S5850 Series Switches Technical White Paper

After-sale Instructions for Error-prone Issues

Models: S5850-24T16S
S5850-48S6Q
S5850-48T4Q
S5850-32S2Q
S5850-24T16B
S5850-48S2Q4C

TECHNICAL WHITE PAPER

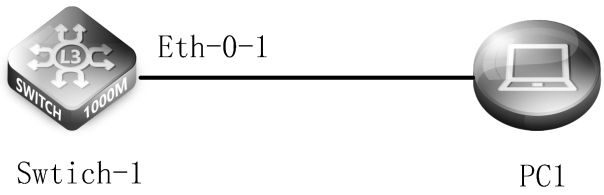
Contents

1. Precautions for Jumbo Frame Function Configuration

1.1 Issue Description

To transmit data streams between switched networks, the switch discards the data frames when MTU is out of range, when the MTU of the transmitted data stream exceeds the MTU value (1500) supported by the S58 series switch platform, which c ausing data loss.

1.2 Topology Information



1.3 Handling Process

Connect the PC and SW with RJ45 network cable according to the network topology. Connect the end of the RJ45 network cable to the PC and the other end to the eth0/0/1 interface on the front
panel of the switch. (Make sure that the network reachable between the PC and the switch port)
Log in to the switch with the PC-side command prompt or SecureCRT tool (login in with Telnet)
Enable the jumbo frame function in the advanced options of the PC network card properties, and then execute "ping -f -l 8 000 192.168.1.254" on the PC side, and you can ping it.

```
Pinging 192.168.1.254 with 8000 bytes of data:
Reply from 192.168.1.254: bytes=8000 time=2ms TTL=64
Reply from 192.168.1.254: bytes=8000 time=2ms TTL=64
Reply from 192.168.1.254: bytes=8000 time=2ms TTL=64
Reply from 192.168.1.254: bytes=8000 time=2ms TTL=64
Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Configure the switch device interface: no jumbo frame enable (the jumbo frame function is enabled by default on the interf ace)

```
Switch-1# configure terminal
Switch-1(config)# interface eth-0-1
Switch-1(config-if)#no jumboframe enable
```

From the PC, execute "ping -f -l 8000 192.168.1.254" again, and you cannot ping at this time.

```
Request timed out.
Request timed out.
Request timed out.
```

```
Request timed out.
Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

You can also configure the MTU value under the interface, first create a Layer 3 interface vlan10

```
Switch-1# configure terminal
Switch-1(config)# vlan database
Switch-1(config-vlan)#vlan 10
Switch-1(config-vlan)# exit
```

Configure the MTU value of interface vlan10 <68-9216>, 1500 by default

```
Switch-1(config)# interface vlan10
Switch-1(config-if)#mtu 1600
```

1.4 Root Cause

After the jumbo frame function is disabled, the maximum allowed packet length on the interface is 1632 bytes.

1.5 Solution

After the jumbo frame function is enabled, the maximum allowed packet length on the interface is 9600 bytes.

1.6 Suggestions and Conclusions

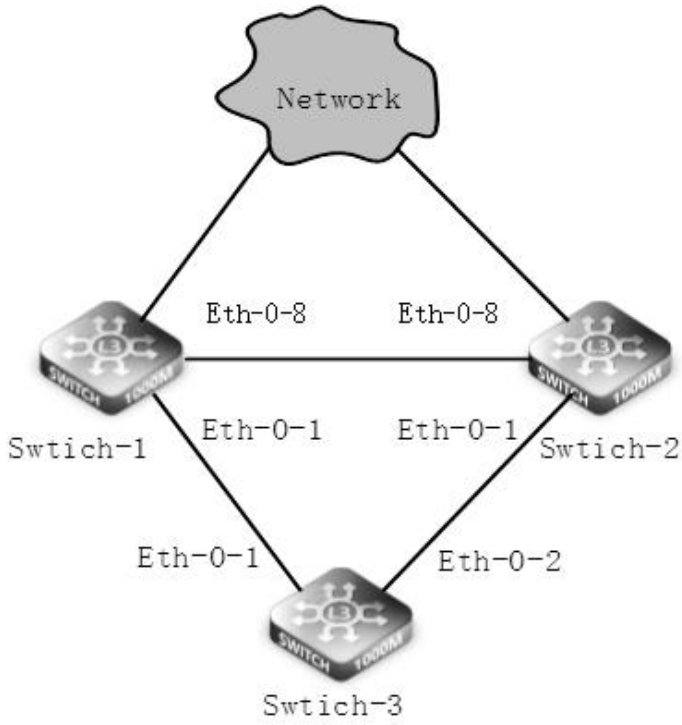
In a scenario where the network bandwidth is sufficient, increasing the frame length can reduce the number of network dat a packets and reduce the additional overhead of the network device in processing the packet header. The reduced frame nu mber will inevitably improve the performance of the device.

1. Precautions for MLAG Function Configuration

2.1 Issue Description

When the S58 series switches use the spanning tree protocol, the MLAG function is configured, which causes the MLAG func tion to be abnormal.

2.2 Topology Information



2.3 Handling Process

4. Enter Vlan configuration mode, create vlan, and create static AGG in global configuration mode

Configure Switch-1(the same as Switch-2)

```
Switch-1# configure terminal
Switch-1(config)# vlan database
Switch-1(config-vlan)# vlan 10,4094
Switch-1(config-vlan)# exit
Switch-1(config)# interface eth-0-1
Switch-1(config-if)# static-channel-group 1
Switch-1(config-if)# no shutdown
Switch-1(config-if)# exit
```

Configure Switch-3

```
Switch-3# configure terminal
Switch-3(config)# vlan database
Switch-3(config-vlan)# vlan 10
Switch-3(config-vlan)# exit
Switch-3(config)# interface eth-0-1
Switch-3(config-if)# static-channel-group 1
```

```
Switch-3(config-if)# no shutdown
Switch-3(config-if)# exit
Switch-3(config)# interface eth-0-2
Switch-3(config-if)# static-channel-group 1
Switch-3(config-if)# no shutdown
```

5. Prepare to configure the attribute of peer link interface, add AGG to MLAG

Configure Switch-1(the same as Switch-2)

```
Switch-1(config)# interface eth-0-8
Switch-1(config-if)# switchport mode trunk
Switch-1(config-if)# switchport trunk allowed vlan all
Switch-1(config-if)# spanning-tree port disable
Switch-1(config-if)# no shutdown
Switch-1(config-if)# exit
Switch-1(config)# interface agg 1
Switch-1(config-if)# switchport mode trunk
Switch-1(config-if)# switchport trunk allowed vlan add 10
Switch-1(config-if)# mlag 1
Switch-1(config-if)# exit
```

