQ scenarios, including dot1q tunnel ports and Selective QinQ

Common Network - STP introduction

1. In order to achieve link redundancy in a LAN, it is usually implemented by interconnecting two physical links on two Layer 2 switches.
2. Redundant links produce physical loops, causing broadcast storms, unstable mac address tables, and other hazards.



Broadcast storm

```
S4600-28P-SI#show interface ethernet counter rate
Interface      IN(pkts/s)  IN(bits/s)  OUT(pkts/s)  OUT(bits/s)
1/0/1          5m 18,122    16,467,633  18,144      16,495,308
               5s 108,583    82,822,845  108,578    82,819,962
1/0/2          5m 18,142    16,493,699  18,124      16,469,275
               5s 108,579    82,819,107  108,583    82,822,763
1/0/3          5m 0         0           0           0
               5s 0         0           0           0
1/0/4          5m 0         0           0           0
               5s 0         0           0           0
1/0/5          5m 0         0           0           0
               5s 0         0           0           0
1/0/6          5m 0         0           0           0
               5s 0         0           0           0
1/0/7          5m 0         0           0           0
               5s 0         0           0           0
1/0/8          5m 0         0           0           0
               5s 0         0           0           0
1/0/9          5m 1       1,679      36,265     32,962,223
               5s 1       557       217,159   165,643,021
1/0/10         5m 0         0           0           0
               5s 0         0           0           0
1/0/11         5m 0         0           0           0
               5s 0         0           0           0
```

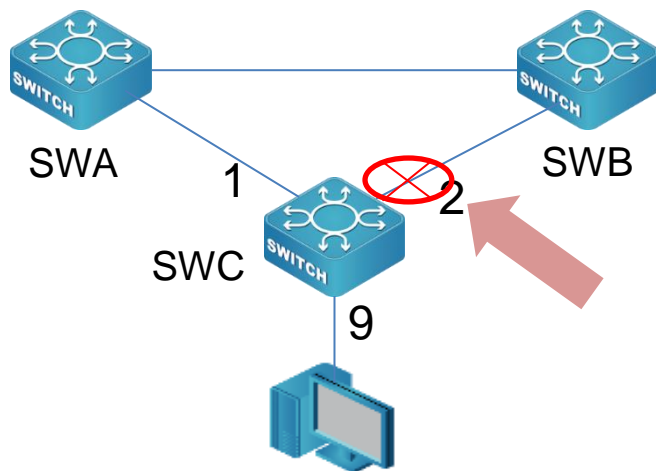
MAC address unstable

```
1 00-03-0f-62-c3-dc STATIC System CPU
1 68-f7-28-0e-27-1f DYNAMIC Hardware Ethernet1/0/1
S4600-28P-SI#show mac-address-table
Read mac address table....
Vlan Mac Address Type Creator Ports
-----
1 00-03-0f-62-c3-dc STATIC System CPU
1 68-f7-28-0e-27-1f DYNAMIC Hardware Ethernet1/0/2
S4600-28P-SI#show mac-address-table
Read mac address table....
Vlan Mac Address Type Creator Ports
-----
1 00-03-0f-62-c3-dc STATIC System CPU
1 68-f7-28-0e-27-1f DYNAMIC Hardware Ethernet1/0/1
S4600-28P-SI#show mac-address-table
Read mac address table....
Vlan Mac Address Type Creator Ports
-----
1 00-03-0f-62-c3-dc STATIC System CPU
1 68-f7-28-0e-27-1f DYNAMIC Hardware Ethernet1/0/2
S4600-28P-SI#show mac-address-table
Read mac address table....
Vlan Mac Address Type Creator Ports
-----
```

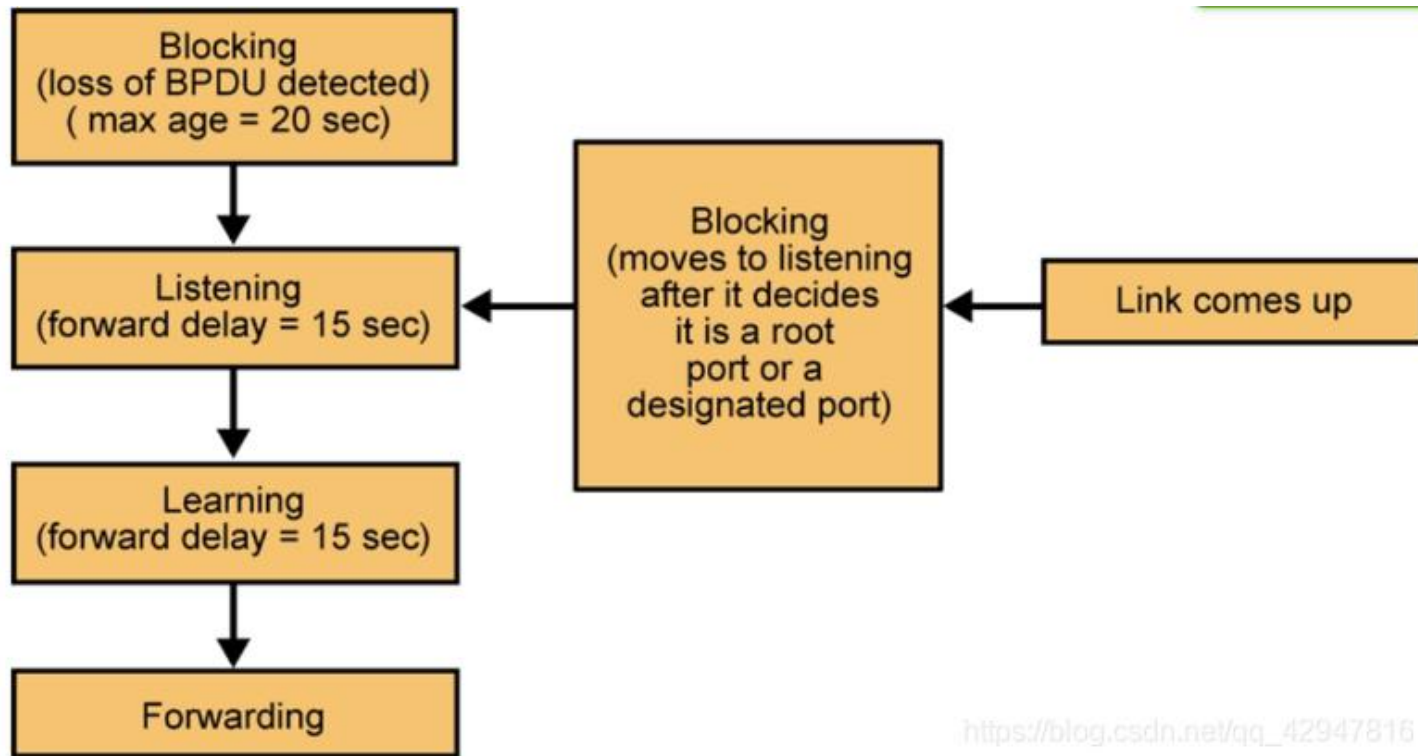
Common Network - STP introduction

Three mode: STP, RSTP, MSTP.

The spanning tree avoids loops by blocking appropriate ports, as shown in the figure below, port 2 of SWC no longer forwards packets to avoid loops.



Common Network - STP state figure



https://blog.csdn.net/qq_42947816

Common Network - STP configuration

SWA:
spanning-tree
spanning-tree mode stp
spanning-tree priority 4096

SWB:
spanning-tree
spanning-tree mode stp
spanning-tree priority 8192

SWC:
spanning-tree
spanning-tree mode stp
spanning-tree priority 32768

“show spanning-tree” to check STP status

***** Process 0 *****

-- STP Bridge Config Info --

Standard : IEEE 802.1d
Bridge MAC : 00:03:0f:17:77:72
Bridge Times : Max Age 20, Hello Time 2, Forward Delay 15
Force Version: 0

Self Bridge Id : 4096.00:03:0f:17:77:72
Root Id : this switch
Ext.RootPathCost : 0
Root Port ID : 0

PortName DsgPort	ID	ExtRPC	State	Role	DsgBridge
Ethernet1/0/1 128.001	128.001	0 FWD	DSGN	4096.00030f177772	
Ethernet1/0/2 128.002	128.002	0 FWD	DSGN	4096.00030f177772	

-- STP Bridge Config Info --

Standard : IEEE 802.1d
Bridge MAC : 00:01:7a:f6:0c:d7
Bridge Times : Max Age 20, Hello Time 2, Forward Delay 15
Force Version: 0

Self Bridge Id : 8192 - 00:01:7a:f6:0c:d7
Root Id : 4096.00:03:0f:17:77:72
Ext.RootPathCost : 20000
Root Port ID : 128.2

PortName DsgPort	ID	ExtRPC	State	Role	DsgBridge
Ethernet1/0/1 128.001	128.001	20000 FWD	DSGN	8192.00017af60cd7	
Ethernet1/0/2 128.002	128.002	0 FWD	ROOT	4096.00030f177772	

***** Process 0 *****

-- STP Bridge Config Info --

Standard : IEEE 802.1d
Bridge MAC : 00:03:0f:62:c3:dd
Bridge Times : Max Age 20, Hello Time 2, Forward Delay 15
Force Version: 0

Self Bridge Id : 32768.00:03:0f:62:c3:dd
Root Id : 4096.00:03:0f:17:77:72
Ext.RootPathCost : 20000
Root Port ID : 128.1

PortName DsgPort	ID	ExtRPC	State	Role	DsgBridge
Ethernet1/0/1 128.001	128.001	0 FWD	ROOT	4096.00030f177772	
Ethernet1/0/2 128.001	128.002	20000 BLK	ALTR	8192.00017af60cd7	
Ethernet1/0/9 128.009	128.009	20000 FWD	DSGN	32768.00030f62c3dd	

In STP mode, when we down the 1/0/1 port of SWC, and the 1/0/2 port of SWC will switch from block to forward state, but the switching time of STP is 30s, but the switching time of RSTP is within 1 second:

```
S4600-28P-SI#show logging buffered level warnings  
Current messages in SDRAM:4
```

```
4 %Jan 01 03:33:14:555 2006 <warnings> MODULE_L2_MSTP[tMstp]:MSTP set port = 2, mst = 65, process = 0 to FORWARDING!
```

```
3 %Jan 01 03:32:58:115 2006 <warnings> MODULE_L2_MSTP[tMstp]:MSTP set port = 2, mst = 65, process = 0 to LEARNING!
```

```
2 %Jan 01 03:32:41:636 2006 <warnings> MODULE_L2_MSTP[tMstp]:MSTP set port = 1, mst = 65, process = 0 to DISCARDING!
```

```
1 %Jan 01 03:32:41:630 2006 <warnings> MODULE_PORT[tphyDaemon]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1, changed state to DOWN
```

Configure SWA,SWB,SWC mode to RSTP: spanning-tree mode stp

```
S4600-28P-SI(config)#show logging buffered level warnings  
Current messages in SDRAM: 13
```

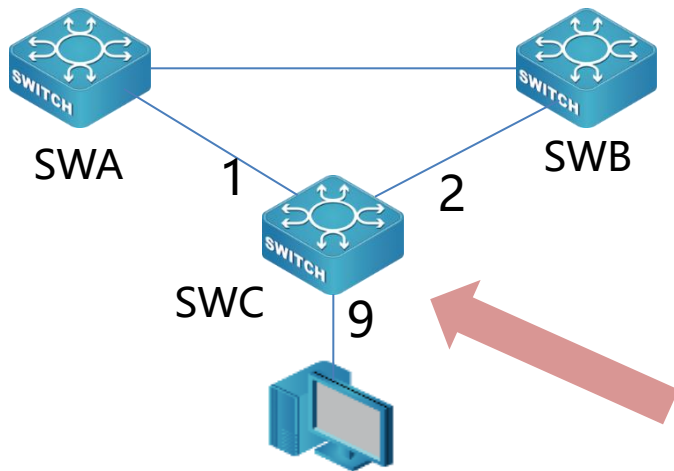
```
13 %Jan 01 03: 39: 34: 267 2006 <warnings> MODULE_L2_MSTP[tMstp]: MSTP set port = 2, mst = 65, process = 0 to  
FORWARDING!
```

```
12 %Jan 01 03: 39: 34: 266 2006 <warnings> MODULE_L2_MSTP[tMstp]: MSTP set port = 2, mst = 65, process = 0 to LEARNING!
```

```
11 %Jan 01 03: 39: 34: 265 2006 <warnings> MODULE_L2_MSTP[tMstp]: MSTP set port = 2, mst = 65, process = 0 to DISCARDING!
```

```
10 %Jan 01 03: 39: 34: 258 2006 <warnings> MODULE_PORT[tphyDaemon]: %LINEPROTO-5-UPDOWN: Line protocol on Interface  
Ethernet1/0/1, changed state to DOWN
```

Common Network - STP & RSTP



Notes:

If the host is connected here, you can use the "portfast". The port configured "portfast" does not participate in the calculation of the spanning tree and directly switches to the forwarding state.

Common Network - STP & RSTP



```
S4600-28P-SI(config-if-ethernet1/0/9)#show logging buffered level warnings
Current messages in SDRAM:18
```

After portfast

```
18 %Jan 01 04:10:15:653 2006 <critical> DEFAULT[zIMI]:[Console] Null, show spanning-tree
```

```
17 %Jan 01 04:10:06:409 2006 <warnings> MODULE_L2_MSTP[tmstp]:MSTP set port = 9, mst = 65, process = 0 to FORWARDING!
```

```
16 %Jan 01 04:10:06:406 2006 <warnings> MODULE_L2_MSTP[tmstp]:MSTP set port = 9, mst = 65, process = 0 to LEARNING!
```

```
15 %Jan 01 04:10:06:399 2006 <warnings> MODULE_L2_MSTP[tmstp]:MSTP set port = 9, mst = 65, process = 0 to DISCARDING!
```

```
14 %Jan 01 04:10:06:392 2006 <warnings> MODULE_PORT[tphyDaemon]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/9, changed state to UP
```

```
13 %Jan 01 04:10:01:719 2006 <warnings> MODULE_L2_MSTP[tmstp]:MSTP set port = 9, mst = 65, process = 0 to DISCARDING!
```

```
12 %Jan 01 04:10:01:705 2006 <warnings> MODULE_PORT[tphyDaemon]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/9, changed state to DOWN
```

```
11 %Jan 01 04:09:36:181 2006 <critical> DEFAULT[zIMI]:[Console] Null, spanning-tree portfast
```

```
10 %Jan 01 04:09:26:612 2006 <critical> DEFAULT[zIMI]:[Console] Null, int ethernet 1/0/9
```

Before portfast

```
9 %Jan 01 04:09:24:609 2006 <critical> DEFAULT[zIMI]:[Console] Null, conf
```

```
8 %Jan 01 04:09:23:470 2006 <critical> DEFAULT[zIMI]:[Console] Null, ena
```

```
7 %Jan 01 03:47:09:065 2006 <critical> DEFAULT[zIMI]:[Console] Null, int ethernet 1/0/9
```

```
6 %Jan 01 03:46:15:638 2006 <warnings> MODULE_L2_MSTP[tmstp]:MSTP set port = 9, mst = 65, process = 0 to FORWARDING!
```

```
5 %Jan 01 03:45:58:471 2006 <warnings> MODULE_L2_MSTP[tmstp]:MSTP set port = 9, mst = 65, process = 0 to LEARNING!
```

```
4 %Jan 01 03:45:42:350 2006 <warnings> MODULE_L2_MSTP[tmstp]:MSTP set port = 9, mst = 65, process = 0 to DISCARDING!
```

```
3 %Jan 01 03:45:42:349 2006 <warnings> MODULE_PORT[tphyDaemon]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/9, changed state to UP
```

```
2 %Jan 01 03:45:21:101 2006 <warnings> MODULE_L2_MSTP[tmstp]:MSTP set port = 9, mst = 65, process = 0 to DISCARDING!
```

```
1 %Jan 01 03:45:21:100 2006 <warnings> MODULE_PORT[tphyDaemon]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/9, changed state to DOWN
```

The port
connected with
host enable
portfast

Common Network - STP & RSTP

```
S4600-28P-SI(config-if-ethernet1/0/1)#spanning-tree portfast bpduguard
S4600-28P-SI(config-if-ethernet1/0/1)#%Jan 01 04:21:15:349 2006 %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/1, changed state to DOWN
%Jan 01 04:21:15:349 2006 %LINK-5-CHANGED: Interface Ethernet1/0/1, changed state to administratively DOWN
%Jan 01 04:21:15 2006 Received a bdp packet from Interface Ethernet1/0/1 , and
S4600-28P-SI(config-if-ethernet1/0/1)#show int ethernet counter rate
Interface      IN(pkts/s)      IN(bits/s)      OUT(pkts/s)      OUT(bits/s)
1/0/1          5m 9,570         12,448,201       9,670            12,576,403
               5s 66,858         89,283,878       66,854           89,279,140
1/0/2          5m 9,670         12,576,694       9,570            12,448,288
               5s 66,855         89,276,620       66,857           89,280,621
1/0/3          5m 0             0                0                0
               5s 0             0                0                0
1/0/4          5m 0             0                0                0
               5s 0             0                0                0
1/0/5          5m 0             0                0                0
               5s 0             0                0                0
1/0/6          5m 0             0                0                0
               5s 0             0                0                0
1/0/7          5m 0             0                0                0
               5s 0             0                0                0
1/0/8          5m 0             0                0                0
               5s 0             0                0                0
S4600-28P-SI(config-if-ethernet1/0/1)#
S4600-28P-SI(config-if-ethernet1/0/1)#
S4600-28P-SI(config-if-ethernet1/0/1)#show spanning-tree

***** Process 0 *****
-- RSTP Bridge Config Info --

Standard      : IEEE 802.1w
Bridge MAC    : 00:03:0f:62:c3:dd
Bridge Times  : Max Age 20, Hello Time 2, Forward Delay 15
Force version: 2

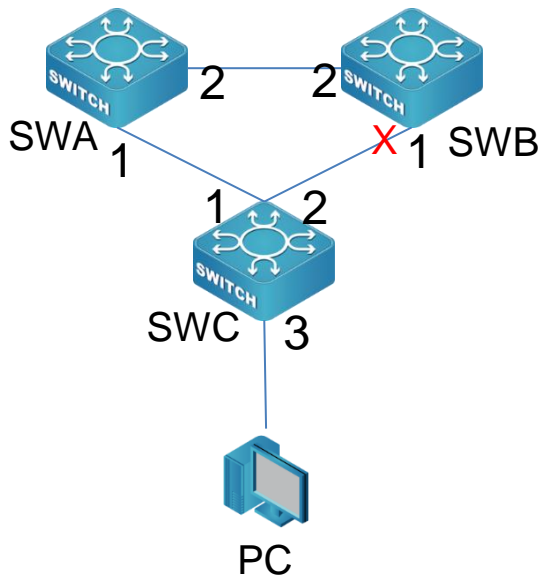
#####
Self Bridge Id : 32768.00:03:0f:62:c3:dd
Root Id        : 4096.00:03:0f:17:77:72
Ext.RootPathCost : 219999
Root Port ID   : 128.2

#####
PortName      ID      EXTRPC  State Role      DsgBridge      DsgPort
-----
Ethernet1/0/1 128.001 219999 FWD  DSGN 32768.00030f62c3dd 128.001
Ethernet1/0/2 128.002 20000  FWD  ROOT 8192.00017af60cd7 128.001
Ethernet1/0/9 128.009 219999 FWD  DSGN 32768.00030f62c3dd 128.009

#####
Self Br
Root Id
Ext. Roc
Root Pc
Port
Etherr
Etherr
Etherr
```

Notes: If portfast is configured on a non-host port, the port will be E-down. If filter is configured, it means that the spanning tree is not enabled on this port.