Configure Switch-3

```
Switch-3# configure terminal
Switch-3(config)# interface agg1
Switch-3(config-if)# switchport mode trunk
Switch-3(config-if)# switchport trunk allowed vlan add 10
```

6. Configure the properties of the Vlan interface

Configure Switch-1

```
Switch-1(config)#interface vlan4094
Switch-1(config-if)# ip address 12.1.1.1/24
Switch-1(config-if)# exit
```

Configure Switch-2

```
Switch-2(config-if)#interface vlan 4094
Switch-2(config-if)# ip address 12.1.1.2/24
Switch-2(config-if)# exit
```

4. Enter MLAG mode and configure related attributes

Configure Switch-1

```
Switch-1(config)# mlag configuration
Switch-1(config-mlag)# peer-link eth-0-8
Switch-1(config-mlag)# peer-address 12.1.1.2
Switch(config-mlag)# exit
```

Configure Switch-2

```
Switch-2(config)# mlag configuration
Switch-2(config-mlag)# peer-link eth-0-8
Switch-2(config-mlag)# peer-address 12.1.1.1
Switch-2(config-mlag)# end
```

7. Verify the configuration result and check the MLAG status information on Switch-1 (Switch-2 view commands are consisten

t)

Check the status of MLAG devices, the two devices are in Master/Slave state

```
Switch-1# show mlag
MLAG configuration:
------------------
role               : Slave
local_sysid   : 001e.080f.2400
remote_sysid : 001e.0810.4093
mlag_sysid     : 001e.0810.4093
local_syspri : 32768
remote_syspri: 32768
mlag_syspri   : 32768
peer-link      : eth-0-8
peer conf      : Yes
reload-delay : 300s
```

Switch-1# View MLAG group status, all interfaces are up

```
Switch-1# show mlag interface
mlagid   local-if   local-state      remote-state
1            agg1          up                    -
```

View MLAG neighbor information

```
Switch-1# show mlag peer
MLAG neighbor is 12.1.1.2, MLAG version 1
MLAG state = Established, up for 00:03:04
Last read 00:00:18, hold time is 240, keepalive interval is 60 seconds
Received 10 messages,Sent 14 messages
Open         : received 1, sent 5
KAlive     : received 4, sent 4
Fdb sync : received 0, sent 0
Failover : received 0, sent 0
Conf         : received 0, sent 1
Syspri     : received 1, sent 1
Peer fdb : received 1, sent 1
STP Total: received 3, sent 2
 Global   : received 3, sent 2
 Packet   : received 0, sent 0
 Instance: received 0, sent 0
 State     : received 0, sent 0
Connections established 1; dropped 0
Local host: 12.1.1.1, Local port: 61000
Foreign host: 12.1.1.2, Foreign port: 36644
remote_sysid: 001e.0810.4093
```

8. On the peer-link interfaces of Swtich-1 and Swtich-2 devices, port spanning tree enable failed.

Configure Switch-1(the same as Switch-2)

```
Switch-1(config)# interface eth-0-8
Switch-1(config-if)# spanning-tree port enable
Can't config on this interface, MLAG Peer link has been configured on it
```

2.4 Root Cause

Due to the characteristics of S5800 series switches, Spanning Tree Protocol and MLAG cannot be used at the same time.

2.5 Solution

When configuring the MLAG function, please disable the spanning tree protocol of the corresponding port.

2.6 Suggestions and Conclusions

Compared with stacking, the devices that make up MLAG still need to be managed separately, and do not need to be restarted after the configuration is completed, and the forwarding decisions are all local. Normally, traffic does not need to take the interconnection path between devices, avoiding the interconnection path Bandwidth becomes a bottleneck while reducing latency.

Note:

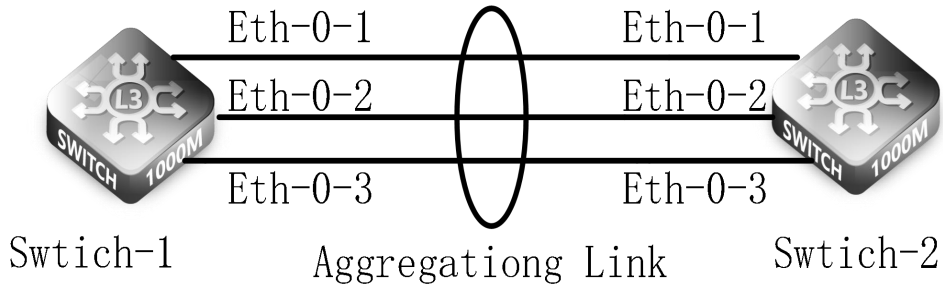
1. The two switches that make up MLAG need to be our switches, and cannot be mixed with other manufacturers' switches to form MLAG Peer-address. Only the directly connected addresses are temporarily supported.
2. Currently, MLAG does not support multicast processing, and multicast traffic is forwarded according to the broadcast.

3. Precautions for Link Aggregation Function Configuration

3.1 Issue Description

When creating the number of failed aggregation groups and adding the number of members of the aggregation group, the link aggregation function configuration becomes invalid.

3.2 Topology Information



3.3 Handling Process

1. Enter configuration mode, configure LACP global attributes, set system priority and implement load sharing based on source MAC address

Configure Switch-1

```
Switch-1# configure terminal
Switch-1(config)# lacp system-priority 2000
Switch-1(config)# port-channel load-balance hash-field-select macsa
```

Configure Switch-2

```
Switch-2# configure terminal
Switch-2(config)# lacp system-priority 1000
Switch-2(config)# port-channel load-balance hash-field-select macsa
```

2. Enter the port configuration mode and add the port to Channel Group 1

Switch-1 configuration (Switch-2 configuration is the same, omitted here)

```
Switch-1# configure terminal
Switch-1(config)# interface eth-0-1
Switch-1(config-if)# no shutdown
Switch-1(config-if)# channel-group 1 mode active
Switch-1(config-if)# exit
Switch-1(config)# interface eth-0-2
Switch-1(config-if)# channel-group 1 mode active
Switch-1(config-if)# no shutdown
Switch-1(config-if)# exit
Switch-1(config)# interface eth-0-3
```

```
Switch-1(config-if)# channel-group 1 mode active
Switch-1(config-if)# no shutdown
Switch-1(config-if)# exit
Switch-1(config)# end
```

3. Check the configuration

```
Switch-1# show channel-group summary
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
        ipsa ipda srcport dstport ip-protocol
port-channel group-mode: 56
Flags:  s - Suspend              T - Standby
        D - Down/Admin down      B - In bundle
        R - Layer3               S - Layer2
        w - Wait                 U - In use
Mode:   SLB  - Static load balance
        DLB  - Dynamic load balance
        RR   - Round robin load balance
        RLB  - Resilient load balance
Aggregator Name   Mode       Protocol      Ports
----------------+---------+--------------+-------------------------------------
agg1(SU)          SLB        LACP            eth-0-1(B)      eth-0-2(B)      eth-0-3(B)
```

4. View AGG port information

```
Switch-1# show interface agg1
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is 001e.080c.ea43 (bia 001e.080c.ea43)
  Bandwidth 30000000 kbits
  Index 2049 , Metric 1 , Encapsulation ARPA
  Speed - 10Gb/s , Duplex - Full  , Media type is Aggregation
  Link type is autonegotiation
  FEC config: DISABLE
  FEC status: DISABLE
  The Maximum Frame Size is 9600 bytes
  VRF binding: not bound
  ARP timeout 01:00:00,  ARP retry interval 1s
  ARP Proxy is disabled, Local ARP Proxy is disabled
    5 minute input rate 67 bits/sec, 0 packets/sec
    5 minute output rate 126 bits/sec, 0 packets/sec
    22 packets input, 3256 bytes
    Received 0 unicast, 0 broadcast, 22 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
```

```
    29 packets output, 5874 bytes
    Transmitted 0 unicast, 7 broadcast, 22 multicast
    0 underruns, 0 output errors, 0 pause output
```

5. Add eth-0-1...-17 member ports in the link aggregation group in sequence, and the 17th member port cannot join the aggregation group.

```
Switch-1(config)# interface eth-0-17
Switch-1(config-if)# channel-group 1 mode active
% Agg 1 has not enough port number
```

6. Create 1, 2, 3....n aggregation groups in sequence. When creating the 64th aggregation group, the command line prompts that the creation failed.

```
Switch-1(config)# interface agg ?
<0-63>  Port number
```

3.4 Root Cause

Due to the limitation of switch performance specifications, at present, we can add up to 16 member ports under the aggregation group of our switch, and can create up to 63 aggregation groups.

3.5 Solution

When creating the number of aggregation groups and adding member ports of the aggregation group, be careful not to exceed the performance specifications, otherwise the configuration will fail.

3.6 Suggestions and Conclusions

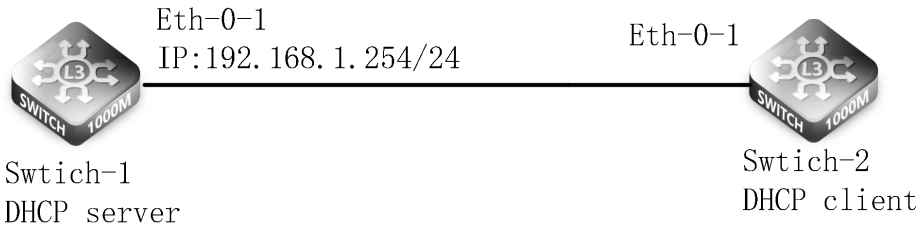
If the link aggregation is abnormal, please check whether the physical line is normal and whether the link aggregation configuration is correct. In summary, when configuring the Link Aggregation function, please refer to the relevant configuration manual.

4. Precautions for DHCP Function Configuration

4.1 Issue Description

As a DHCP client, S58 series switches cannot quickly obtain the dynamic IP address assigned by the DHCP server.

4.2 Topology Information



4.3 Handling Process

1. Configure the DHCP server and address pool on the S58 switch.

Configure Switch-1

```
Switch-1# configure terminal
Switch-1(config)# service dhcp enable
Switch-1(config)# dhcp server
Switch-1(config)# dhcp pool pool1
Switch-1(dhcp-config)# network 192.168.1.0/24
Switch-1(dhcp-config)# gateway 192.168.1.254
Switch-1(dhcp-config)# exit
```

2. Enter the interface configuration mode and configure the interface attributes and IP address.

Configure Switch-1

```
Switch-1(config)# interface eth-0-1
Switch-1(config-if)# no switchport
Switch-1(config-if)# no shutdown
Switch-1(config-if)# ip address 192.168.1.254/24
Switch-1(config-if)# dhcp server enable
Switch-1(config-if)# exit
```

3. Configure the DHCP client and enable DHCP dynamic address acquisition under the interface.

Configure Switch-2

```
Switch-2# configure terminal
Switch-2(config)# interface eth-0-1
Switch-2(config-if)# no switchport
Switch-2(config-if)# no shutdown
Switch-2(config-if)# ip address dhcp
Switch-2(config-if)# exit
```

4. Check the configuration on the DHCP server.

```
Switch-1# show running-config
!
service dhcp enable
!
interface eth-0-1
no switchport
dhcp server enable
ip address 192.168.1.254/24!
!
dhcp server
dhcp pool pool1
network 192.168.1.0/24
gateway 192.168.1.254
```

5. View the address allocation and interface information on the DHCP server.

```
Switch-1# show dhcp server binding all
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.1.1 6e:6e:36:1f:84:00 Sat 2020.02.04 08:00:12 Dynamic
```

```
Switch-1# show dhcp server interfaces
List of DHCP server enabled interface(s):
DHCP server service status: enabled
Interface Name
============================================================
eth-0-1
```

6. Configure the interface on the DHCP client as an edge port, and then enable DHCP dynamic address pool acquisition under the client interface. (After setting as the edge port, the efficiency of the client to obtain the DHCP address is significantly improved)

```
Switch-2(config)# interface eth-0-1
Switch-2(config-if)# spanning-tree edgeport
Switch-2(config-if)# no ip address dhcp
Switch-2(config-if)# ip address dhcp
```

7. Turn off the STP spanning tree on the DHCP client, and then enable DHCP dynamic address pool acquisition under the client interface. (After turning off the STP spanning tree function, the efficiency of the client to obtain the DHCP address is significantly improved)

```
Switch-2(config)# interface eth-0-1
Switch-2(config-if)# spanning-tree port disable
Switch-2(config-if)# no ip address dhcp
Switch-2(config-if)# ip address dhcp
```

8. The problem of network cable and address pool allocation is eliminated. Finally, it is found that turning on STP of the device will also cause DHCP to slowly obtain an IP address. You can turn off STP or set the interface connecting to the PC as an STP edge port.