Common Network - STP configuration

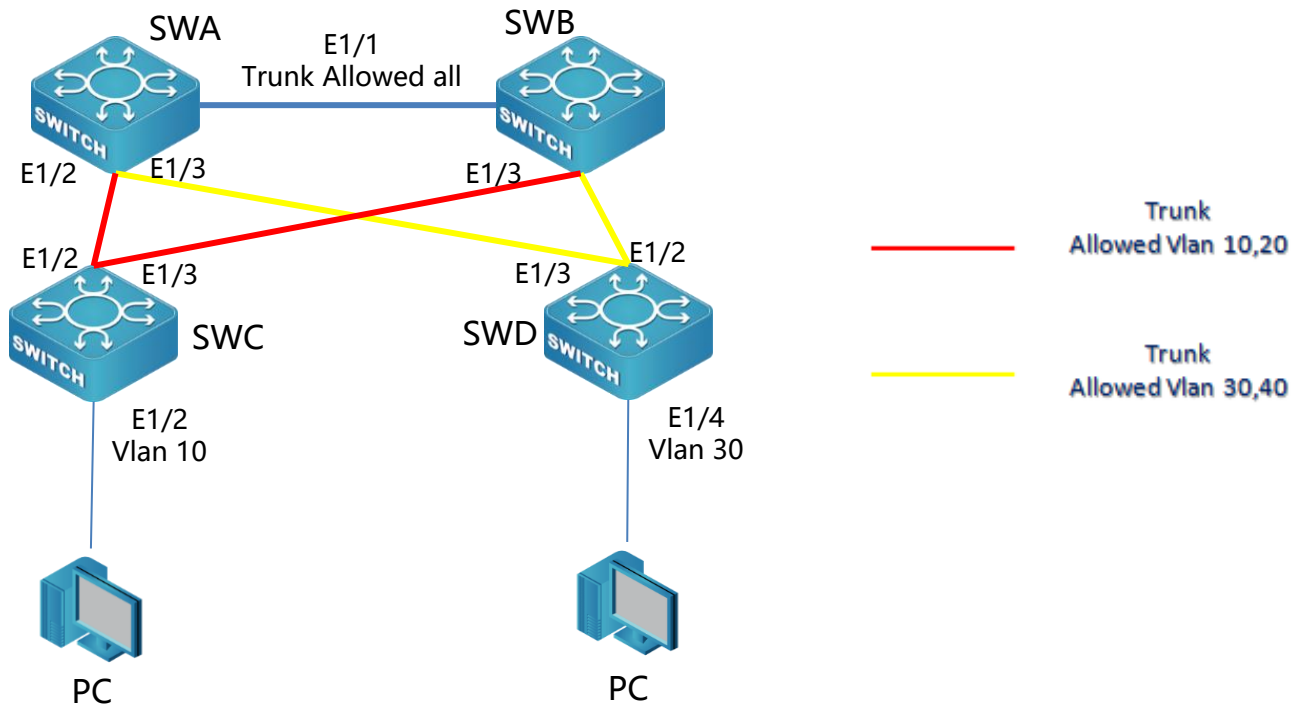


- Three switches running STP, make sure SWA become STP root bridge, SWB port1 block
- Port 3 of SWC up and instantly become forwarding state
- Command:
- **SWA:**
 - `switch(config)#spanning-tree`
 - `switch(config)#spanning-tree mode stp`
 - `switch(config)#spanning-tree priority 4096`
- **SWB:**
 - `switch(config)#spanning-tree`
 - `switch(config)#spanning-tree mode stp`
- **SWC:**
 - `switch(config)#spanning-tree`
 - `switch(config)#spanning-tree mode stp`
 - `switch(config)#spanning-tree priority 8192`
 - `Switch(Config-If-Ethernet0/0/3)#spanning-tree portfast bpdupfilter`

- MSTP divides a switching network into multiple domains, and multiple spanning trees are formed in each domain, and the spanning trees are independent of each other. Each spanning tree is called a multiple spanning tree instance(MSTI), and each domain is called an MST region(MST Region: Multiple Spanning Tree Region).
- The so-called instance is a collection of multiple VLANs. By bundling multiple VLANs into one instance, you can save communication overhead and resource usage. The calculations of each MSTP instance are independent of each other, and load balancing can be achieved on these instances. Multiple VLANs with the same topology can be mapped to one instance, and the forwarding status of these VLANs on the port depends on the status of the port in the corresponding MSTP instance.
- Bridges in each domain have the following three properties:
 - A configuration name containing numbers and letters (Configuration Name)
 - A configuration revision level (Revision Level)
 - Configuration Digest of VLAN to Spanning Tree Instance Mapping in Bridge (Configuration Digest)

Common Network - MSTP configuration

4 switches running MSTP, SWA as root bridge of VLAN 10/20, SW B as root bridge of VLAN 30/40.



Common Network - MSTP configuration

SW A configuration

```
#Configure MSTP, create MSTP multiple instance
switch(config)#spanning-tree
switch(config)#spanning-tree mst configuraion
switch(config-Mstp-Region)#name test
switch(config-Mstp-Region)#instance 0 VLAN 10;20
switch(config-Mstp-Region)#instance 1 VLAN 30;40
switch(config-Mstp-Region)#exit
switch(config)#spanning-tree mst 0 priority 4096
switch(config)#spanning-tree mst 1 priority 8192
#Configure port mode and transparently transmitted Vlan information
```

SW B configuration

```
# Configure MSTP, create MSTP multiple instance
switch(config)#spanning-tree
switch(config)#spanning-tree mst configuraion
switch(config-Mstp-Region)#name test
switch(config-Mstp-Region)#instance 0 VLAN 10;20
switch(config-Mstp-Region)#instance 1 VLAN 30;40
switch(config-Mstp-Region)#exit
switch(config)#spanning-tree mst 0 priority 8192
switch(config)#spanning-tree mst 1 priority 4096
#Configure port mode and transparently transmitted Vlan
information
```

SW C configuration

```
#Configure MSTP, create MSTP multiple instance
switch(config)#spanning-tree
switch(config)#spanning-tree mst configuraion
switch(config-Mstp-Region)#name test
switch(config-Mstp-Region)#instance 0 VLAN 10;20
switch(config-Mstp-Region)#instance 1 VLAN 30;40
switch(config-Mstp-Region)#exit
#Configure port mode and transparently transmitted Vlan information
```

SW D configuration

```
#Configure MSTP, create MSTP multiple instance
switch(config)#spanning-tree
switch(config)#spanning-tree mst configuraion
switch(config-Mstp-Region)#name test
switch(config-Mstp-Region)#instance 0 VLAN 10;20
switch(config-Mstp-Region)#instance 1 VLAN 30;40
switch(config-Mstp-Region)#exit
#Configure port mode and transparently transmitted Vlan information
```

In the same MSTP spanning tree domain, the domain name and instance configuration must be the same

Common Network - STP trouble-shooting

When the root bridge of the spanning tree fluctuates repeatedly, you need to enable debug to check the status of sending and receiving packets:

S4600-10P-SI, TX direction enable "debug" to check sending packets:

```
debug spanning-tree
```

```
debug driver send interface 1/0/10 protocol stp
```

```
debug spanning-tree fsm-port ptx interface ethernet 1/0/10
```

```
debug spanning-tree timer hello instance 0 interface ethernet 1/0/10
```

S4600-28P-P-SI, RX direction enable "debug" to check receiving packets:

```
debug driver receive interface 1/0/28 protocol stp
```

```
debug spanning-tree fsm-port pim instance 0 interface ethernet 1/0/28
```

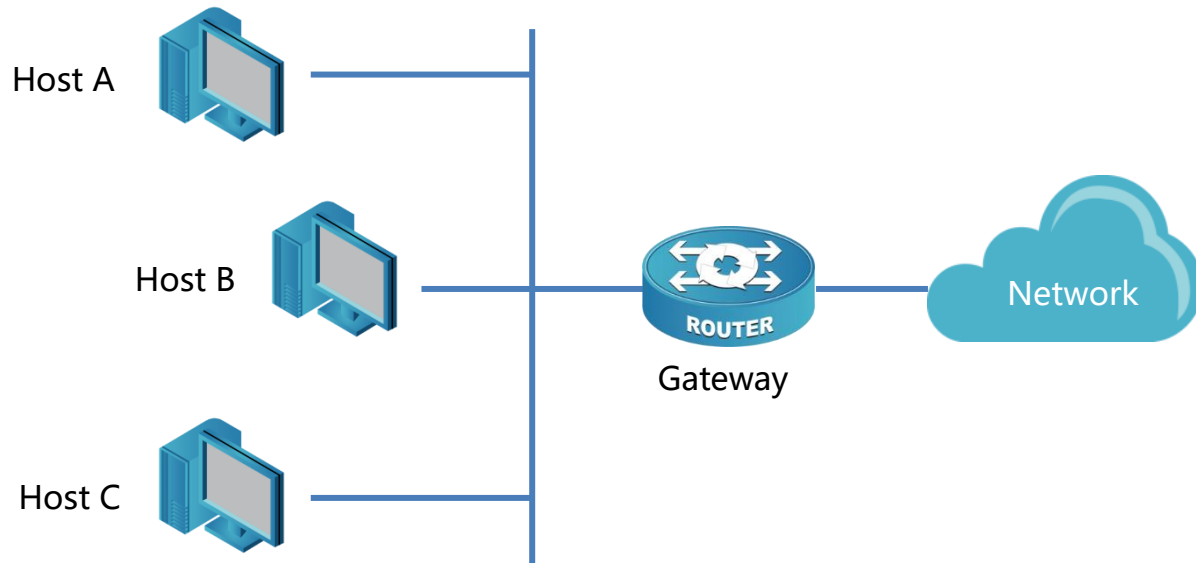
```
debug spanning-tree timer hello instance 0 interface ethernet 1/0/28
```

```
debug spanning-tree timer rcvdInfo instance 0 interface ethernet 1/0/28
```

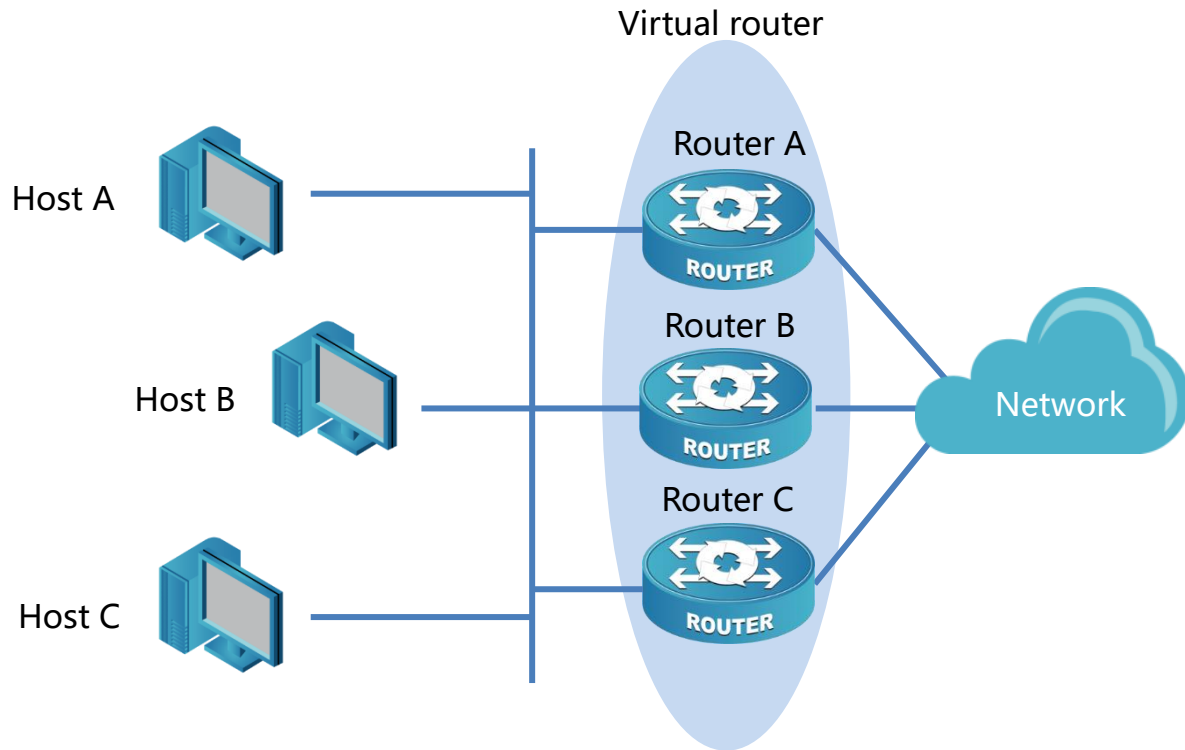
```
debug spanning-tree
```

- VRRP: Virtual Router Redundancy Protocol, defined in RFC2338 & FRC3768.
- VRRP is a fault-tolerant protocol.
- VRRP can obtain a more reliable default route without changing the networking situation or configuring any dynamic routing or route discovery protocol on the host.
- Version: VRRPv2 & VRRPv3.

Common Network - VRRP typical network

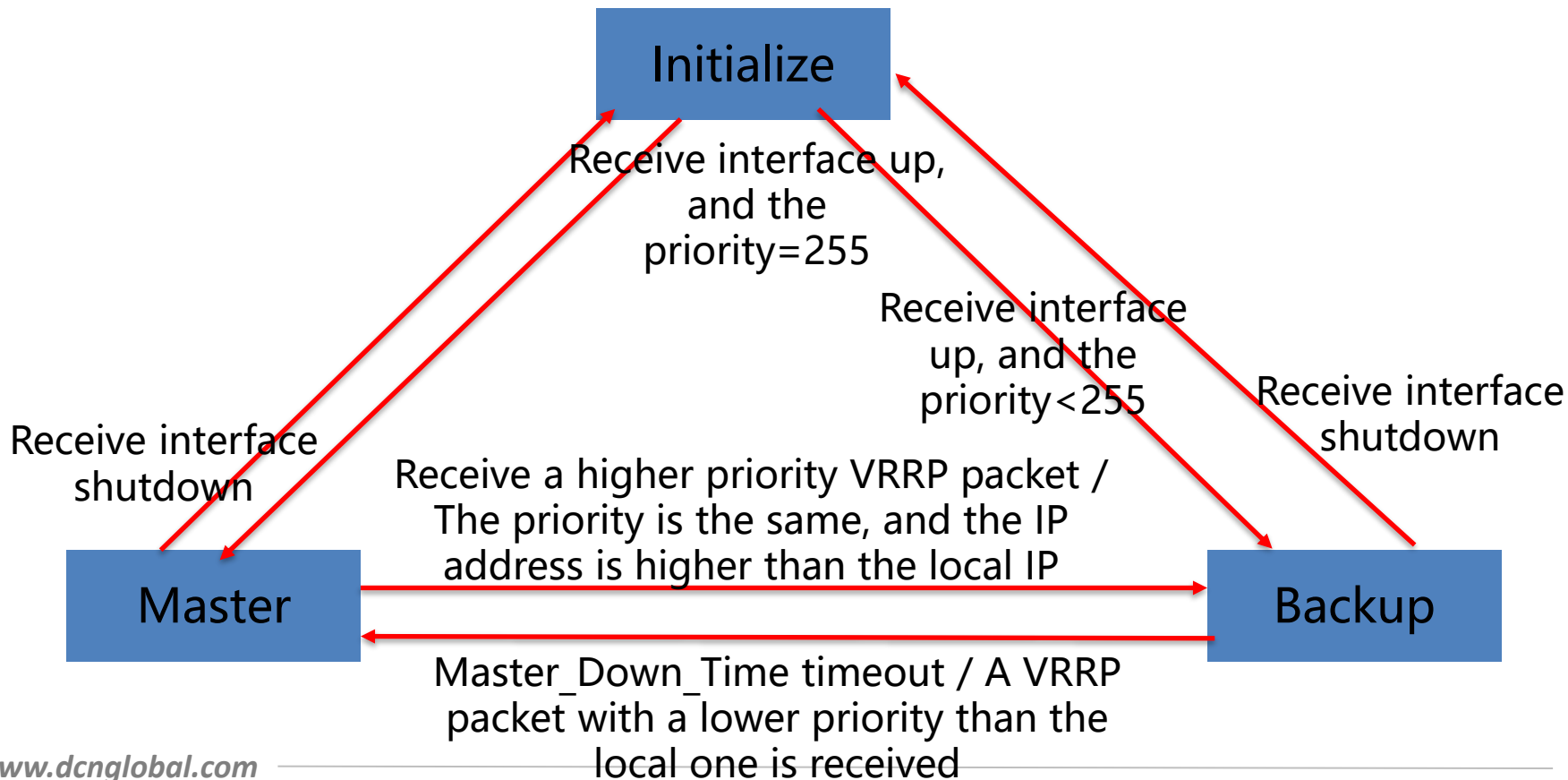


Common Network - VRRP link backup network

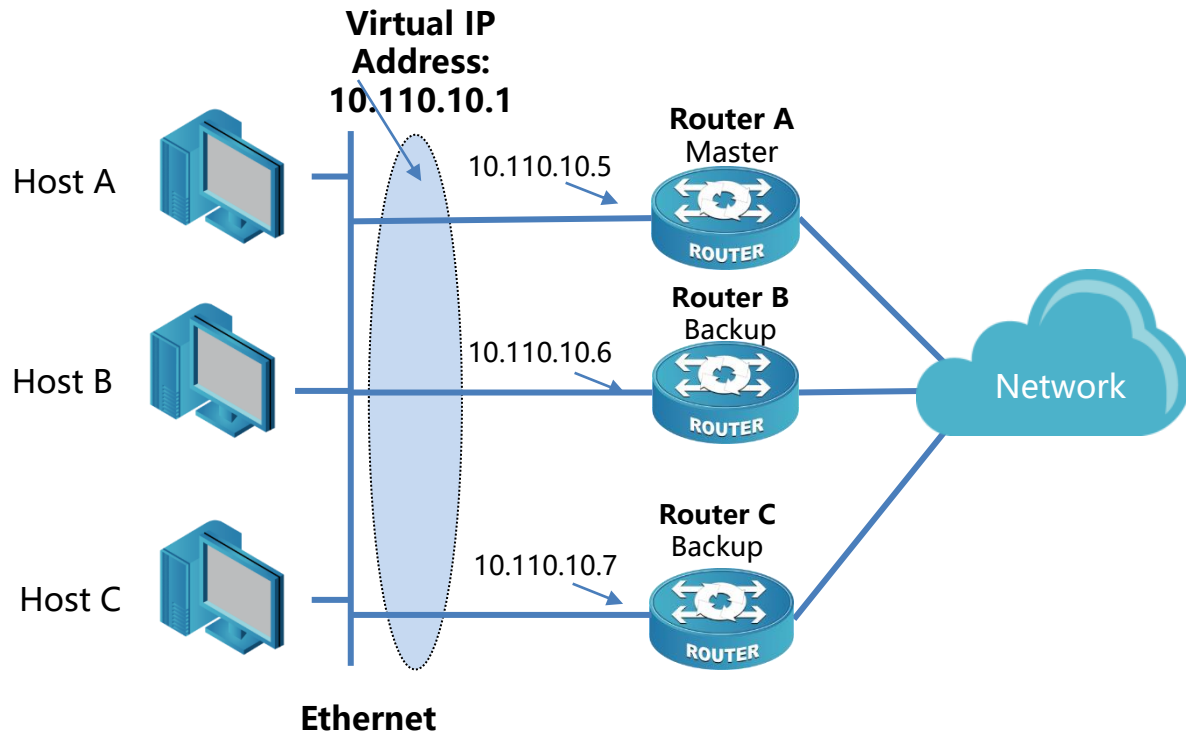


- VRRP router
- Virtual router
- VRID
- Master router
- Backup router
- Virtual IP address
- IP address owner
- Primary IP address
- Virtual MAC address