Note:

The device and the PC need to wait for the completion of the DHCP message exchange before the PC can obtain the IP address.

4.4 Root Cause

After checking step by step under the same environment built in our lab, the final reason can be identified that the client switch opens STP which leads to slow IP address acquisition.

4.5 Solution

Turn off the DHCP client switch STP or set the interface connected to the PC as an STP edge port.

4.6 Suggestions and Conclusions

It is a common problem that DHCP cannot obtain an IP address. The trouble exclusion should start with the basic configuration. Under the condition that the physical line is working, the specific conditions of the address lease or address pool allocation are not checked, nor does the client's own problem be ruled out.

Description:

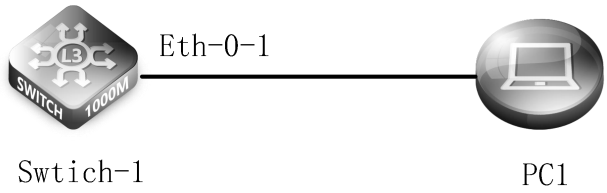
1. Occasionally, some terminal manufacturers have different understanding of the RFC, and the Option field of some packets is defined differently, resulting in a verification errors. The packet sent by the switch is not processed, and the IP address cannot be obtained. This is a compatibility issue and requires customers to coordinate with both equipment manufacturers to solve it.
2. When deploying services, an unreasonable port broadcast suppression value is set. The client discovers an available DHCP server by broadcasting a DHCP DISCOVER message, which will affect the user's automatic acquisition of an IP address.

5. Precautions for WEB Login in Configuration

5.1 Issue Description

When web image files are not packed in S58 series switches, web administration can't be remotely operated.

5.2 Topology Information



5.3 Handling Process

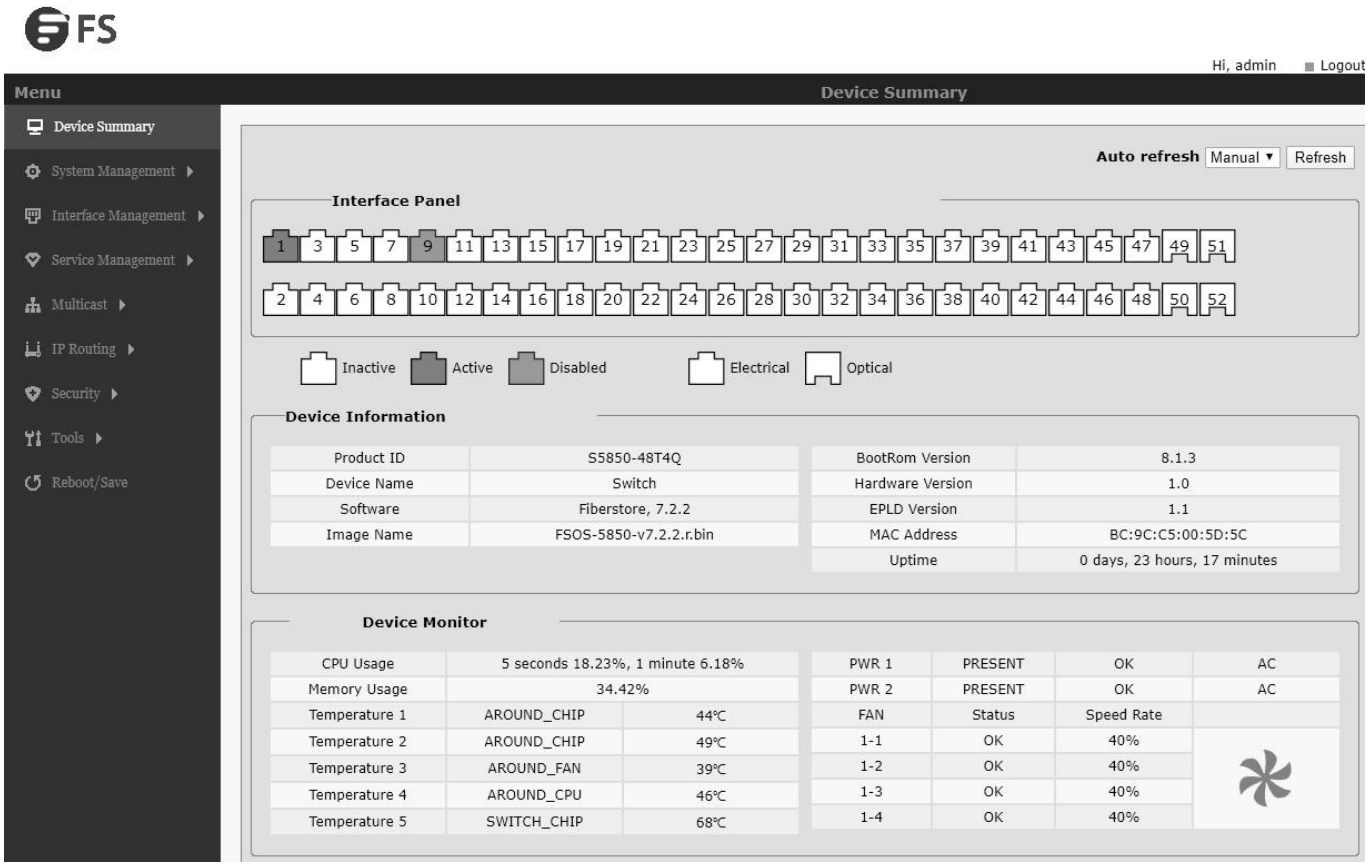
1. After logging in to the device, check that the if the web image files (FSOS-webimage-v6.2.28.r.bin) are uploaded in the flash local folder. By default, the web image files are uploaded at the factory.

```
Switch-1# dir
Directory of flash:/
total 31680
-rw------- 1   1440308 Jul 22   2000 48T4Q-1.bin
-rw-r--r-- 1   1440308 Jul 22   2000 48T4Q-2.bin
-rwxr-xr-x 1    295938 May 23   2017 AQR-G2_v3.2.5_ID19866_VER537.cld
-rw-r--r-- 1      1345 Jan 31   2001 BC9CC5005D5C.3.lic
-rw------- 1   1440308 Aug 15   2000 FSOS-S5850-48T4Q-V6.2.28.r.bin
-rw------- 1   1440308 Sep 21   2000 FSOS-webimage-v6.2.28.r.bin
-rw-r--r-- 1       339 Jan 25   2001 Identity.pub
drwxr-xr-x 2       624 Jul 13   2001 boot
-rw-r--r-- 1 26142408 Jan 31   2001 centecOS-e580-v7.2.0.10.r.bin
```

2. Upload the webImage file to the flash local folder through the TFTP protocol, enable the HTTP service, and finally restart the device.

```
Switch-1# copy mgmt-if tftp:// flash:
TFTP server [] 10.32.133.1
Name of the TFTP file to access [] fs.r.bin
service http enable & service https enable
Switch-1(config)# http server load flash:/fs.bin
Switch-1(config)# service http enable
Switch-1(config)# service https enable
Switch-1(config)#exit
Switch-1#write
Switch-1#reboot
```

3. Open a browser, enter the remote management IP, add a user name and password to log in to the web page, and perform configuration management.



5.4 Root Cause

The web management page is designed by a independent software development, so you need to upload the webimage file first so that you can log in to the web page for management operations.

5.5 Solution

When uploading and upgrading webimage files, S58 series switches can choose TFTP protocol for file transfer.

5.6 Suggestions and Conclusions

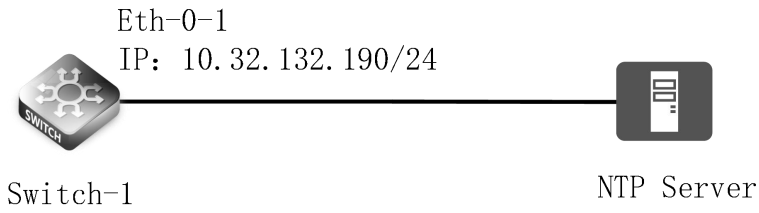
When uploading and updating webimage files on S58 series switches, please follow the standard steps to avoid web page lo gin failure.

6. Precautions for NTP Function Configuration

6.1 Issue Description

As a client, S58 series switches fail to synchronize time with the NTP server, and there is a time difference between the device time and the NTP time.

6.2 Topology Information



6.3 Handling Process

1. Build the environment according to the topology diagram, and configure the NTP server on the switch.

```
Switch-1(config)#ntp server 10.32.132.191
Switch-1(config)# ntp ace 10.32.132.191 none
Switch-1(config)# interface eth-0-1
Switch-1(config-if)# no switchport
Switch-1(config-if)# no shutdown
Switch-1(config-if)# ip address 10.32.132.190/24
```

2. Check the switch configuration.

```
Switch-1# show ntp
Current NTP configuration:
============================================================
NTP access control list:
  10.32.132.191 mask 255.255.255.255 none
Unicast peer:
Unicast server:
  10.32.132.191
Local reference clock:
Disable management interface
```

3. Check the NTP status and display synchronization.

```
Switch-1# show ntp status
Current NTP status:
============================================================
clock is synchronized
stratum              :7
reference clock :10.32.132.191
frequency            :0.833 ppm
precision            :2^20
reference time   :e23677f1.9204d106  ( 3:54:25.570 UTC Tue Apr  7 2020)
root delay           :1.122 ms
```

```
root dispersion :18.035 ms
peer dispersion :43.970 ms
clock offset :1.345 ms
stability :0.184 ppm
synchronization state: clock synchronized
```

4. Check the current time, the display time zone is Kabul.

```
Switch-1# show clock detail
13:31:10 dst Sat Oct 26 2019
Time zone: (GMT + 04:30:00) Kabul
```

5. Delete the Kabul time zone.

```
Switch-1# configure terminal
Switch-1(config)# no clock set timezone
```

6. Check the time again, the clock returns to UTC time, and the time is normal.

```
Switch-1# show clock
11:00:22 UTC Tue Apr 07 2020
```

Description:

The device time is composed of three parts: NTP UTC time, time zone and daylight saving time. The update process of these three parts is completely independent, but the final time is the sum of these three times.

1>The UTC time of NTP is obtained from the NTP server, and the time zone and daylight saving time of the NTP server will not be transmitted through NTP.

2> The time zone is the fixed configuration of this machine.

3> Daylight saving time is determined according to the configuration of the machine and the current date.

6.4 Root Cause

Since the current system time zone of the device is the Kabul time zone, failure to synchronize with the UTC time zone leads to a fault. The fault is resolved after deleting the local Kabul time zone of the system.

6.5 Solution

Use the command "no clock set timezone" in configuration mode to delete the local time zone of the system.

6.6 Suggestions and Conclusions

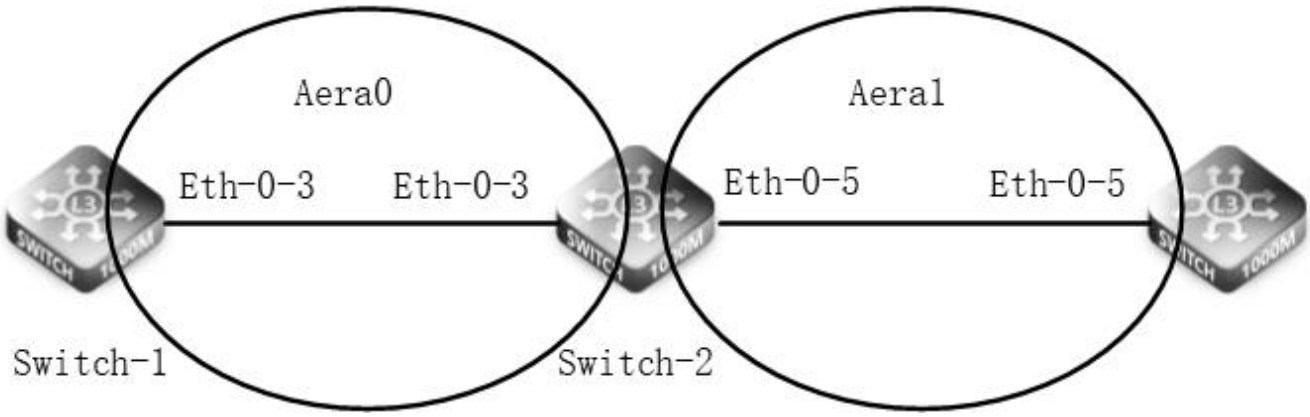
When the client's time is incorrect, first determine which part of NTP, time zone, or daylight saving time is the problem. If the time zone and daylight saving time are configured correctly, you need to check the configuration on the NTP server.