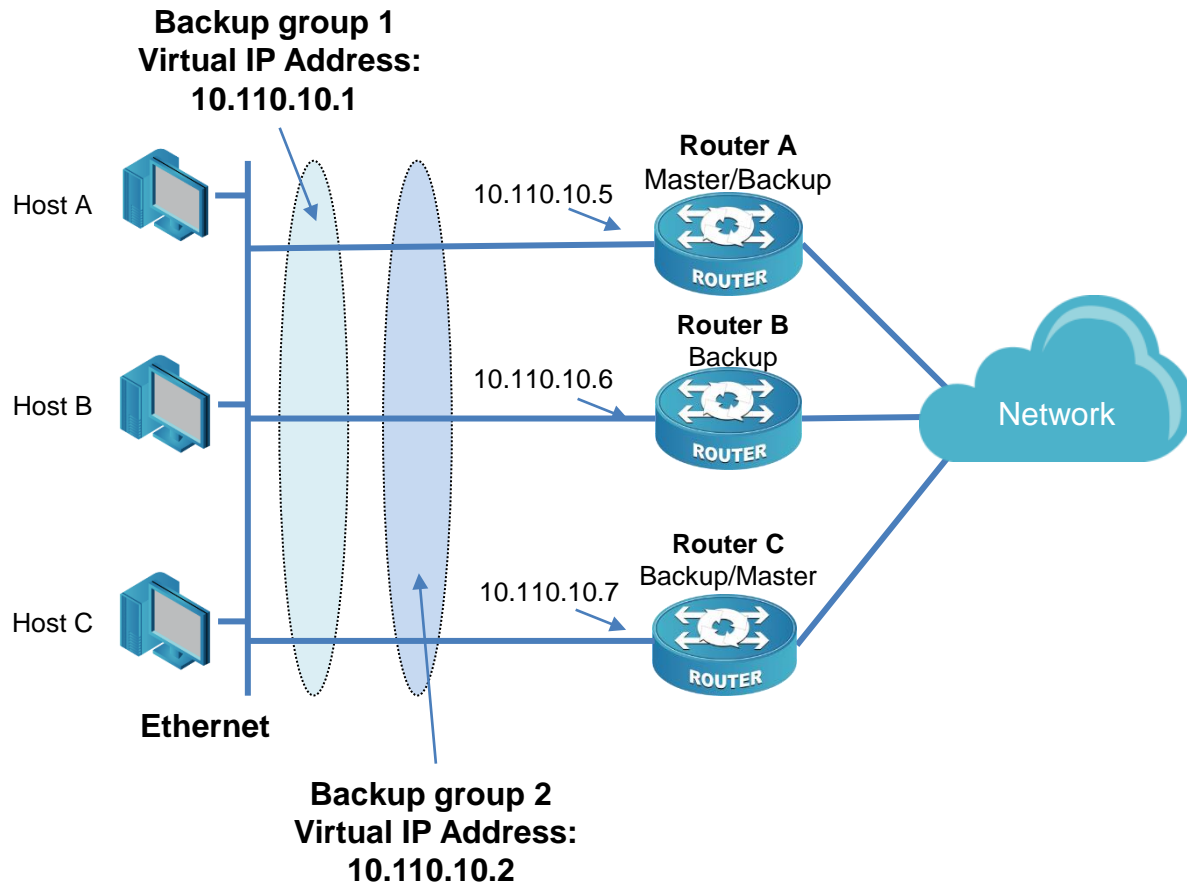
Common Network - VRRP state figure



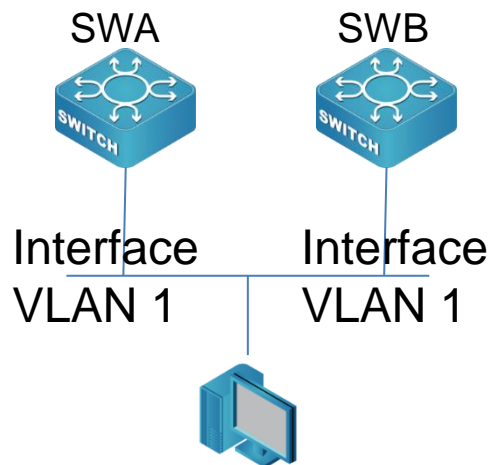
Common Network - VRRP active-standby backup



Common Network - VRRP load balance



Common Network - VRRP configuration



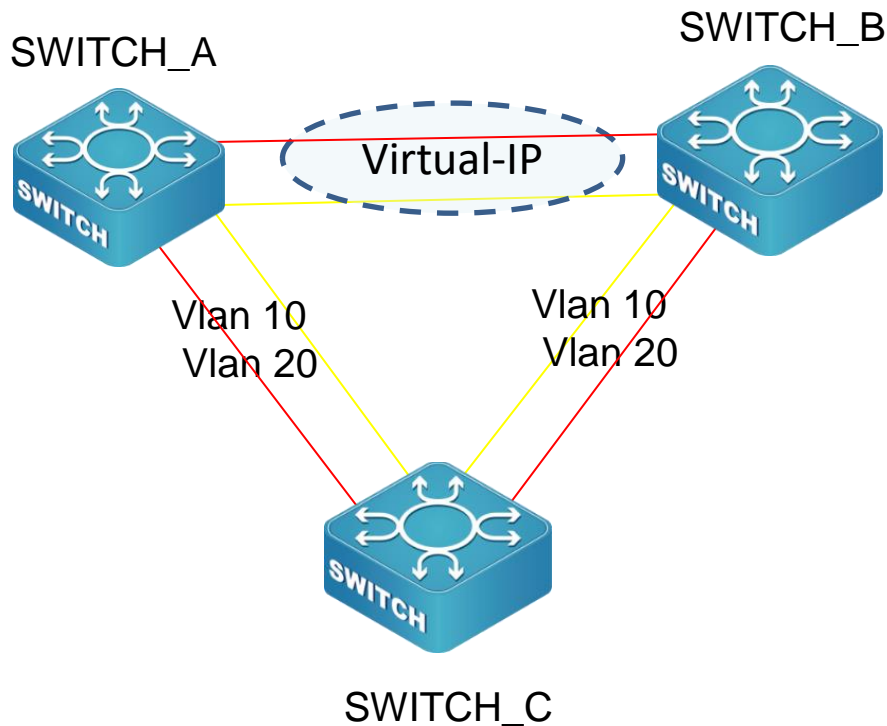
SwitchA:

```
SwitchA(config)#interface VLAN 1
SwitchA(Config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0
SwitchA(config)#router vrrp 1
SwitchA(config-router)#virtual-ip 10.1.1.5
SwitchA(config-router)#interface VLAN 1
SwitchA(config-router)#enable
```

SwitchB:

```
SwitchB(config)#interface VLAN 1
SwitchB (Config-if-Vlan1)#ip address 10.1.1.7 255.255.255.0
SwitchB (config)#router vrrp 1
SwitchB (config-router)#virtual-ip 10.1.1.5
SwitchB (config-router)#interface VLAN 1
SwitchB (config-router)#enable
```

Common Network - VRRP + MSTP



The red one is MSTP instance 1, SWITCH A as root bridge.

The yellow one is MSTP instance 2, SWITCH B as root bridge.

Virtual ip is the address created by SWA and SWB that is different from the VLAN interface of the device

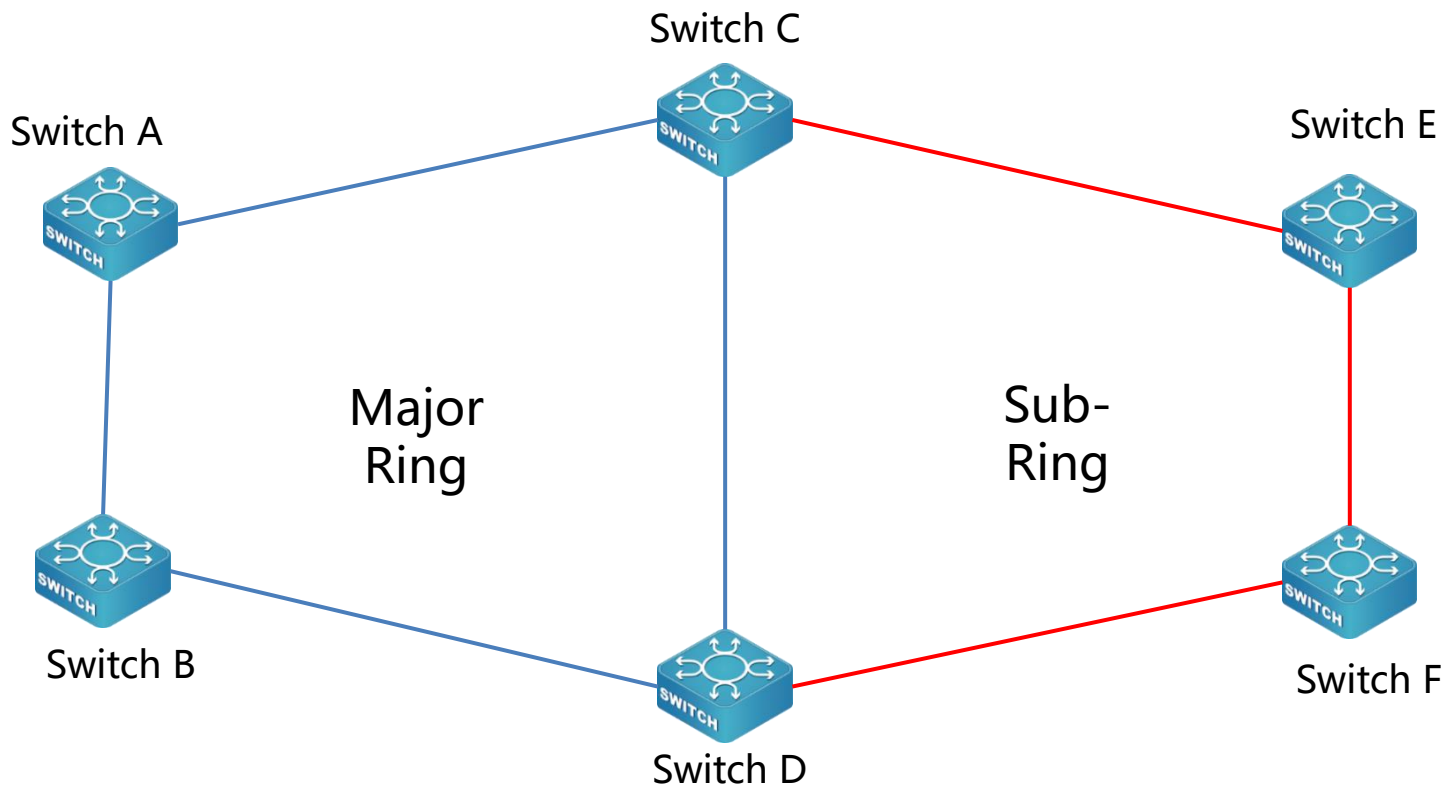
ERPS (Ethernet Ring Protection Switching)

- Only applying in ring network
- Fast convergency time, less than 50ms
- Need network schedule, configuration is complicated
- Unable achieve self link detection

STP/RSTP/MSTP

- Applying in any network
- Slow convergence time, about 1~2 seconds
- Simple configuration
- It can detect the link status by itself

Common Network - ERPS typical scenario



Common Network - ERPS port

RPL: Ring Protection Link

RPL Owner:

- Only one in each ring and there must be one
- Blocked in usual, open when link failure

RPL Neighbour:

- Directly connected to RPL owner
- Blocked in usual, open when link failure

ERPS ring could have none RPL Neighbour

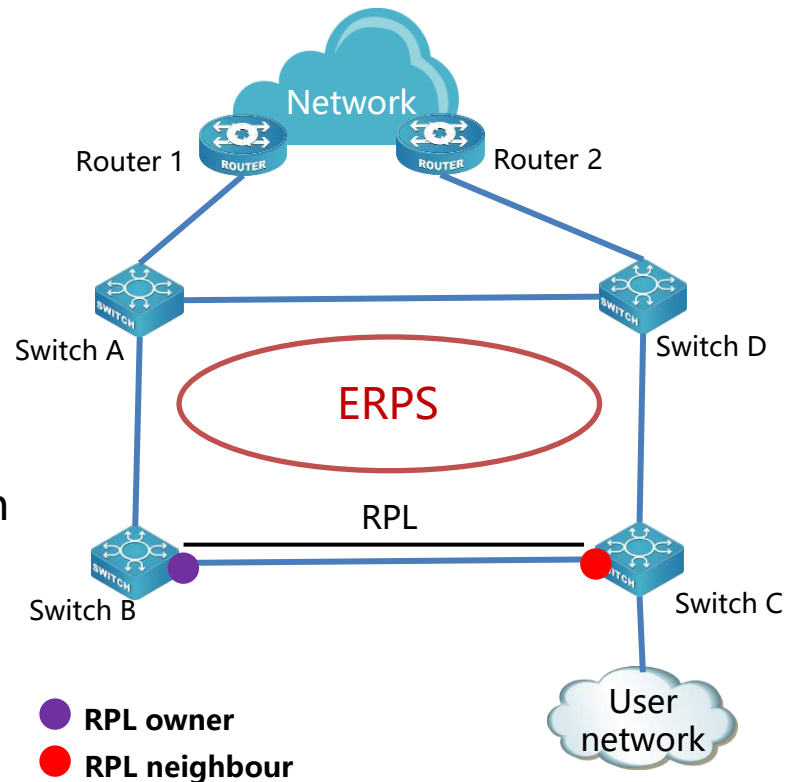
Normal:

- All ports except RPL ports, the usual status is open

Notes: Each node cannot join more than two ports in the same ring

Discarding:

- The port only deal with ERPS protocol packets, not forwarding data



Common Network - ERPS traffic forwarding

Control VLAN

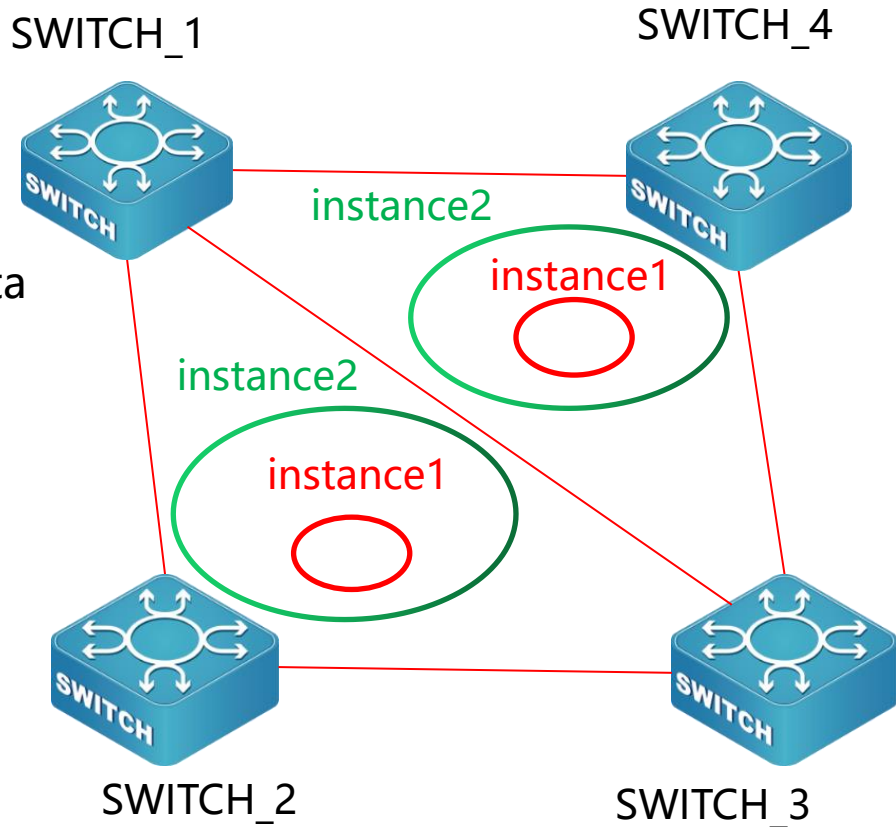
- Forwarding ERPS protocol packet
- Each ERPS should have control VLAN
- Different ERPS rings uses different control VLAN
- In usual, Control VLAN not forwarding data traffic

Data VLAN

- Forwarding data packets

Protected instance

- The mapping relationship of VLAN is the same as the instance of STP
- Each ERPS ring only forwards VLAN traffic within the instance
- Control VLAN is not mandatory



Common Network - Multi ring & Multi instance **DCN** 业务定义网络

Common configuration:

spanning-tree mst configuration

instance 0 VLAN 6-9;401-4094

instance 1 VLAN 1

instance 2 VLAN 2

instance 3 VLAN 3

instance 4 VLAN 4

instance 5 VLAN 5

instance 6 VLAN 10-100

instance 7 VLAN 101-200

instance 8 VLAN 201-300

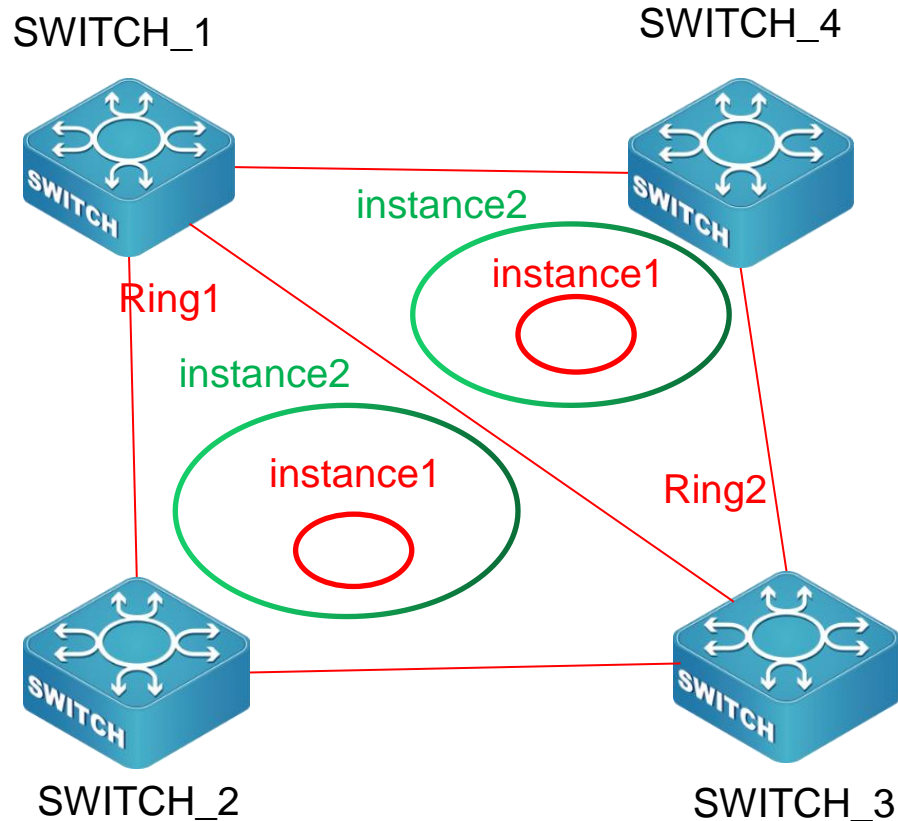
instance 9 VLAN 301-400

exit

!