7. Precautions for OSFP Routing Protocol Configuration

7.1 Issue Description

When configuring OSPF protocol on S58 series switches, directly connecting two devices with different area numbers will cau se abnormal OSPF neighbor relationship.

7.2 Topology Information



7.3 Handling Process

1. Configure the interface attributes and ip address in interface mode (the default attribute of the port is the layer 2 forwar ding port, and you need to switch to the layer 3 forwarding interface before configuring the ip address)

Configure Switch-1

```
Switch-1# configure terminal
Switch-1(config)# interface eth-0-3
Switch-1(config-if)# no switchport
Switch-1(config-if)# no shutdown
Switch-1(config-if)# ip address 10.1.12.1/24
Switch-1(config-if)# exit
```

Configure Switch-2

```
Switch-2# configure terminal
Switch-2(config)# interface eth-0-3
Switch-2(config-if)# no switchport
Switch-2(config-if)# no shutdown
Switch-2(config-if)# ip address 10.1.12.2/24
Switch-2(config-if)# exit
Switch-2(config)# interface eth-0-5
Switch-2(config-if)# no switchport
Switch-2(config-if)# no shutdown
Switch-2(config-if)# ip address 10.1.23.2/24
Switch-2(config-if)# exit
```

Configure Switch-3

```
Switch-3# configure terminal
Switch-3(config)# interface eth-0-5
Switch-3(config-if)# no switchport
```

```
Switch-3(config-if)# no shutdown
Switch-3(config-if)# ip address 10.1.23.3/24
Switch-3(config-if)# exit
```

1.Create an OSPF instance and publish the required network segment to the corresponding area (OSPF configuration for two directly connected devices, the instance can be different, but the area number must be the same)

Configure Switch-1

```
Switch-1(config)# router ospf 1
Switch-1(config-router)# network 10.1.12.1/24 area 0
```

Configure Switch-2

```
Switch-2(config)# router ospf 1
Switch-2(config-router)# network 10.1.12.2 area 0
Switch-2(config-router)# network 10.1.23.2 area 1
```

Configure Switch-3

```
Switch-3(config)# router ospf 2
Switch-3(config-router)# network 10.1.23.3/24 area 1
```

2.View OSPF related information

View the OSPF database (view on Switch-2)

```
Switch-2# show ip ospf database
            OSPF Router with ID (10.1.23.2) (Process ID 1)
                Router Link States (Area 0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.1.12.1       10.1.12.1       34  0x80000005 0xd519 1
10.1.23.2       10.1.23.2       31  0x80000004 0x12c3 1
                Net Link States (Area 0)
Link ID         ADV Router      Age  Seq#       CkSum
10.1.12.1       10.1.12.1       33  0x80000001 0x2fbe
                Summary Link States (Area 0)
Link ID         ADV Router      Age  Seq#       CkSum  Route
10.1.23.0       10.1.23.2       40  0x80000001 0xd83d 10.1.23.0/24
                Router Link States (Area 1)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.1.23.2       10.1.23.2       24  0x80000004 0x19a4 1
10.1.23.3       10.1.23.3       29  0x80000003 0x16a6 1
                Net Link States (Area 1)
Link ID         ADV Router      Age  Seq#       CkSum
10.1.23.3       10.1.23.3       30  0x80000001 0xbf07
                Summary Link States (Area 1)
Link ID         ADV Router      Age  Seq#       CkSum  Route
10.1.12.0       10.1.23.2       40  0x80000001 0x52ce 10.1.12.0/24
```

View OSPF port status

```
Switch-2# show ip ospf interface
eth-0-3 is up, line protocol is up
  Internet Address 10.1.12.2/24, Area 0, MTU 1500
  Process ID 1, Router ID 10.1.23.2, Network Type BROADCAST, Cost: 1
```

```
  Transmit Delay is 1 sec, State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.1.12.1, Interface Address 10.1.12.1
  Backup Designated Router (ID) 10.1.23.2, Interface Address 10.1.12.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 1581957819
  Hello received 13 sent 14, DD received 4 sent 5
  LS-Req received 1 sent 1, LS-Upd received 3 sent 3
  LS-Ack received 2 sent 2, Discarded 0
eth-0-5 is up, line protocol is up
  Internet Address 10.1.23.2/24, Area 1, MTU 1500
  Process ID 1, Router ID 10.1.23.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.1.23.3, Interface Address 10.1.23.3
  Backup Designated Router (ID) 10.1.23.2, Interface Address 10.1.23.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 1581957830
  Hello received 12 sent 13, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 2
  LS-Ack received 2 sent 2, Discarded 0
```

View OSPF neighbor information

```
Switch-2# show ip ospf neighbor
OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.12.1         1   Full/DR         00:00:35    10.1.12.1       eth-0-3
10.1.23.3         1   Full/DR         00:00:35    10.1.23.3       eth-0-5
```

View OSPF routing information

```
Switch-2# show ip ospf route
OSPF process 1:
Codes: C - connected, D - Discard, 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

C   10.1.12.0/24 [1] is directly connected, eth-0-3, Area 0
C   10.1.23.0/24 [1] is directly connected, eth-0-5, Area 1
```

When the directly connected device is configured with OSPF, different area numbers are used. At this time, the OSPF neighbor relationship is abnormal.

Change the configuration on Switch-2:

```
Switch-2(config)# router ospf 2
Switch-2(config-router)# no network 10.1.23.3/24 area 1
Switch-2(config-router)# network 10.1.23.3/24 area 2
```

Check the OSPF neighbor relationship. The neighbor relationship between Switch-2 and Switch-3 is broken.

```
Switch-2# show ip ospf neighbor
OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.12.1         1   Full/DR         00:00:39    10.1.12.1       eth-0-3
```

7.4 Root Cause

Directly connected devices in different areas cannot send lsa information to each other, resulting in a neighbor relationship not being established properly.

7.5 Solution

When establishing OSPF neighbor relationships between directly connected devices, the area IDs must be consistent.