VLAN 1-500

Each switch must be configured with the VLAN corresponding to the erps of the mstp instance



Common Network - Multi ring & Multi instance DCN 业务定义网络

Ring1 add two erps instance

The instance1 in ring1 is the same with mstp's
protected-instance 1-2;4;6

Command:

```
erps-ring 1
```

```
erps-instance 1
```

```
rpl port0 neighbour
```

```
protected-instance 1-2;4;6
```

```
control-VLAN 2
```

The instance2 in ring1 is same with mstp's
protected-instance 3;5;7

Command:

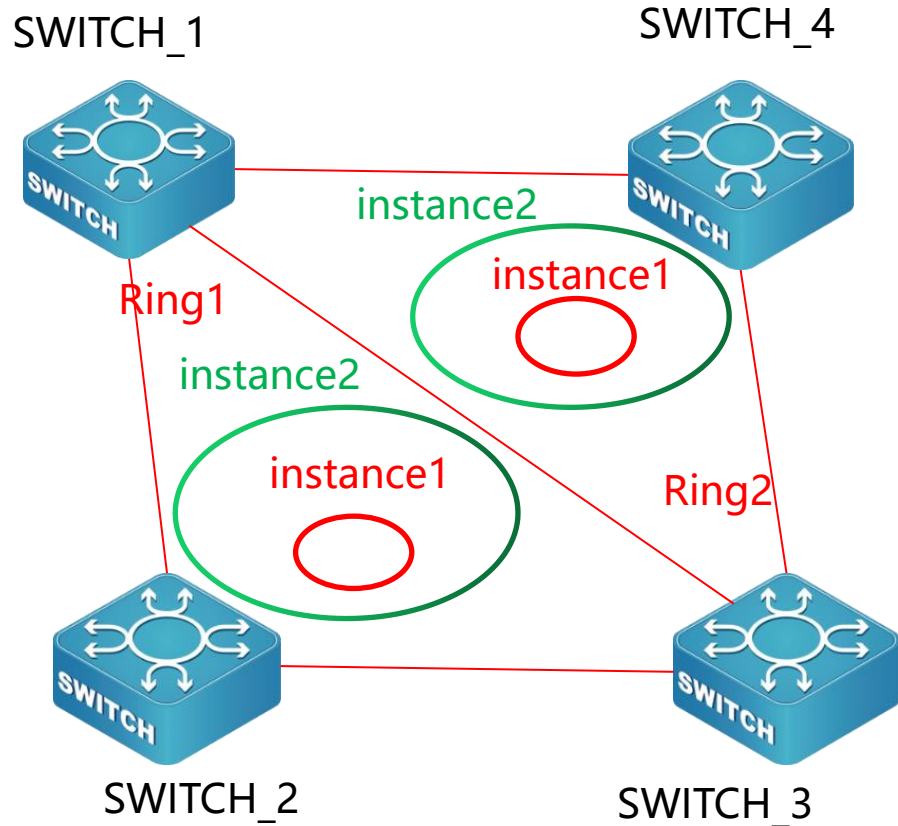
```
erps-ring 1
```

```
erps-instance 1
```

```
rpl port0 neighbour
```

```
protected-instance 3;5;7
```

```
control-VLAN 3
```



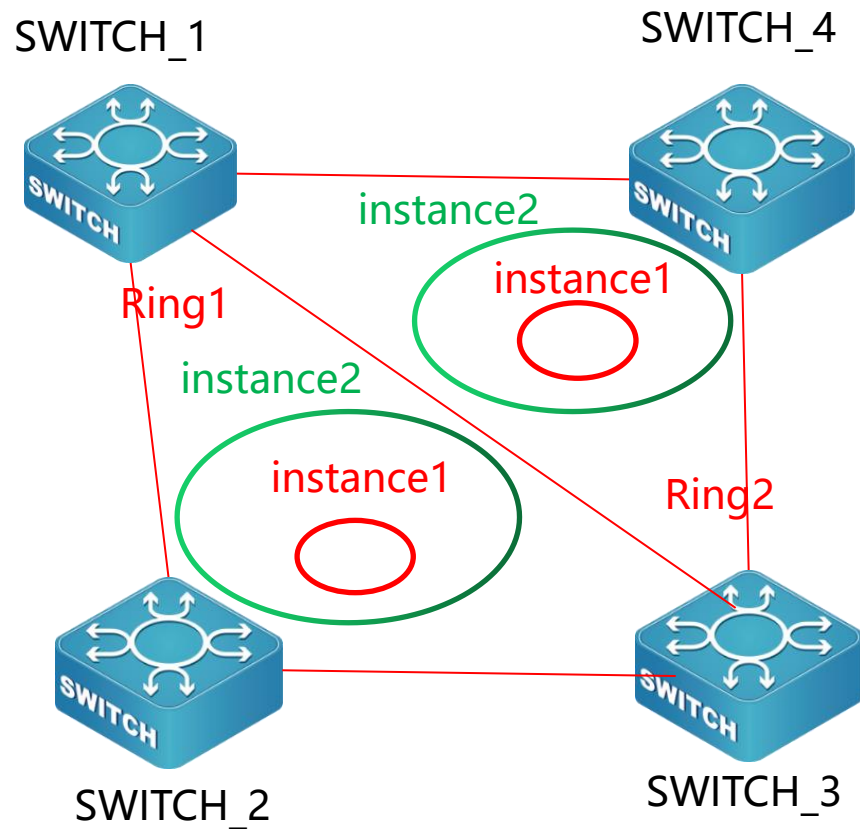
Common Network - Multi ring & Multi instance **DCN** 业务定义网络

For sw1, it is located between two rings, need to configure ring2 also

```
erps-ring 2
erps-instance 1
  rpl port0 owner
  protected-instance 1;6
  control-VLAN 10
exit
erps-instance 2
  protected-instance 7
  control-VLAN 101
```

Configuring the rest switch according to the sw1 erps ring and instance configuration

Notes: Each instance in ring are independent each other, pls refer to mstp. The control VLANs in each instance must be consistent.



Common Network - Multi ring & Multi instance **DCN**

- To check the result of configuration. After configuring successfully, show related configuration running on the switch.
- S2# show erps ring brief
- Ring-ID Description Ring-topo Port0 Port1 Version Inst-Count
- -----
- 1 majior_ring1 majior-ring 1/0/1 1/0/2 V2 1

- Switch#show erps instance
- ERPS Ring majior_ring1
- Instance 1
- Description: instance1
- Protected Instance : 2 Revertive mode: revertive
- RAPS MEL: 3 R-APS-Virtual-Channel:
- Control Vlan : 2
- Guard Timer (csec) : 100
- Holdoff Timer (seconds) : 5
- WTR Timer (min) : 8
- Port Role Port-Status
- -----
- port0 Common Forwarding
- port1 RPL Owner Blocked

Common Network - ERPS running mechanism

1. Only ERPS ring configuration complete would active instance

1.1 Major ring must configure two ERPS ports

1.2 Must configure Control VLAN

1.3 Must configure protected instance

1.4 Sub ring must configure port0, if there were no port1-none configuration, then must configure port1

2. ERPS state figure

2.1 Init: before active ERPS instance

2.2 Idle: The normal stable state of the loop, starting from the RPL owner

2.3 Protection: After link failure

2.4 MS: Manually switch the traffic forwarding path

2.5 FS: Force switching the traffic forwarding path

2.6 Pending: temporary state, unstable

Common Network - State switchover log view

1. Interface down

%Nov 17 13: 00: 30 2020 <critical> MODULE_L2_MAC_NOTIFICATION[tErps]:
Signal failure **detected** on 60-63-fd-82-5d-5f in ERPS ring: 3, instance: 3, port
PORT0

2. Interface up

%Nov 17 13: 00: 30 2020 <critical> MODULE_L2_MAC_NOTIFICATION[tErps]:
Signal failure **cleared** on 60-63-fd-82-5d-5f in ERPS ring: 3, instance: 3, port
PORT0

3. Set port state

%Jan 01 00: 00: 58: 619 2006 <critical> MODULE_L2_ERPS[tErps]:
Ethernet1/0/1 on ring instance 1 is set to **STATE**, reason is **REASON**

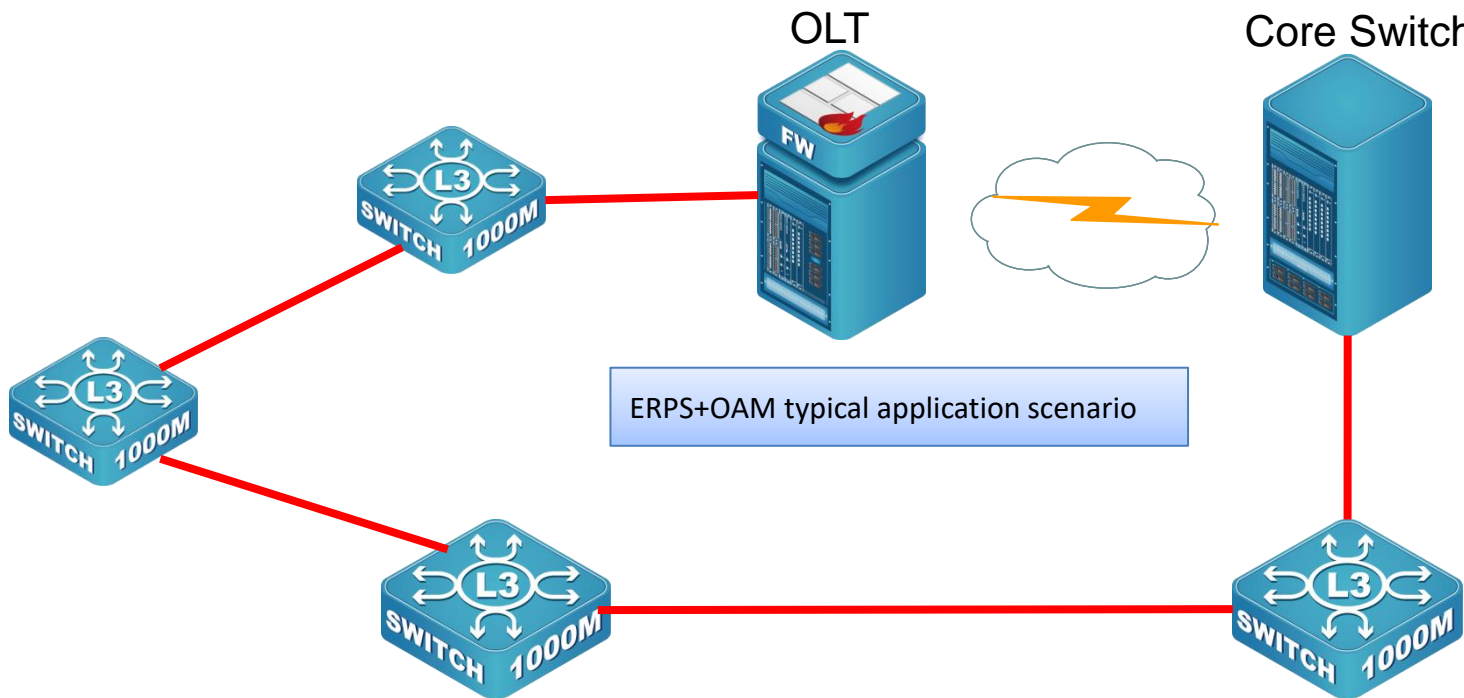
Common Network - State switchover log view

STATE: block or forward

REASON:

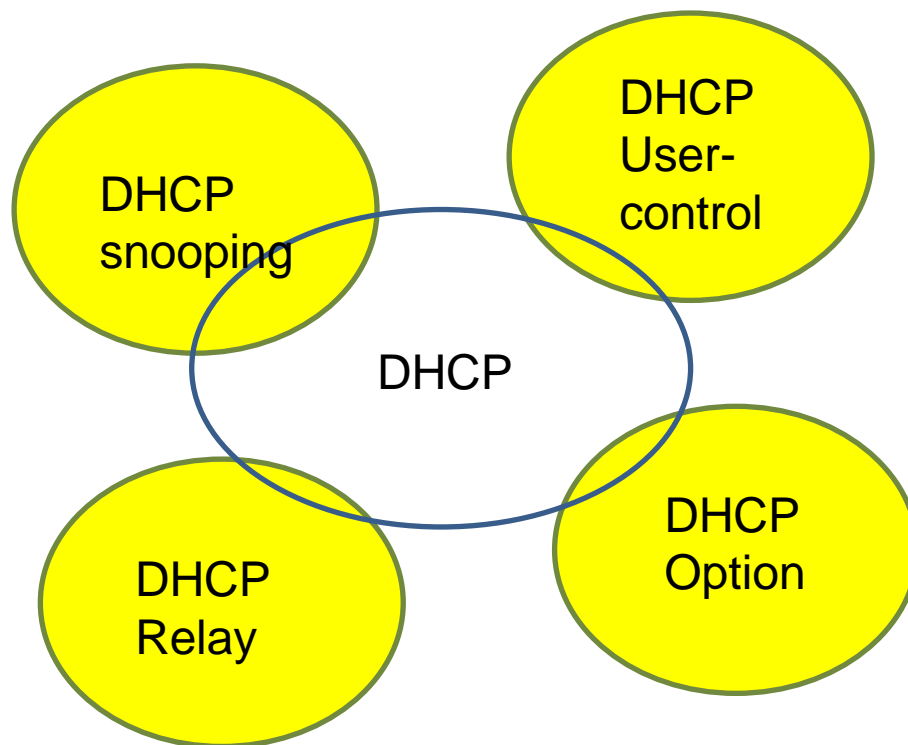
- a) instance unactive: delete ERPS instance、PORT0、PORT1、control VLAN...
- b) config protected instance: configure protected instance
- c) update instance port state: update instance port status
- d) update instance VLAN: update instance VLAN
- e) port group update: update port group
- f) start fsm: start fsm status machine
- g) fsm clear: running clear command
- h) fsm local clear sf: clear Signal Failure locally
- i) fsm local fs: running Forced Switch locally
- j) fsm local ms: running Manual Switch locally
- k) fsm local sf: generate Signal Failure locally
- l) fsm raps fs: receive Forced Switch packets
- m) fsm raps ms: receive Manual Switch packets
- n) fsm raps sf: receive Signal Failure packets
- o) fsm raps nr: receive NR packets
- p) fsm raps nr rb: receive NR-RB packets
- q) fsm wtr-wtb expire: WTR or WTB timer expired

Common Network - ERPS+OAM



03

Common IP Service



Problem: Manually assigning IP addresses requires a lot of work

In the early stage of IP address application, the use range is small, and manual assignment of IP addresses can meet the allocation demand. However, with the increase of users, the use scale of IP addresses is also increasing, and manual assignment is also prone to errors.

Then how we gonna solve this?

DHCP[RFC2131] Abbreviation of Dynamic Host Configuration Protocol , It can dynamically assign IP addresses to the requesting host from the address pool, and also provide other network configuration parameters, such as the default gateway, DNS server, domain name, and the location of host image files within the network range.

DHCP It is a mainstream technology, which reduces the amount of time users spend managing network information. Another advantage of DHCP is that it can partially alleviate the shortage of IP addresses. When a user of an IP address leaves the Network, the IP address can be re-allocated to another user.


```
switch(config)#vlan 10 Create the corresponding vlan10  
switch(config-Vlan10)#ip address 192.168.10.1 255.255.255.0 Config the L3 interface  
switch(config-Vlan10)#exit  
switch(config)#service dhcp Enable DHCP service  
switch(config)#ip dhcp pool vlan10 Create a new dhcp server named vlan10  
switch(dhcp-vlan10-config)#network 192.168.10.1 24 Specify the distribute network segment  
switch(dhcp-vlan10-config)#default-router192.168.10.1 Specify default gateway address  
switch(dhcp-vlan10-config)#exit
```

```
SW2(config)#ip dhcp excluded-address 150.1.1.2
```

If you do not want to assign an address to the terminal, you can exclude this address. For example, the core or aggregation layer 3 interconnection interface can be excluded from the DHCP pool

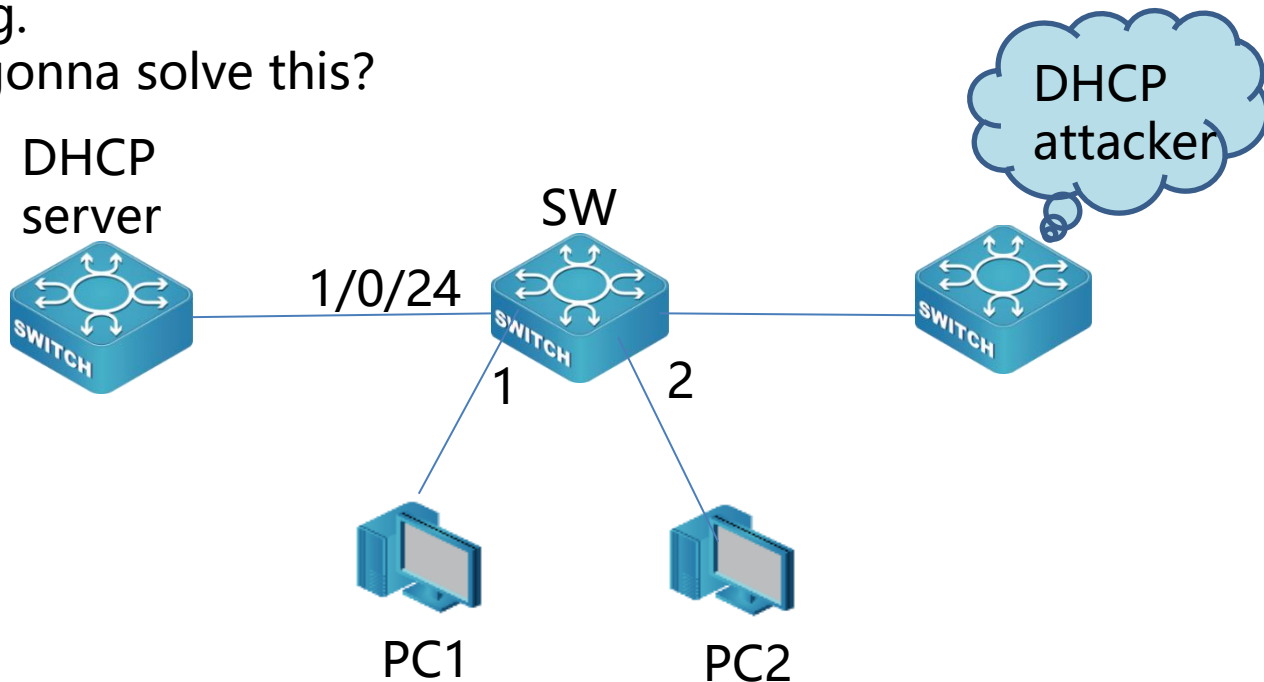
```
SW2(config)#ip dhcp excluded-address 150.1.1.2
```

If u don' t wanna distribute this address to terminal, then just get it excluded. Like the address of core switch or aggregation switch. We can exclude it out of the address pool.

DHCP-DHCP SNOOPING

When a user sets himself as a DHCP SERVER, other users cannot identify him. They may apply for addresses from this illegal DHCP SERVER. These addresses may be unavailable or conflicting.

How we gonna solve this?



DHCP-DHCP SNOOPING Configuration

Trust interface

Function:

switch(config)#ip dhcp snooping enable

Enable DHCP snooping function globally

Switch(config)#ip dhcp snooping vlan 2

Switch(config-if-ethernet1/0/1)#ip dhcp snooping trust

```
sw4#show ip dhcp snooping binding all
ip dhcp snooping static binding count:0, dynamic binding count:1
```

MAC	IP address	Interface	Vlan ID	Flag
68-f7-28-0e-27-1f	150.1.1.2	Ethernet1/0/1	10	D

```
sw4#
sw4#
```

1. Forbidden set private static IP Scenario

The IP address is uniformly assigned by DHCP SERVER. However, if a user configures a static IP address privately, DHCP SERVER will assign the IP address to other users without knowing that the IP address has been used, and there will be IP conflicts.

The **user control** function can be configured for the above problems:

```
Switch(config-if-ethernet1/0/1)#ip dhcp snooping binding user-control
```

After this function is enabled, the port does not allow messages besides DHCP message to pass through. Only after the IP is applied through DHCP and the switch generates the binding table item, can the corresponding IP message pass through.

```
Switch(config-if-ethernet1/0/1)#ip  
dhcp snooping  
binding user-  
control max-user 2
```

```
Switch(config)#ip  
dhcp snooping  
binding arp
```

2.Allow set private static IP senario

After enabled user-control, all terminals can only get IP from DHCP server. What if some clients want to set static IP address?

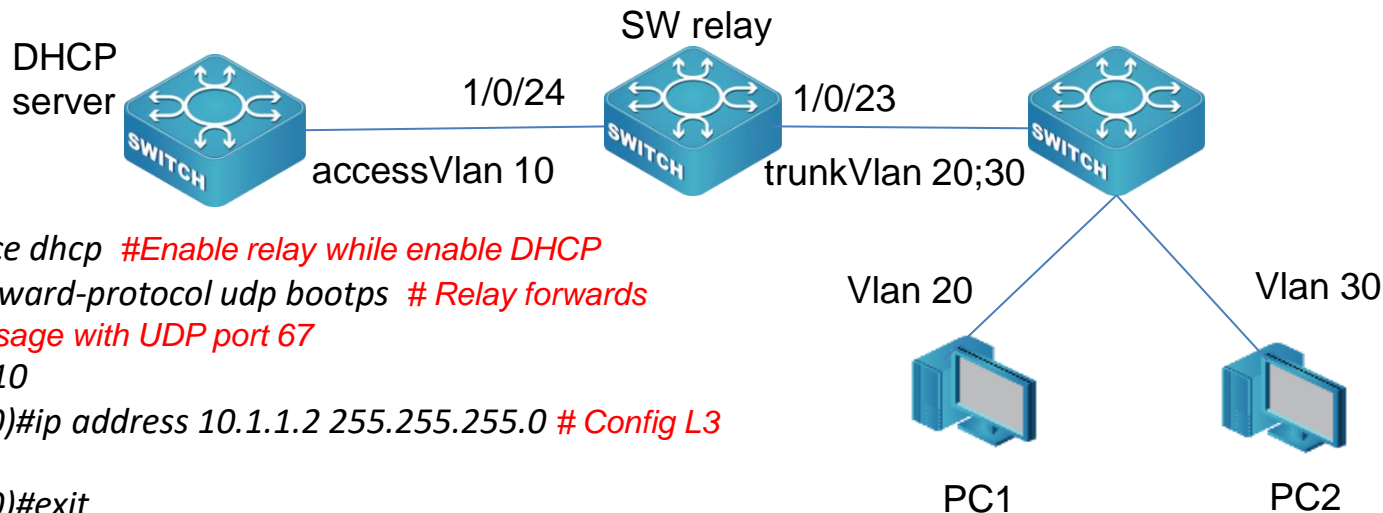
For the issue above we can config static binding table function:

```
Switch(config)#ip dhcp snooping binding user 00-00-00-00-00-01 address 1.1.1.1 vlan 1 interface ethernet 1/0/1
```

After enabled this function, the message of "ip+mac+vlan+port" can pass without DHCP process.

DHCP-DHCP Relay

DHCP discovery message is broadcast message. What if PC1 and PC2 are not in the same IP segment with DHCP server?



```
switch(config)#service dhcp #Enable relay while enable DHCP
switch(config)#ip forward-protocol udp bootps # Relay forwards
DHCP broadcast message with UDP port 67
switch(config)#vlan 10
switch(config-Vlan10)#ip address 10.1.1.2 255.255.255.0 # Config L3
interface
switch(config-Vlan10)#exit
switch(config)#vlan 20
switch(config-Vlan20)#ip address 10.1.2.1 255.255.255.0 # Config L3
interface
switch(config-Vlan20)#ip help-address 10.1.1.1 # Specify the
destination IP for relay forwarding
```

DHCP-DHCP Option

DHCP-option:

Switch(config)#ip dhcp snooping information enable

Switch(config)#ip dhcp snooping information option ?

allow-untrusted Allow DHCP request packet with option-82 information from untrusted port

delimiter Select delimiter in colon(':',), dot('.'), slash('/') and space(' ')

remote-id User remote-id mode

reply DHCP Snooping Information Option Reply

self-defined Self-defined option82 format

subscriber-id User subscriber-id mode

After this function is enabled, add option message into DHCP frame.

DHCP-Debug Dhcp

```
SW2#  
SW2#debug ip dhcp server events  
dhcp event debug is on  
SW2#%Jan 01 00:16:45 2006 DHCPD EVENT: assigned address 150.1.1.2 to the client 68-f7-28-0e-27-1f  
%Jan 01 00:17:10 2006 DHCPD EVENT: client released address 150.1.1.2 to pool  
%Jan 01 00:17:18 2006 DHCPD EVENT: assigned address 150.1.1.2 to the DHCPDISCOVER client 68-f7-28-0e-27-1f  
%Jan 01 00:17:18 2006 DHCPD EVENT: assigned address 150.1.1.2 to the client 68-f7-28-0e-27-1f
```

```
SW2#  
SW2#debug ip dhcp server packets  
dhcp server packet debug is on  
SW2#%Jan 01 00:21:58 2006 DHCPD PACKET: depositing option 60 MSFT 5.0 from request packet  
%Jan 01 00:21:58 2006 DHCPD PACKET: DHCPREQUEST rcvd from client 68-f7-28-0e-27-1f on interface 150.1.1.1  
%Jan 01 00:21:58 2006 DHCPD PACKET: sent DHCPACK to client 68-f7-28-0e-27-1f (150.1.1.2)  
%Jan 01 00:21:58 2006 DHCPD: unicasting BOOTPREPLY to client 68-f7-28-0e-27-1f (150.1.1.2)
```

```
SW2#  
SW2#  
SW2#conf  
SW2(config)#ip dhcp excluded-address 150.1.1.2 ?  
A.B.C.D 高端 IP 地址  
<cr>
```

```
SW2(config)#ip dhcp excluded-address 150.1.1.2  
SW2(config)#  
SW2#%Jan 01 00:24:14 2006 DHCPD PACKET: depositing option 60 MSFT 5.0 from request packet  
%Jan 01 00:24:14 2006 DHCPD PACKET: DHCPREQUEST rcvd from client 68-f7-28-0e-27-1f on interface 150.1.1.1  
%Jan 01 00:24:18 2006 DHCPD PACKET: depositing option 60 MSFT 5.0 from request packet  
%Jan 01 00:24:18 2006 DHCPD PACKET: DHCPREQUEST rcvd from client 68-f7-28-0e-27-1f on interface 150.1.1.1  
%Jan 01 00:24:18 2006 DHCPD PACKET: sent DHCPNAK to client 68-f7-28-0e-27-1f  
%Jan 01 00:24:18 2006 DHCPD: unicasting BOOTPREPLY to client 68-f7-28-0e-27-1f  
%Jan 01 00:24:19 2006 DHCPD PACKET: depositing option 60 MSFT 5.0 from request packet  
%Jan 01 00:24:19 2006 DHCPD PACKET: DHCPDISCOVER rcvd from client 68-f7-28-0e-27-1f on interface 150.1.1.1  
%Jan 01 00:24:19 2006 DHCPD PACKET: sent DHCPPOFFER to client 68-f7-28-0e-27-1f (150.1.1.3)  
%Jan 01 00:24:19 2006 DHCPD: unicasting BOOTPREPLY to client 68-f7-28-0e-27-1f (150.1.1.3)  
%Jan 01 00:24:19 2006 DHCPD PACKET: depositing option 60 MSFT 5.0 from request packet  
%Jan 01 00:24:19 2006 DHCPD PACKET: DHCPREQUEST rcvd from client 68-f7-28-0e-27-1f on interface 150.1.1.1  
%Jan 01 00:24:19 2006 DHCPD PACKET: sent DHCPACK to client 68-f7-28-0e-27-1f (150.1.1.3)  
%Jan 01 00:24:19 2006 DHCPD: unicasting BOOTPREPLY to client 68-f7-28-0e-27-1f (150.1.1.3)
```

Server debug
command:
debug ip dhcp
server events;
debug ip dhcp
server packets

DHCP- enable debug dhcp on snooping device

Command lines to enable debug on snooping devices:

debug ip dhcp snooping binding

debug ip dhcp snooping event

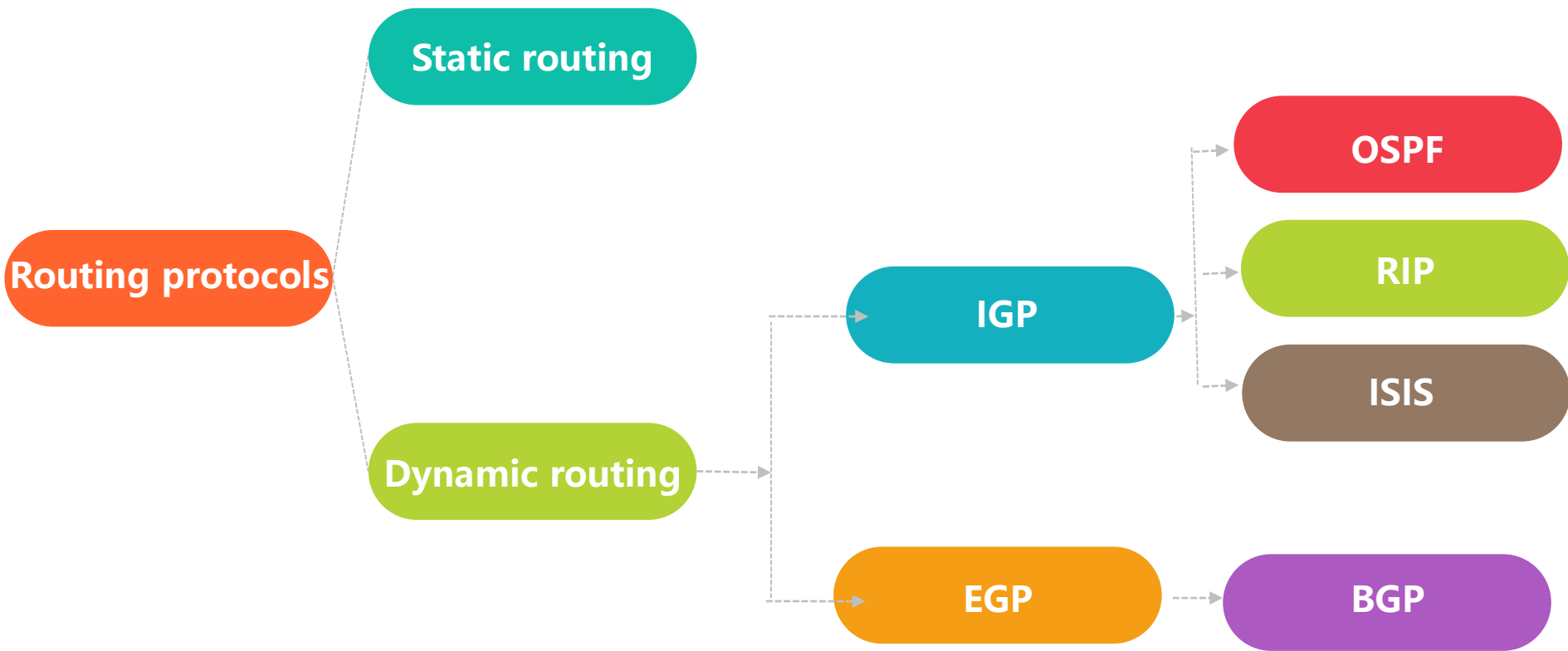
debug ip dhcp snooping packet

debug ip dhcp snooping update

Command lines to enable debug on Relay device:

debug ip dhcp relay packet

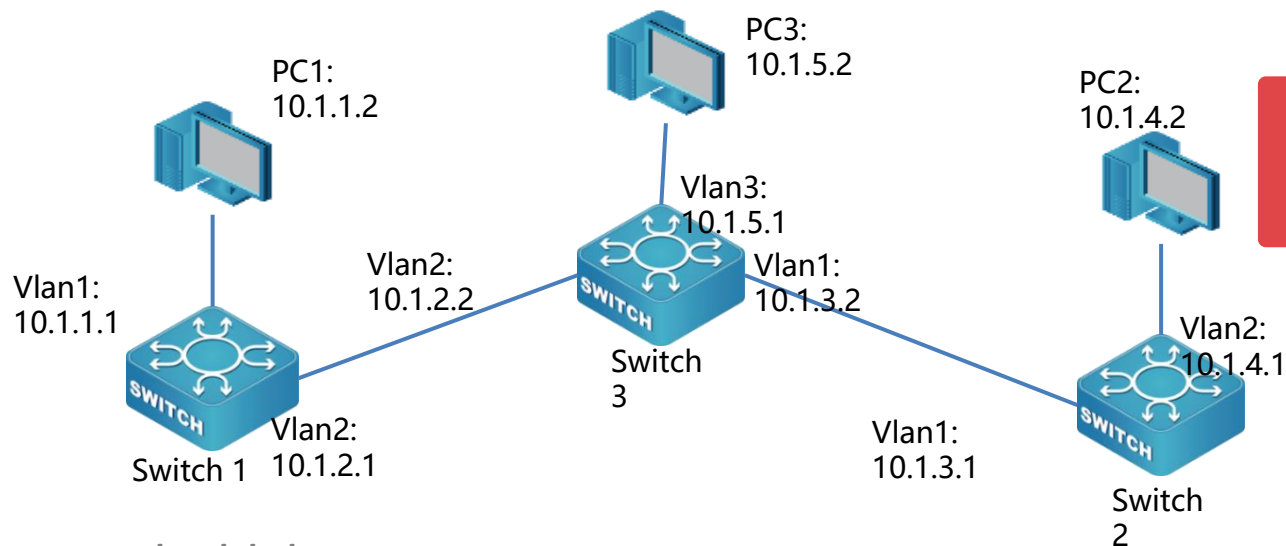
Routing-Introduction of routing protocols



Routing-Static routing

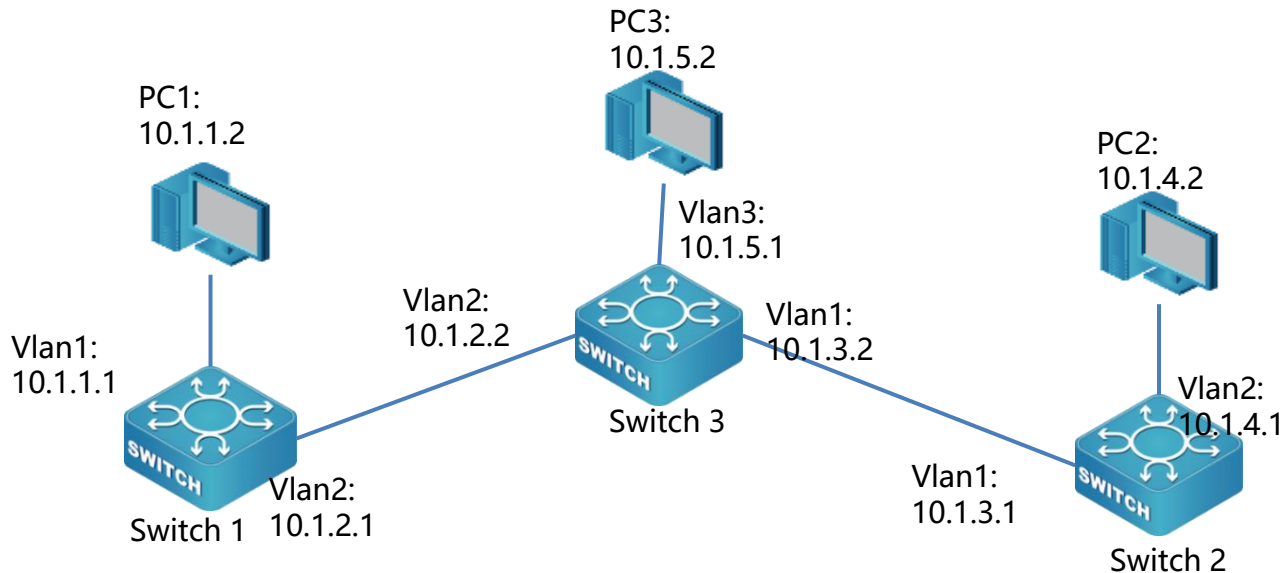
Static routing: Manually specified path to a network or a specific host.

Default route is kind of static routing shown as a route with a destination address of 0.0.0.0 and a network mask of 0.0.0.0



How to realize the interworking of all hosts with static routing

Routing



```
ip route 10.1.5.0 255.255.255.0  
10.1.2.2
```

**Target
network
segment**

**Subnet
mask**

**Next
jump**

```
ip route 0.0.0.0 0.0.0.0 10.1.3.2
```

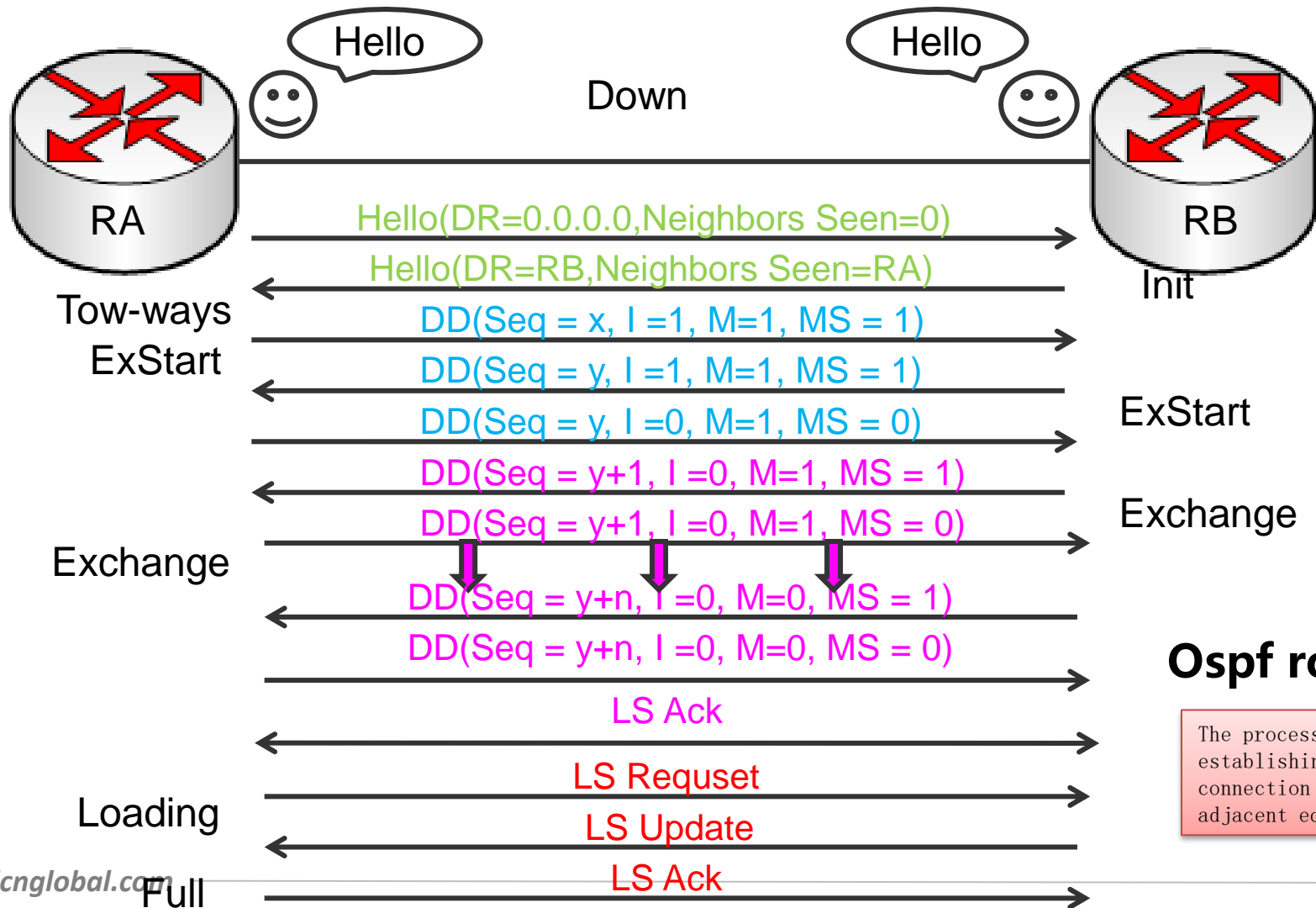
**Default
routing
form**

Routing-OSPF routing protocol

OSPF (Open Shortest Path First)