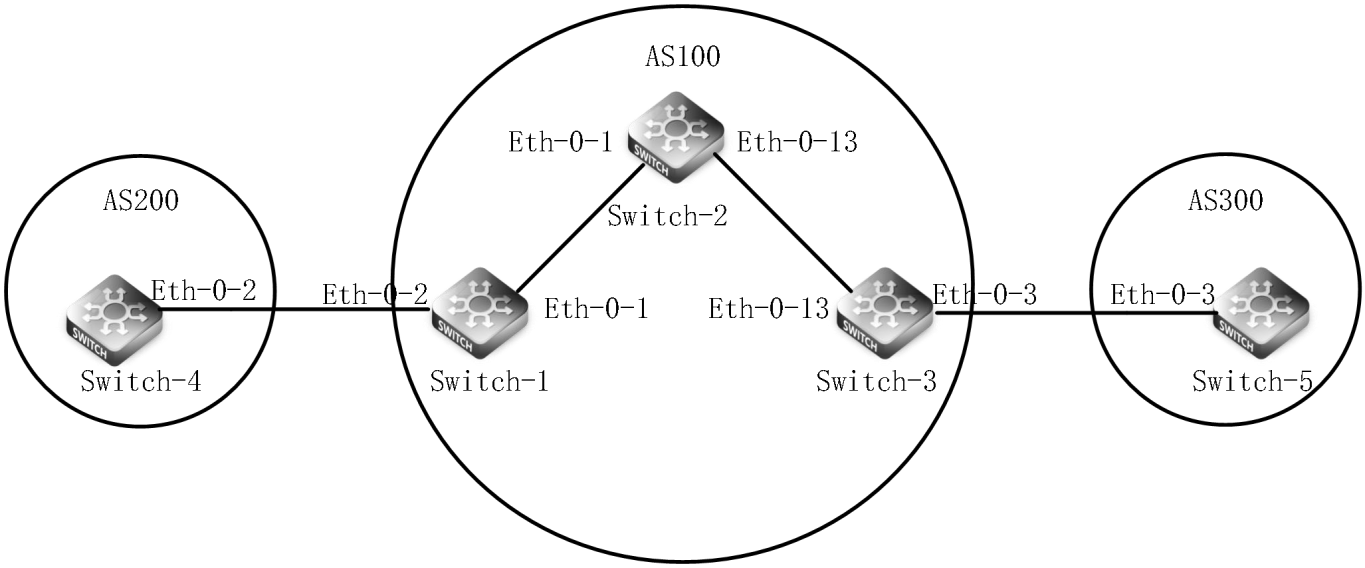
7.6 Suggestions and Conclusions

When the OSPF neighbor relationship is abnormally established, first check whether the physical link is reachable, secondly, whether the configuration is normal, whether the area ID is consistent, whether the published network is correct, and whether the Router-ID conflicts, etc. Configuration manual for related configuration.

8. Precautions for BGP Routing Protocol Configuration

8.1 Issue Description

In the scenario where BGP routes are configured, BGP routes are lost, causing the BGP routing table to be out of synchroniz ation and affecting the normal communication of services.



8.2 Handing Process

1. Create a LoopBack0 interface on Switch-1, establish an IBGP neighbor relationship in the AS100 domain, and establish an EBGP neighbor relationship outside the AS100 domain.

Configuration Switch-1

```
Switch-1(config)# interface eth-0-1
Switch-1(config-if)# no shutdown
Switch-1(config-if)# no switchport
Switch-1(config-if)# ip address 10.1.12.1/24
Switch-1(config-if)# exit
Switch-1(config)# interface eth-0-2
Switch-1(config-if)# no shutdown
Switch-1(config-if)# no switchport
Switch-1(config-if)# ip address 10.1.14.1/24
Switch-1(config-if)# exit
Switch-1(config)#interface loopback 0
Switch-1(config-if)# ip address 1.1.1.1/32
Switch-1(config-if)# exit
Switch-1(config)# router ospf 1
Switch-1(config-router)# network 10.1.12.1/24 area 0
Switch-1(config)# router bgp 100
Switch-1(config-router)# neighbor 2.2.2.2 remote-as 100
Switch-1(config-router)# neighbor 2.2.2.2 update-source loopback0
Switch-1(config-router)# neighbor 10.1.14.4 remote-as 200
```

```
Switch-1(config-router)# neighbor 10.1.14.4 update-source 10.1.14.1
Switch-1(config-if)# exit
```

Create a LoopBack0 interface on Switch-2, and establish an IBGP neighbor relationship with Switch-1 and Switch-3 through the loopback port.

Configuration Switch-2

```
Switch-2(config)# interface eth-0-1
Switch-2(config-if)# no shutdown
Switch-2(config-if)# no switchport
Switch-2(config-if)# ip address 10.1.12.2/24
Switch-2(config-if)# exit
Switch-2(config)# interface eth-0-13
Switch-2(config-if)# no shutdown
Switch-2(config-if)# no switchport
Switch-2(config-if)# ip address 10.1.23.2/24
Switch-2(config-if)# exit
Switch-2(config)#interface loopback 0
Switch-2(config-if)# ip address 2.2.2.2/32
Switch-2(config-if)# exit
Switch-2(config)# router ospf 1
Switch-2(config-router)# network 10.1.12.2/24 area 0
Switch-2(config-router)# network 10.1.23.2/24 area 0
Switch-2(config)# router bgp 100
Switch-2(config-router)# neighbor 1.1.1.1 remote-as 100
Switch-2(config-router)# neighbor 1.1.1.1. update-source loopback0
Switch-2(config-router)# neighbor 3.3.3.3 remote-as 100
Switch-2(config-router)# neighbor 3.3.3.3 update-source loopback0
Switch-2(config-if)# exit
```

3. Create a LoopBack0 interface on the Switch-3 switch, establish an IBGP neighbor relationship with the Switch-2 through the loopback port, and establish an EBGP neighbor relationship with the Switch-5 through the local interface.

Configuration Switch-3

```
Switch-3(config)# interface eth-0-13
Switch-3(config-if)# no shutdown
Switch-3(config-if)# no switchport
Switch-3(config-if)# ip address 10.1.23.3/24
Switch-3(config-if)# exit
Switch-3(config)# interface eth-0-3
Switch-3(config-if)# no shutdown
Switch-3(config-if)# no switchport
Switch-3(config-if)# ip address 10.1.35.3/24
Switch-3(config-if)# exit
Switch-3(config)#interface loopback 0
Switch-3(config-if)# ip address 3.3.3.3/32
Switch-3(config-if)# exit
Switch-3(config)# router ospf 1
```

```
Switch-3(config-router)# network 10.1.23.3/24 area 0
Switch-3(config)# router bgp 100
Switch-3(config-router)# neighbor 2.2.2.2 remote-as 100
Switch-3(config-router)# neighbor 2.2.2.2 update-source loopback0
Switch-3(config-router)# neighbor 10.1.35.5 remote-as 300
Switch-3(config-router)# neighbor 10.1.35.5 update-source 10.1.35.3
Switch-3(config-if)# exit
```