- Belongs to IGP (interior gateway protocol)
- Routing Protocol Based on Link State Algorithm (SPF)
- Developed by IETF
- Latest version is 2/3
- Related protocols: RFC1583, RFC2178, RFC2328

- No route loop
- Adaptable to large-scale networks
- Fast convergence rate of route change
- Support regional division
- Support ECMP routing
- Support authentication
- Support hierarchical routing management
- Send protocol message with multicast address

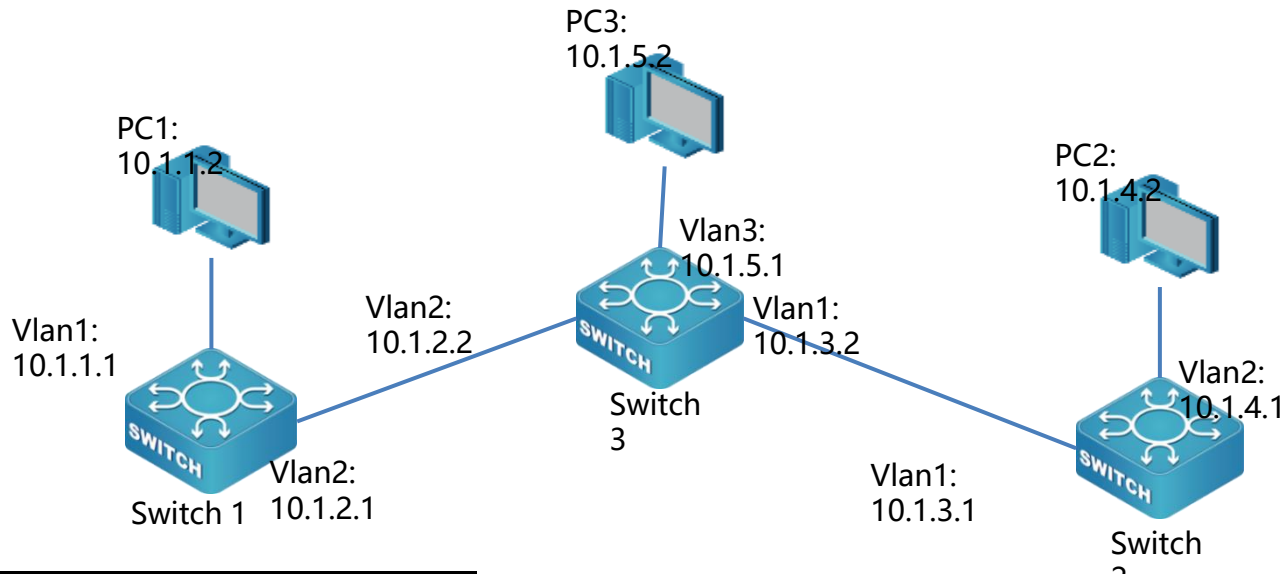


Ospf routing

The process of establishing the connection between adjacent equipment

OSPF

```
router ospf 1
 network 10.1.2.0/24 area 0
 network 10.1.3.0/24 area 0
 redistribute connected
```

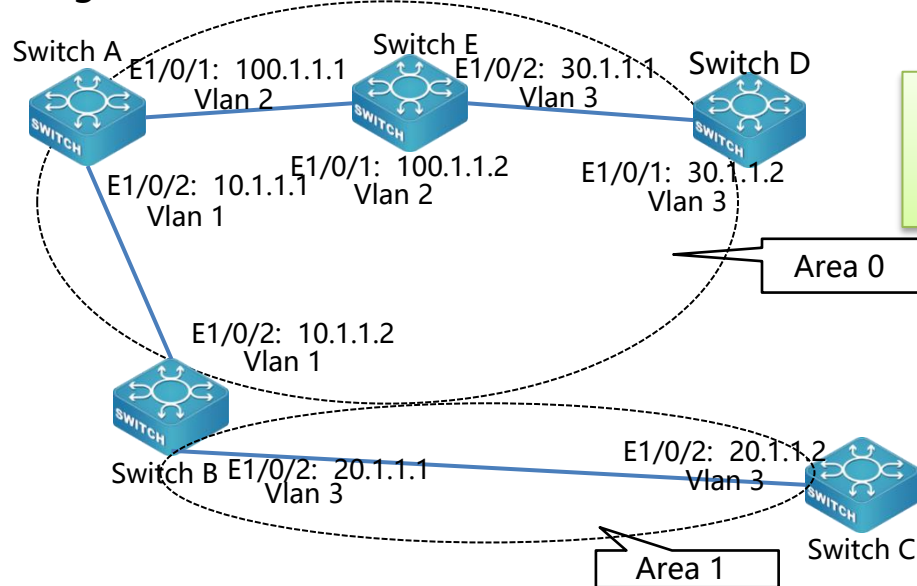


```
router ospf 1
 network 10.1.2.0/24 area 0
 redistribute connected
```

```
router ospf 1
 network 10.1.3.0/24 area 0
 redistribute connected
```

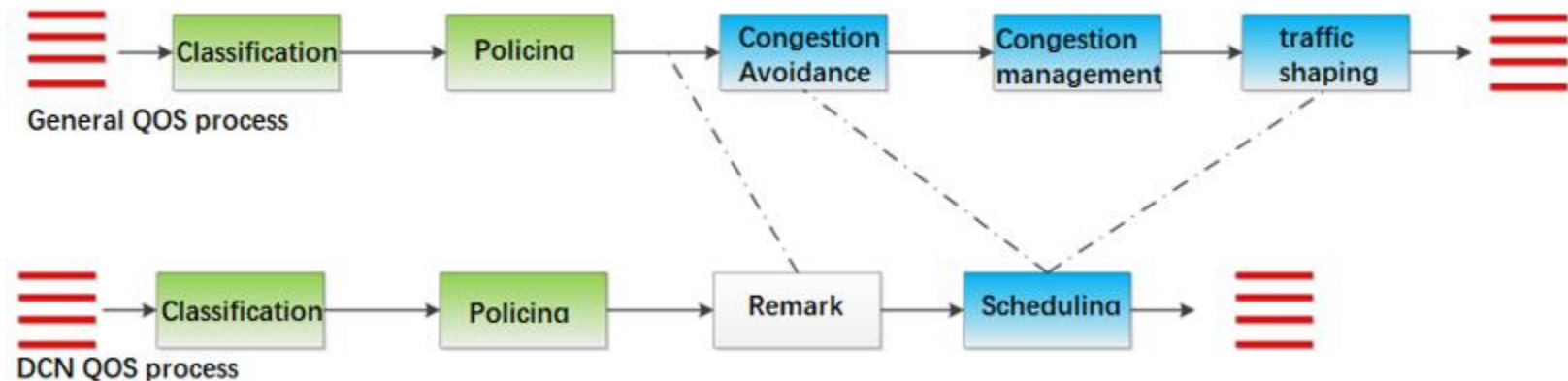
Routing- ospf typical scenario

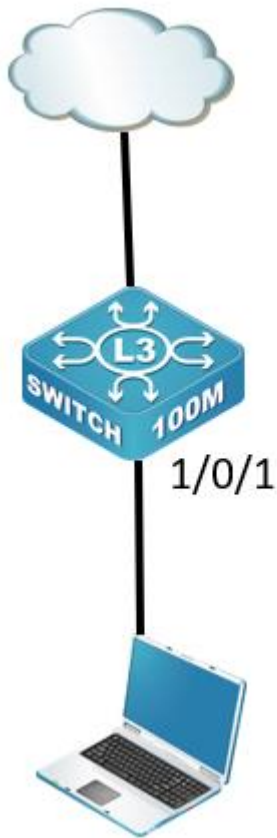
When there are many route entries and the static route configuration is very complex, dynamic routing can be considered BGP is applicable to large networks such as metropolitan area networks. Small and medium-sized networks such as campus networks use ospf, rip, isis, and the most commonly used is ospf. Simple configuration and maintenance.



```
Switch1(config)#router ospf
Switch1(config-router)#network 10.1.1.0/24 area 0
Switch1(config-router)#network 100.1.1.0/24 area 0
```


QoS (Quality of Service) It refers to the ability to use a variety of technologies to provide better services to selected network.





The background is XX enterprise build a new network, dedicate 40M bandwidth from the ISP. The staff (150.1.1.0/24) 's online bandwidth can reach up to 30M without any limitation. And the company need to ensure the quality of the production network 192.168.1.0/24.

Scenario 1: To ensure the quality of the production network, set the interface connecting the production network to trust cos, and adjust the priority so that the messages of the production network will be forwarded first

```
Switch#show mls qos maps

Ingress COS-TO-Internal-Priority map:
COS:  0   1   2   3   4   5   6   7
-----
INTP: 0   1   2   3   4   5   6   7

Switch(config)#int e 1/0/11
Switch(config-if-ethernet1/0/11)#mls qos trust cos
Switch(config-if-ethernet1/0/11)#mls qos cos 5
Switch(config-if-ethernet1/0/11)#q
Switch(config)#mls qos map cos-intp 0 1 2 3 4 7 6 7
Switch#show mls qos maps

Ingress COS-TO-Internal-Priority map:
COS:  0   1   2   3   4   5   6   7
-----
INTP: 0   1   2   3   4   7   6   7
```

Scenario 2: To ensure the quality of the production network, it is required to limit the speed of the network segment for employees to 10M

```
vlan 1
!
access-list 1 permit 150.1.1.0 0.0.0.255
!
policy-map
!
policy-map
class c1
policy 10000 burst-group 1
accounting
exit
!
Interface Ethernet1/0/1
service-policy input p1
```

Modify here to
change the rate limit

[5]	13.00-14.00	sec	3.46 MBytes	29.1 Mbits/sec	0.037 ms	14/457 (3.1%)
[5]	14.00-15.00	sec	3.55 MBytes	29.8 Mbits/sec	0.031 ms	1/455 (0.22%)
[5]	15.00-16.00	sec	3.47 MBytes	29.1 Mbits/sec	0.025 ms	13/457 (2.8%)
[5]	16.00-17.01	sec	3.43 MBytes	28.5 Mbits/sec	0.034 ms	19/458 (4.1%)
[5]	17.01-18.01	sec	3.57 MBytes	29.9 Mbits/sec	0.043 ms	0/457 (0%)
[5]	18.01-19.01	sec	3.58 MBytes	30.2 Mbits/sec	0.048 ms	0/458 (0%)
[5]	19.01-20.00	sec	3.57 MBytes	30.1 Mbits/sec	0.038 ms	0/457 (0%)
[5]	20.00-21.00	sec	1.16 MBytes	9.76 Mbits/sec	0.048 ms	279/428 (65%)
[5]	21.00-22.00	sec	1.12 MBytes	9.39 Mbits/sec	0.070 ms	317/460 (69%)
[5]	22.00-23.00	sec	1.10 MBytes	9.25 Mbits/sec	0.069 ms	316/457 (69%)
[5]	23.00-24.00	sec	1.11 MBytes	9.30 Mbits/sec	0.058 ms	316/458 (69%)
[5]	24.00-25.01	sec	1.10 MBytes	9.13 Mbits/sec	0.044 ms	316/457 (69%)
[5]	25.01-26.01	sec	1.11 MBytes	9.31 Mbits/sec	0.068 ms	315/457 (69%)
[5]	26.01-27.01	sec	1.09 MBytes	9.14 Mbits/sec	0.061 ms	320/459 (70%)
[5]	27.01-28.01	sec	1.11 MBytes	9.22 Mbits/sec	0.052 ms	316/458 (69%)

Scenario 3: Due to the increase of turnover and profit, the company changed the bandwidth of 50M for export. In order to improve the online experience of employees as much as possible on the premise of ensuring the quality of production network, it is required to limit the network segment for employees to 10M. If the speed of employees' online access exceeds 10M, 5M bursts will be provided

```

vlan 1
!
access-list 1 permit 150.1.1.0 0.0.0.255
!
class-map c1
match access-group 1
!
policy-map p1
class c1
policy 10240 10240 pir 15360 15360 conform-action transmit exceed-action transmit
accounting
exit
!
Interface Ethernet1/0/1
service-policy input p1
    
```

committed
value+bursts

5]	106.00-107.00	sec	2.05	MBytes	17.2	Mbits/sec	0.203	ms	194/457	(42%)
5]	107.00-108.00	sec	2.30	MBytes	19.3	Mbits/sec	0.197	ms	183/457	(38%)
5]	108.00-109.00	sec	2.32	MBytes	19.5	Mbits/sec	0.206	ms	181/458	(35%)
5]	109.00-110.00	sec	2.29	MBytes	19.2	Mbits/sec	0.173	ms	184/457	(36%)
5]	110.00-111.00	sec	2.39	MBytes	20.1	Mbits/sec	0.221	ms	150/456	(33%)
5]	111.00-112.00	sec	2.29	MBytes	19.2	Mbits/sec	0.164	ms	185/458	(36%)
5]	112.00-113.00	sec	2.41	MBytes	20.2	Mbits/sec	0.209	ms	150/458	(33%)
5]	113.00-114.00	sec	2.23	MBytes	18.7	Mbits/sec	0.170	ms	170/456	(37%)
5]	114.00-115.00	sec	2.64	MBytes	22.1	Mbits/sec	0.208	ms	119/457	(26%)
5]	115.00-116.00	sec	2.17	MBytes	18.2	Mbits/sec	0.199	ms	180/458	(39%)
5]	116.00-117.00	sec	1.97	MBytes	18.5	Mbits/sec	0.181	ms	202/454	(44%)
5]	117.00-118.00	sec	1.70	MBytes	14.3	Mbits/sec	0.200	ms	242/460	(53%)
5]	118.00-119.00	sec	1.72	MBytes	14.4	Mbits/sec	0.186	ms	238/458	(52%)
5]	119.00-120.00	sec	1.70	MBytes	14.3	Mbits/sec	0.175	ms	239/457	(52%)
5]	120.00-121.00	sec	1.72	MBytes	14.4	Mbits/sec	0.241	ms	237/457	(52%)
5]	121.00-122.00	sec	1.74	MBytes	14.6	Mbits/sec	0.207	ms	238/461	(52%)
5]	122.00-123.00	sec	1.70	MBytes	14.3	Mbits/sec	0.206	ms	239/457	(52%)
5]	123.00-124.00	sec	1.71	MBytes	14.4	Mbits/sec	0.185	ms	237/456	(52%)
5]	124.00-125.00	sec	1.70	MBytes	14.3	Mbits/sec	0.188	ms	239/457	(52%)
5]	125.00-126.00	sec	1.70	MBytes	14.3	Mbits/sec	0.244	ms	240/458	(52%)
5]	126.00-127.00	sec	1.70	MBytes	14.3	Mbits/sec	0.243	ms	239/457	(52%)
5]	127.00-128.00	sec	1.71	MBytes	14.4	Mbits/sec	0.200	ms	238/457	(52%)

Scenario 4: After the profit growth, the company has newly deployed a monitoring system and added a monitoring network segment of 150.1.2.0/24. The company requires that the monitoring network segment be limited to 10M on the premise of ensuring that employees can access the Internet for 10M and a burst of 5M

Employee

```

vlan 1
!
access-list 1 permit 150.1.1.0 0.0.0.255
access-list 2 permit 150.1.2.0 0.0.0.255
!
class-map 2
 match access-group 2
!
class-map c1
 match access-group 1
!
policy-map p1
 class c1
  policy 10240 10240 pir 15360 15360 conform-action transmit exceed-action transmit
 accounting
 exit
 class 2
  policy 10000 10000 conform-action transmit exceed-action drop
 exit
!
Interface Ethernet1/0/1
 service-policy input p1
  
```

5	8.00-9.00	sec	2.96 MBytes	24.8 Mbits/sec	0.195 ms	78/457 (17%)
5	9.00-10.00	sec	2.57 MBytes	21.6 Mbits/sec	0.202 ms	113/442 (26%)
5	10.00-11.00	sec	2.45 MBytes	20.8 Mbits/sec	0.153 ms	157/471 (33%)
5	11.00-12.00	sec	2.51 MBytes	21.0 Mbits/sec	0.191 ms	120/441 (27%)
5	12.00-13.00	sec	2.52 MBytes	21.1 Mbits/sec	0.215 ms	135/457 (30%)
5	13.00-14.00	sec	2.73 MBytes	22.9 Mbits/sec	0.153 ms	130/480 (27%)
5	14.00-15.00	sec	3.57 MBytes	29.9 Mbits/sec	0.184 ms	0/457 (0%)
5	15.00-16.00	sec	2.70 MBytes	22.6 Mbits/sec	0.153 ms	90/435 (21%)
5	16.00-17.00	sec	2.93 MBytes	24.2 Mbits/sec	0.200 ms	95/464 (20%)
5	17.00-18.00	sec	2.93 MBytes	24.6 Mbits/sec	0.153 ms	81/456 (18%)
5	18.00-19.00	sec	2.81 MBytes	23.6 Mbits/sec	0.180 ms	95/456 (21%)
5	19.00-20.00	sec	1.75 MBytes	14.7 Mbits/sec	0.217 ms	231/455 (51%)
5	20.00-21.00	sec	1.70 MBytes	14.3 Mbits/sec	0.201 ms	239/457 (52%)
5	21.00-22.00	sec	1.70 MBytes	14.2 Mbits/sec	0.200 ms	240/457 (53%)
5	22.00-23.00	sec	1.70 MBytes	14.3 Mbits/sec	0.175 ms	239/457 (52%)
5	23.00-24.00	sec	1.71 MBytes	14.4 Mbits/sec	0.145 ms	238/457 (52%)
5	24.00-25.00	sec	1.73 MBytes	14.5 Mbits/sec	0.248 ms	236/458 (52%)
5	25.00-26.00	sec	1.72 MBytes	14.4 Mbits/sec	0.181 ms	237/457 (52%)
5	26.00-27.00	sec	1.71 MBytes	14.4 Mbits/sec	0.231 ms	242/461 (52%)
5	27.00-28.00	sec	1.70 MBytes	14.3 Mbits/sec	0.176 ms	240/458 (52%)
5	28.00-29.00	sec	1.70 MBytes	14.3 Mbits/sec	0.202 ms	238/456 (52%)
5	29.00-30.00	sec	1.74 MBytes	14.6 Mbits/sec	0.193 ms	237/460 (52%)
5	30.00-30.13	sec	160 KBytes	10.1 Mbits/sec	0.231 ms	25/45 (56%)

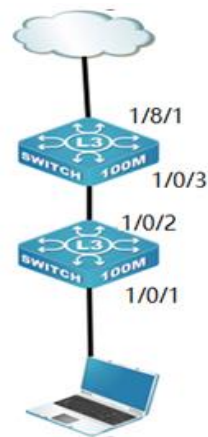
Monitor system

5	5.00-6.00	sec	2.82 MBytes	23.7 Mbits/sec	0.202 ms	96/457 (21%)
5	6.00-7.00	sec	2.52 MBytes	21.1 Mbits/sec	0.149 ms	157/479 (33%)
5	7.00-8.00	sec	2.84 MBytes	23.9 Mbits/sec	0.206 ms	93/457 (20%)
5	8.00-9.00	sec	2.93 MBytes	24.6 Mbits/sec	0.160 ms	82/457 (18%)
5	9.00-10.00	sec	2.88 MBytes	24.1 Mbits/sec	0.201 ms	74/442 (17%)
5	10.00-11.00	sec	3.09 MBytes	26.1 Mbits/sec	0.214 ms	61/457 (13%)
5	11.00-12.00	sec	2.67 MBytes	22.4 Mbits/sec	0.222 ms	114/456 (25%)
5	12.00-13.00	sec	2.70 MBytes	22.6 Mbits/sec	0.230 ms	113/458 (25%)
5	13.00-14.00	sec	2.98 MBytes	25.0 Mbits/sec	0.143 ms	97/479 (20%)
5	14.00-15.00	sec	3.05 MBytes	25.6 Mbits/sec	0.157 ms	66/457 (14%)
5	15.00-16.00	sec	1.62 MBytes	13.6 Mbits/sec	0.224 ms	215/423 (51%)
5	16.00-17.00	sec	1.10 MBytes	9.24 Mbits/sec	0.265 ms	317/458 (69%)
5	17.00-18.00	sec	1.09 MBytes	9.18 Mbits/sec	0.244 ms	317/457 (69%)
5	18.00-19.00	sec	1.09 MBytes	9.11 Mbits/sec	0.234 ms	321/460 (70%)
5	19.00-20.00	sec	1.11 MBytes	9.31 Mbits/sec	0.213 ms	318/458 (69%)
5	20.00-21.00	sec	1.12 MBytes	9.44 Mbits/sec	0.191 ms	315/459 (68%)
5	21.00-22.00	sec	1.11 MBytes	9.31 Mbits/sec	0.215 ms	315/457 (68%)
5	22.00-23.00	sec	1.11 MBytes	9.31 Mbits/sec	0.178 ms	314/456 (68%)
5	23.00-24.00	sec	1.08 MBytes	9.04 Mbits/sec	0.200 ms	322/480 (70%)
5	24.00-25.00	sec	1.11 MBytes	9.31 Mbits/sec	0.318 ms	315/457 (68%)
5	25.00-26.00	sec	1.11 MBytes	9.31 Mbits/sec	0.249 ms	315/457 (68%)
5	26.00-27.00	sec	1.12 MBytes	9.46 Mbits/sec	0.245 ms	315/459 (68%)
5	27.00-28.00	sec	1.11 MBytes	9.31 Mbits/sec	0.171 ms	315/457 (68%)

```
access-list 1 permit 150.1.1.0 0.0.0.255
access-list 2 permit 150.1.2.0 0.0.0.255
access-list 3 permit 150.1.3.0 0.0.0.255
access-list 4 permit 150.1.4.0 0.0.0.255
!
class-map 2
match access-group 2
!
class-map 3
match access-group 3
!
class-map 4
match access-group 4
!
class-map c1
match access-group 1
!
policy-map p1
class c1
set cos 1
exit
class 2
set cos 2
exit
class 3
set cos 3
exit
class 4
set cos 4
exit
!
Interface Ethernet1/0/1
service-policy input p1
```

Scenario 5:

The company continued to make profits, bought a new switch, re planned the network and divided its employees into eight departments. Hopes that the proportion of online bandwidth of the four departments is 2: 2: 2: 4: 4: 4: 4



SW2:

```
mls qos queue algorithm wdr
mls qos queue wdr weight 2 2 2 2 4 4 4 4
```

Port Name	Vlan 0 - Priority (bits)	Destination (IPv4)	Stream Index	Rx Count (Frames)	Rx Count (bits)	Rx Rate (bps)	Rx LI Count (bits)	Rx LI Rate (bps)	Rx Sig Count (Frames)	Rx Rate (fps)
1/0/1	000	192.0.0.1	0	43,470	89,026,560	16,666,664	95,991,760	17,968,750	43,470	8,138
1/0/1	001	192.0.0.1	1	43,470	89,026,560	16,666,664	95,991,760	17,968,750	43,470	8,138
1/0/1	010	192.0.0.1	2	43,470	89,026,560	16,666,664	95,991,760	17,968,750	43,470	8,138
1/0/1	011	192.0.0.1	3	21,735	89,026,560	16,667,968	92,504,160	17,319,061	21,735	4,069
1/0/1	100	192.0.0.1	4	43,471	178,057,216	33,334,632	185,012,576	34,636,770	43,471	8,139
1/0/1	101	192.0.0.1	5	43,470	178,053,120	33,334,632	185,008,320	34,636,770	43,470	8,139
1/0/1	110	192.0.0.1	6	31,795	178,052,000	33,335,880	183,139,200	34,288,330	31,795	5,953
1/0/1	111	192.0.0.1	7	31,796	178,057,600	33,335,880	183,144,960	34,288,330	31,796	5,953

Qos- QOS trouble shooting

1. To measure the effect of dropping priority, WRED support is required. some specific models do not support the WRED discard algorithm
2. After modifying the cos on a device and entering the queue, the original cos of the message is still matched
3. The WRR specific gravity can be modified on some specific models, such as the S4600. But there is a problem. The percentage of packets in each queue is set to 127, if it is greater than or equal to 127, and the original value is maintained if it is less than 127. This is effective normally

S4600-52P-SI(config-if-ethernet1/0/3)#mls qos queue wrr weight 120 3000 4000 126 3000 3000 3000 3000

Info: actual weight is 120, 127, 127, 126, 127, 127, 127, 127

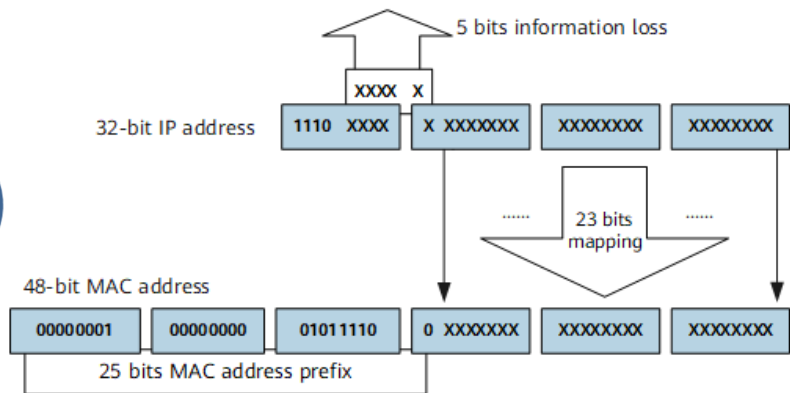
04

Multicast

Multicast-multicast address

IP address	meaning
224.0.0.0 ~ 224.0.0.255	Permanent group address. Address 224.0.0.0 is reserved and not allocated. Other addresses are used for routing protocol
224.0.1.0 ~ 231.255.255.255	ASM multicast address ,is valid in the whole network.
232.0.0.0 ~ 238.255.255.255	SSM multicast address ,is valid in the whole network.
239.0.0.0 ~ 239.255.255.255	The local management group address is only valid in the local management domain. Repeated use of the same local management group address in different management domains will not cause conflicts.

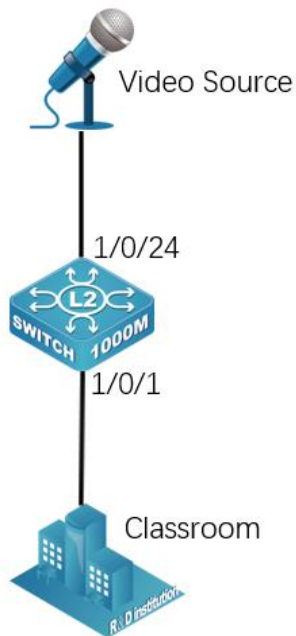
IANA stipulates that the upper 24 bits of the IPv4 multicast MAC address are 0x01005e, the 25th bit is 0, and the lower 23 bits are the lower 23 bits of the IPv4 multicast address



Multicast-Scenarios

Scenario 1: In a primary school, all classrooms are required to see demonstration videos when playing eye exercises

Without SW config



Broadcast room video:

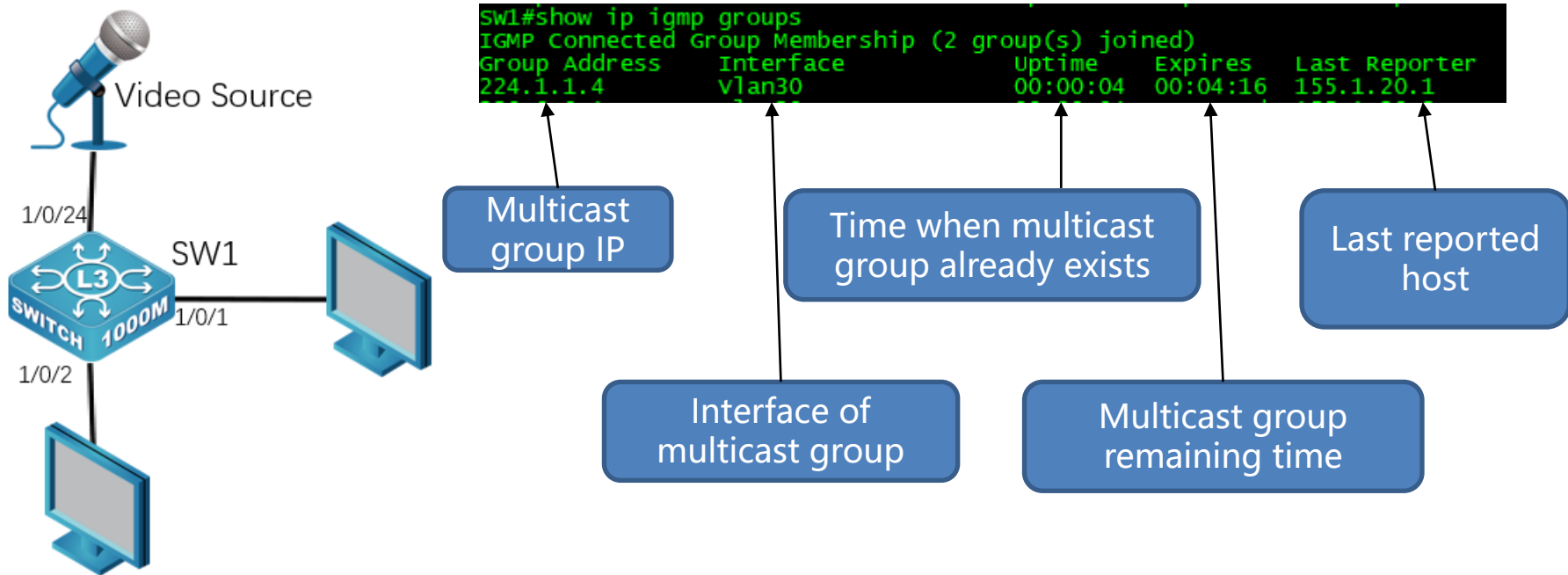


Videos in every classroom:

[illegible]

Multicast- IGMP

Scenario 2: The school requires to know which videos are playing.

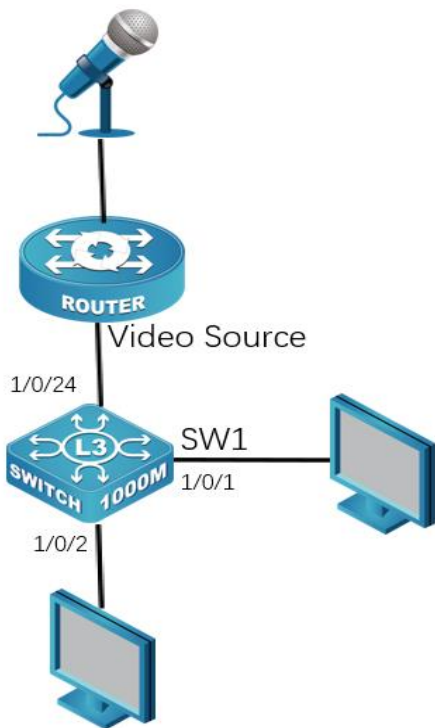


Multicast- IGMP

Protocol	IGMPv1	IGMPv2	IGMPv3
Querier election method	elect by Multicast Routing Protocol PIM	elect between multicast routers in the same network segment	elect between multicast routers in the same network segment
Specific group query message	No	Yes	Yes
Member leaving message	No	Yes	no special member leaving message, and member leaving is report by specific type of report message
Specific source group query message	No	No	Yes
Specify multicast source	No	No	Yes
Identifiable message protocol version	IGMPv1	IGMPv1、IGMPv2	IGMPv1、IGMPv2、IGMPv3
ASM model	Yes	Yes	Yes
SSM model	Need IGMP SSM Mapping	Need IGMP SSM Mapping	Yes

Multicast- IGMP Snooping

Scenario 3: The school requires to reduce the flooding of multicast traffic in the broadcast domain and only send multicast information to the required terminals



```
!
ip igmp snooping
ip igmp snooping vlan 10
ip igmp snooping vlan 10 12-general-querier
ip igmp snooping vlan 10 mrouter-port interface Ethernet1/0/24
!
```

```
SW1#show ip igmp snooping vlan 10
Igmp snooping information for vlan 10
```

```

Igmp snooping L3 multicasting           :running
Igmp snooping L2 general querier        :Yes(SUPPRESSED)
Igmp snooping query-interval            :125(s)
Igmp snooping max response time         :10(s)
Igmp snooping specific-query max response time :1(s)
Igmp snooping robustness                 :2
Igmp snooping mrouter port keep-alive time :255(s)
Igmp snooping query-suppression time    :255(s)
```

IGMP Snooping Connect Group Membership

Note: *-All Source, (s)- Include Source, [s]-Exclude Source

Groups	Sources	Ports	Exptime	SrcMac	System Level
224.1.1.4	*	Ethernet1/0/1	00:02:51	38:F3:AB:89:89:20	V3
239.0.0.1	(155.1.10.1)	Ethernet1/0/1	00:02:45	54:89:98:49:16:9A	V3
239.255.102.18	*	Ethernet1/0/1	00:02:50	38:F3:AB:89:89:20	V3
239.255.255.250	*	Ethernet1/0/1	00:02:49	38:F3:AB:89:89:20	V3
		Ethernet1/0/24	00:02:54	38:F3:AB:89:89:21	V3

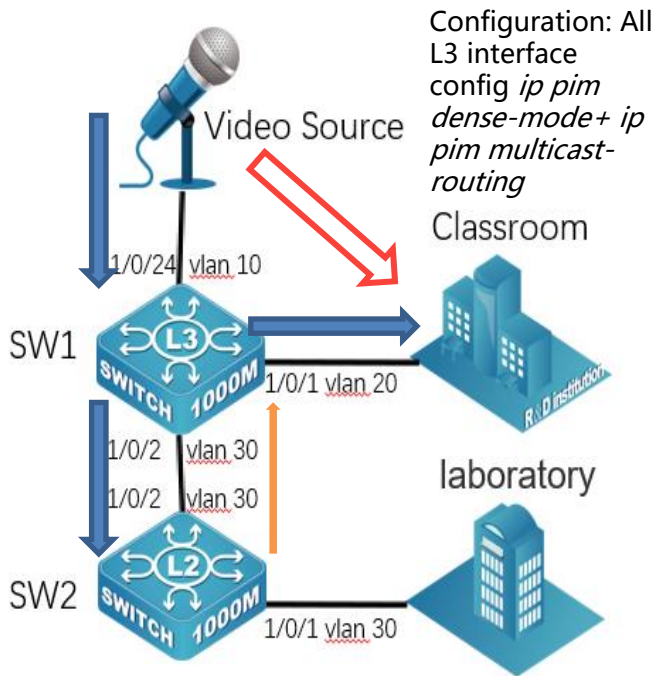
```
IGMP snooping vlan 10 current/limit groups :4/50
```

```

Igmp snooping vlan 10 mrouter port
Note:!"-static mrouter port
!Ethernet1/0/24
```

Multicast - PIM-DM

Scenario 2: When the school requires to play the video, only most of the classrooms in the teaching building can see the demonstration video. Other buildings will not attempt to receive multicast messages, nor do they want multicast traffic flooding



```
SW1#show ip igmp groups 224.1.1.4
IGMP Connected Group Membership(4 group(s) joined)
Group Address      Interface      Uptime      Expires      Last Reporter
224.1.1.4          vlan20        00:02:01    00:03:28    155.1.20.1
SW1#show ip pim neighbor
Neighbor           Interface      Uptime/Expires  Ver  DR
Address            Interface      Uptime/Expires  Ver  Priority/Mode
155.1.30.253       vlan30        00:01:42/00:01:41 v2   1 /
```

```
SW1#show ip mroute 224.1.1.4
Name: Ethernet0, Index: 1158, State: 1002
Name: Loopback, Index: 17500, State: 49
Name: vlan10, Index: 11010, State: 1043
Name: vlan20, Index: 11020, State: 1043
Name: vlan30, Index: 11030, State: 1043
The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0
Group      Origin      Iif      wrong      Oif:TTL
224.1.1.4  155.1.10.1  Vlan10   0          11020:1
                                   11030:1
```

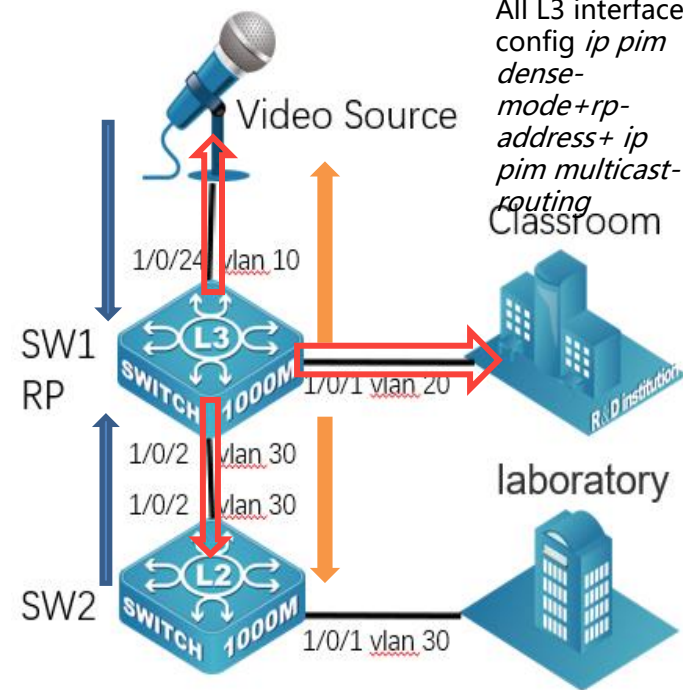
```
SW2#show ip pim neighbor
Neighbor           Interface      Uptime/Expires  Ver  DR
Address            Interface      Uptime/Expires  Ver  Priority/Mode
155.1.30.254       vlan30        00:03:10/00:01:35 v2   1 / DR
```

```
SW2#show ip igmp groups 224.1.1.4
IGMP Connected Group Membership(0 group(s) joined)
Group Address      Interface      Uptime      Expires      Last Reporter
SW2#show ip mroute 224.1.1.4
Name: Ethernet0, Index: 1158, State: 1002
Name: Loopback, Index: 17500, State: 49
Name: vlan30, Index: 11030, State: 1043
The total matched ipmr active mfc entries is 0, unresolved ipmr entries is 1
Group      Origin      Iif      wrong      Oif:TTL
224.1.1.4  155.1.10.1  NULL    4          0:0
```

Multicast- PIM-SM

Scenario 3: The school has re planned and deployed. There are two teacher offices in each building. It is required to play Party members' learning videos every day, which are only visible to teachers

Configuration:
All L3 interface
config *ip pim*
dense-
mode+rp-
address+ ip
pim multicast-
routing
Classroom



```
SW1#show ip igmp groups 224.1.1.4
IGMP Connected Group Membership(4 group(s) joined)
Group Address      Interface      Uptime    Expires    Last Reporter
224.1.1.4          vlan20        00:06:00  00:03:34   155.1.20.1
SW1#show ip pim neighbor
Neighbor           Interface      Uptime/Expires    Ver    DR
Address            Interface      Uptime/Expires    Ver    Priority/Mode
155.1.30.253        vlan30        00:06:13/00:01:23 v2      1 /
```

```
SW1#show ip mroute 224.1.1.4
Name: Ethernet0, Index: 1158, State: 1002
Name: Loopback, Index: 17500, State: 49
Name: Vlan10, Index: 11010, State: 1043
Name: Vlan20, Index: 11020, State: 1043
Name: Vlan30, Index: 11030, State: 1043
Name: pimreg, Index: 1162, State: c1
The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0
Group      origin      iif      wrong      oif:TTL
224.1.1.4  155.1.10.1  vlan10   0          11020:1
```

```
SW2#show ip pim neighbor
Neighbor           Interface      Uptime/Expires    Ver    DR
Address            Interface      Uptime/Expires    Ver    Priority/Mode
155.1.30.254        vlan30        00:10:31/00:01:44 v2      1 / DR
```

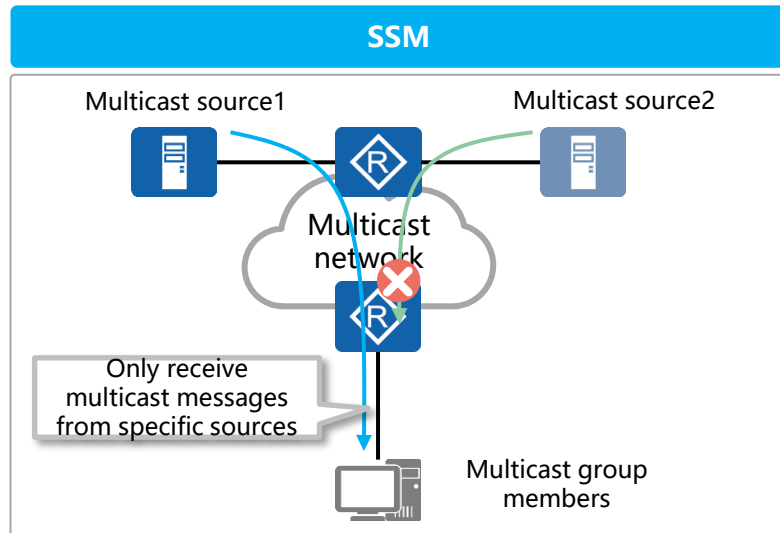
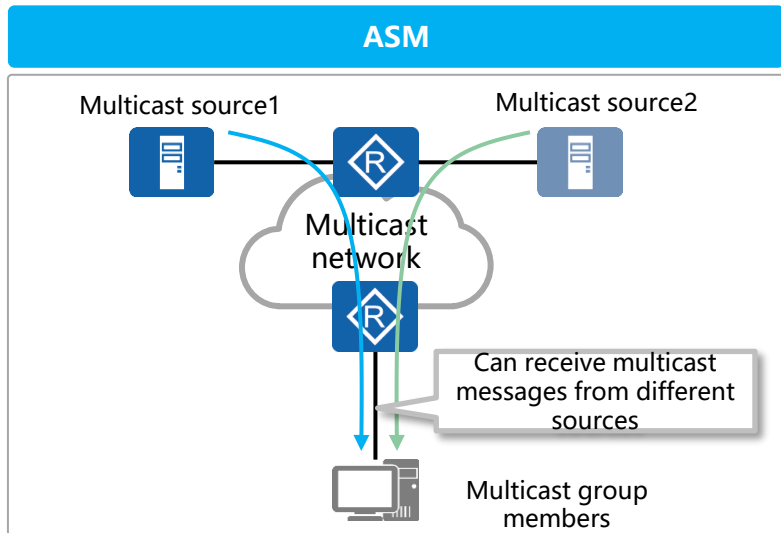
```
SW2#show ip igmp groups 224.1.1.4
IGMP Connected Group Membership(2 group(s) joined)
Group Address      Interface      Uptime    Expires    Last Reporter
224.1.1.4          vlan30        00:11:37  00:04:12   155.1.30.1
SW2#show ip mroute 224.1.1.4
Name: Ethernet0, Index: 1158, State: 1002
Name: Loopback, Index: 17500, State: 49
Name: Vlan30, Index: 11030, State: 1043
Name: pimreg, Index: 1162, State: c1
The total matched ipmr active mfc entries is 0, unresolved ipmr entries is 1
Group      origin      iif      wrong      oif:TTL
224.1.1.4  155.1.10.1  NULL     4          0:0
```


Multicast- ASM & SSM

Members of a multicast group can select the multicast data source when receiving multicast data. Therefore, two multicast service models, ASM (Any Source Multicast) and SSM (Source Specific Multicast), are generated.

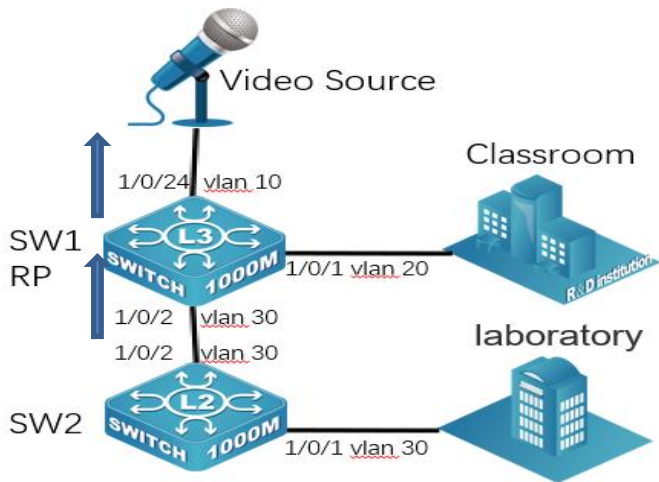
ASM: After a group member joins a multicast group, the group member can receive data sent to the group from any source.

SSM: After a group member joins a multicast group, the group member will only receive the data sent to the group from the specified source.



Multicast- SSM

Scenario 4: The school requires that on the basis of the previous scenario, the classroom can only receive 239.0.0.1 multicast messages sent by the broadcasting room



Open Media

File Disc Network Capture Device

Network Protocol

Please enter a network URL:

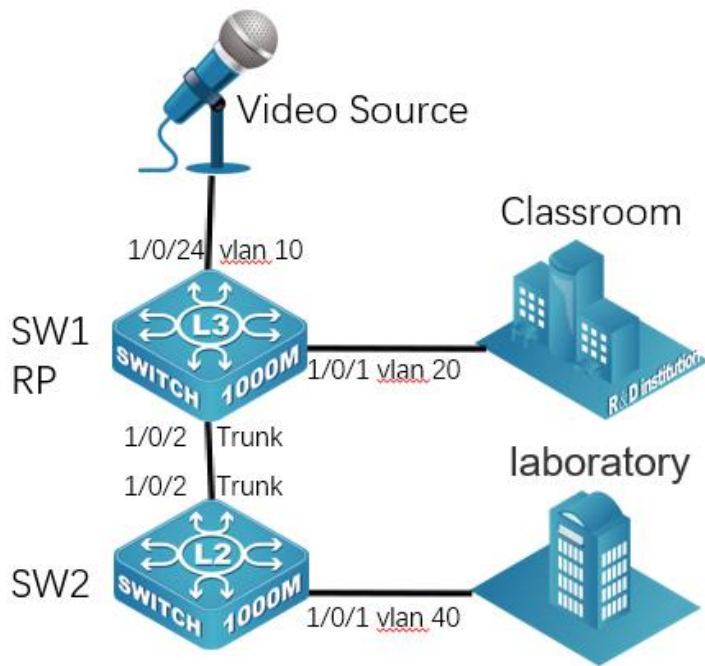
<http://www.example.com/stream.avi>
<rtp://@:1234>
<mms://mms.examples.com/stream.asx>
<rtsp://server.example.org:8080/test.sdp>
<http://www.youtube.com/watch?v=gg64x>

1897925	2022-09-02 18:04:25.175406	155.1.20.2	224.0.0.22	IGMPv3	58 Membership Report / Join group 239.0.0.1 for source {155.1.10.1}
1897926	2022-09-02 18:04:25.175413	155.1.20.2	224.0.0.22	IGMPv3	58 Membership Report / Join group 239.0.0.1 for source {155.1.10.1}


```
> Frame 1897925: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Ethernet II, Src: HuaweiTe_49:16:9a (54:89:98:49:16:9a), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 155.1.20.2, Dst: 224.0.0.22
> Internet Group Management Protocol
  [IGMP Version: 3]
  Type: Membership Report (0x22)
  Reserved: 00
  Checksum: 0x48f9 [correct]
  [Checksum Status: Good]
  Reserved: 0000
  Num Group Records: 1
  > Group Record : 239.0.0.1 Mode Is Include
    Record Type: Mode Is Include (1)
    Aux Data Len: 0
    Num Src: 1
    Multicast Address: 239.0.0.1
    Source Address: 155.1.10.1
```

Multicast-Multicast VLAN

Scenario 5: In order to ensure the information security of the laboratory, the school divides the laboratory into VLAN 40 and connects it to the layer2 switch, and requires the laboratory to receive video



SW1: every L3 interface config DM
SW2: No need to enable *ip pim multicast-routing*
SW2:

```
vlan 1;40
!  
vlan 30  
  multicast-vlan  
  multicast-vlan association 40  
!  
Interface Ethernet1/0/1  
  switchport access vlan 40  
!  
Interface Ethernet1/0/2  
  switchport mode trunk  
!  
ip igmp snooping  
ip igmp snooping vlan 30
```

Multicast- Multicast trouble shooting

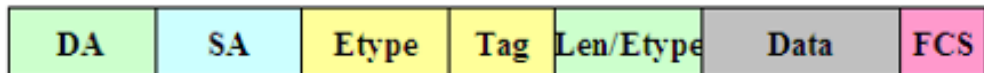
1. Although multicast messages can flood, if IP multicast source control is configured, all multicast messages will be discarded
2. some specific models such as 42 and 46 series equipment do not support PIM-DM and PIM-SM

05

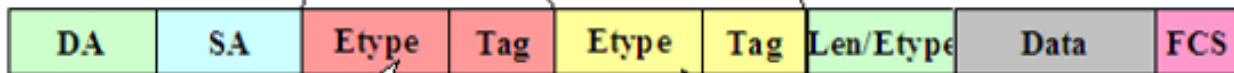
QinQ

QinQ - QinQ encapsulation

802.1Q encapsulation



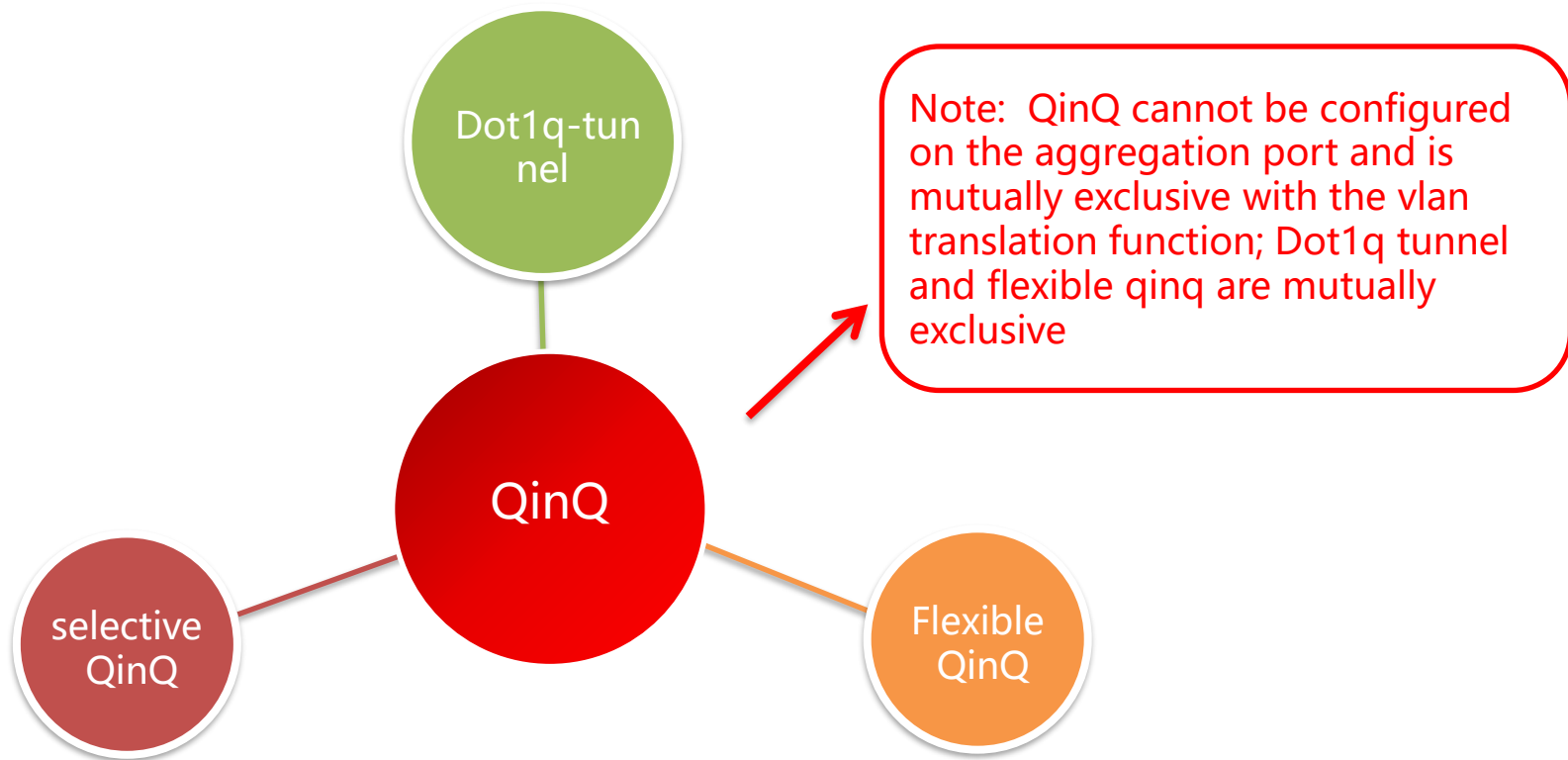
QinQ encapsulation



compared with 802.1Q frame, here added a tag. Usually we call it outer tag.

inner tag. added by users.

QinQ – QinQ function modules



QinQ – QinQ Configuration

Dot1q-tunnel

```
Interface Ethernet1/0/3
dot1q-tunnel enable
switchport access vlan 100
```

Flexible QinQ

Based on stream, match vlan, mac, port number, etc Apply matching policies to ports

```
!
class-map
match vlan 100 200
!
policy-map p1
class c1
add s-vid 1000
exit
!
```

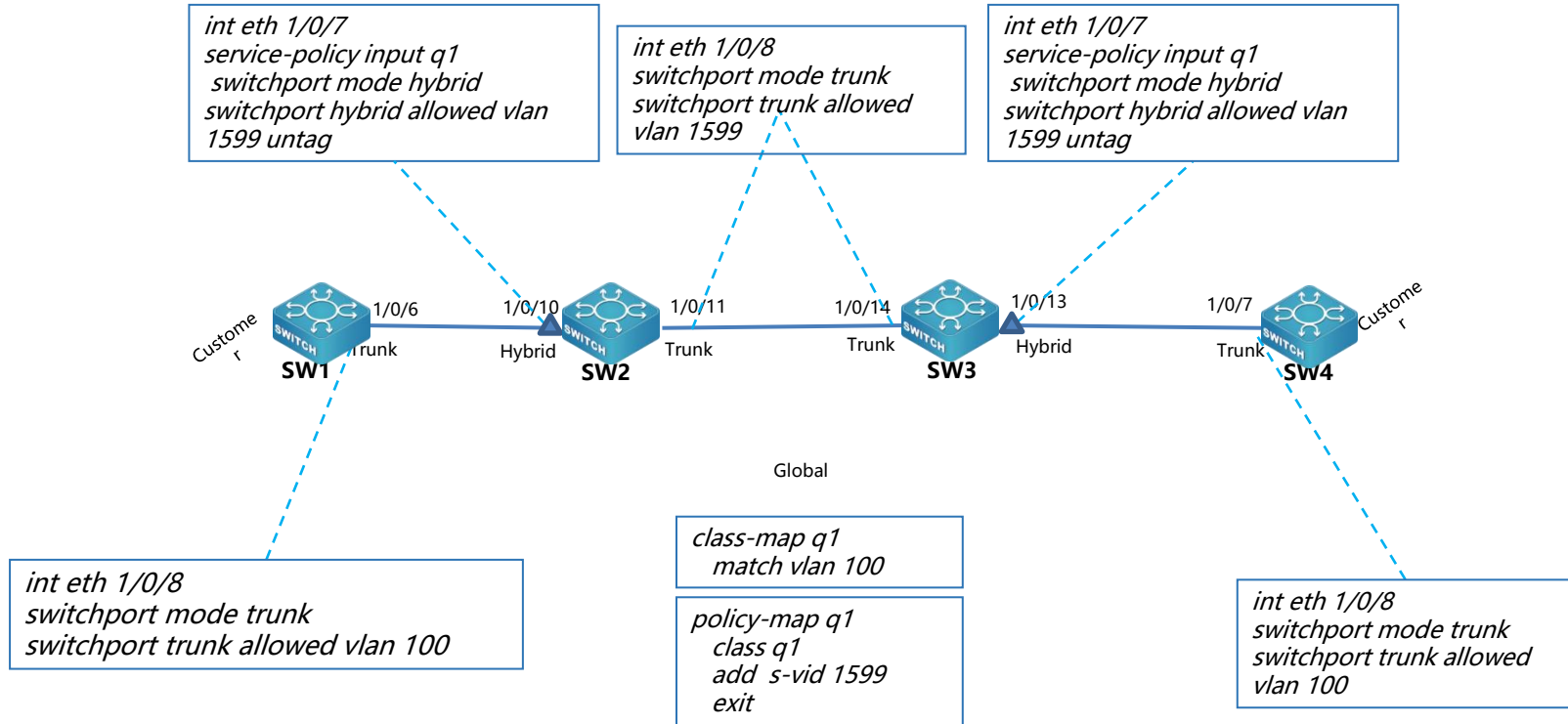
Selective QinQ

```
Interface Ethernet1/0/4
dot1q-tunnel selective s-vlan 100 c-vlan 1-20
dot1q-tunnel selective enable
switchport mode hybrid
switchport hybrid allowed vlan 100 untag
```

Flexible QinQ

```
!
Interface Ethernet1/0/3
switchport mode hybrid
switchport hybrid allowed vlan 100;200 tag
switchport hybrid allowed vlan 1000 untag
!
```

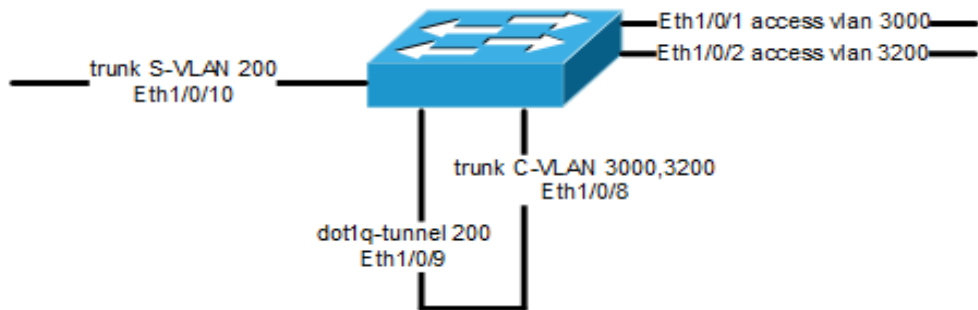

QinQ – Scenario 1:



It is required that the PCs of the vlan 100 connected to sw1 and sw4 can access each other, but sw2 and sw3 cannot create vlan 100

QinQ – Scenario 2

Scenario 2:
To add double tags
via access switch



Example from DCN switch

```
Interface Ethernet1/0/8
description "loop-port entrance"
switchport mode trunk
switchport trunk allowed vlan 3000;3200
!
Interface Ethernet1/0/9
description "loop-dot1q-tunnel"
dot1q-tunnel enable
switchport access wlan 200
!
Interface Ethernet1/0/10
description "uplink:port trunk S-VLAN"
switchport mode trunk
switchport trunk allowed vlan 200
```