Create a LoopBack0 interface on Switch-4, establish an EBGP neighbor relationship with Switch-1 on the local interface, and publish the loopback port address under the BGP process

Configuration Switch-4

```
Switch-4(config)# interface eth-0-2
Switch-4(config-if)# no shutdown
Switch-4(config-if)# no switchport
Switch-4(config-if)# ip address 10.1.14.4/24
Switch-4(config)#interface loopback 0
Switch-4(config-if)# ip address 4.4.4.4/32
Switch-4(config-if)#exit
Switch-4(config)# router bgp 200
Switch-4(config-router)# neighbor 10.1.14.1 remote-as 100
Switch-4(config-router)# neighbor 10.1.14.1 update-source 10.1.14.4
Switch-4(config-router)# network 4.4.4.4/32
```

5. Create LoopBack0 interface on Switch-5, establish EBGP neighbor relationship with Switch-1 on the local interface, and publish the loopback port address under the BGP process

Configuration Switch-5

```
Switch-5(config)# interface eth-0-3
Switch-5(config-if)# no shutdown
Switch-5(config-if)# no switchport
Switch-5(config-if)# ip address 10.1.35.5/24
Switch-5(config)#interface loopback 0
Switch-5(config-if)# ip address 5.5.5.5/32
Switch-5(config-if)#exit
Switch-5(config)# router bgp 300
Switch-5(config-router)# neighbor 10.1.35.3 remote-as 100
Switch-5(config-router)# neighbor 10.1.35.3 update-source 10.1.35.5
Switch-5(config-router)# network 5.5.5.5/32
```

1.Check the configuration

Viewing BGP routing information, Switch-1 cannot learn forwarded from Switch-3 through Switch-2, and On Switch-3, EBGP routing information forwarded from Switch-1 cannot be learned through Switch-2. (Causing BGP routing black holes)

```
Switch-1# show ip route bgp
B          4.4.4.4/32 [20/0] via 10.1.14.4 eth-0-2, 00:32:50
```

```
Switch-2# show ip route bgp
B          4.4.4.4/32 [20/0] via 10.1.14.4 eth-0-2, 00:32:55
B          5.5.5.5/32 [20/0] via 10.1.35..5 eth-0-3, 00:32:55
```

```
Switch-3# show ip route bgp
B          5.5.5.5/32 [20/0] via 10.1.35..5 eth-0-3, 00:32:59
```

1.Solution: The following methods can be used to solve the BGP black hole routing phenomenon

1>Logical full interconnection, deployment of static routing or dynamic routing, and BGP full interconnection can achieve the role of logical full interconnection (simple scenes are more suitable, when the scene is complex, manual configuration is relatively large)

2>Deploy BGP reflector (Simple scenes are more suitable, when the scene is complex, the manual configuration is relatively large)

3>Establish a label tunnel (switch must support MPLS protocol)

4>Deploy BGP alliance (large backbone network is more suitable)

2.Take the deployment of BGP reflector as an example to solve the above BGP routing black hole phenomenon

Configuration Switch-2

```
Switch-2(config)# router bgp 100
Switch-2(config-router)# neighbor 1.1.1.1 route-reflector-client
Switch-2(config-router)# neighbor 3.3.3.3 route-reflector-client
```

Check the BGP routing information on Switch-1, Switch-2 and Switch-3, and find that the BGP routing table has been synchronized

```
Switch-1# show ip route bgp
B          4.4.4.4/32 [20/0] via 10.1.14.4 eth-0-2, 00:38:40
B          5.5.5.5/32 [20/0] via 10.1.35..5 eth-0-3, 00:38:40
```

```
Switch-2# show ip route bgp
B          4.4.4.4/32 [20/0] via 10.1.14.4 eth-0-2, 00:38:50
B          5.5.5.5/32 [20/0] via 10.1.35..5 eth-0-3, 00:38:50
```

```
Switch-3# show ip route bgp
B          4.4.4.4/32 [20/0] via 10.1.14.4 eth-0-2, 00:38:57
B          5.5.5.5/32 [20/0] via 10.1.35..5 eth-0-3, 00:38:57
```

8.4 Root Cause

To prevent loops in the AS, the BGP device does not advertise the routes learned from the IBGP peers to other IBGP peers.

8.5 Solution

When S58 series switches encounter BGP routing black holes when deploying BGP routing protocols, they can choose to deploy static routes or dynamic routes, deploy BGP reflectors, fully interconnect BGP, establish label tunnels, deploy BGP alliances, etc. in combination with business scenarios.

8.6 Suggestions and Conclusions

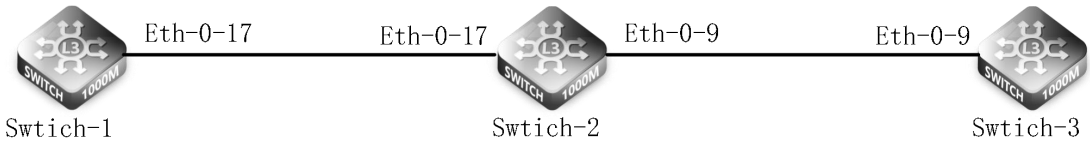
When deploying the BGP routing protocol, please follow the BGP routing delivery rules; when encountering the phenomenon of BGP routing black holes, it is recommended to select the appropriate solution to deal with the BGP routing black holes according to the business scenario.

9. Precautions for MPLS Protocol Configuration Considerations

9.1 Problem Description

In the scenario where the underlying network is reachable, LDP remote session establishment fails.

9.2 Topology Information



9.3 Handing Access

1.In interface mode, configure interface attributes, enable LDP and enable label forwarding, and configure the remote

Configure Switch-1

```
Switch-1(config)# interface eth-0-17
Switch-1(config-if)# no switchport
Switch-1(config-if)# ip address 11.11.17.1/24
Switch-1(config-if)# enable-ldp
Switch-1(config-if)# label-switching
Switch-1(config-if)# exit
Switch-1(config)# router ldp
Switch-1(config-router)# targeted-peer 3.3.3.3
Switch-1(config-router)# exit
```

Configure Switch-2

```
Switch-2(config)# interface eth-0-17
Switch-2(config-if)# no switchport
Switch-2(config-if)# ip address 11.11.17.2/24
Switch-2(config-if)# exit
Switch-2(config)# interface eth-0-9
Switch-2(config-if)# no switchport
Switch-2(config-if)# ip address 11.11.9.1/24
Switch-2(config-if)# exit
```

Configure Switch-3

```
Switch-3(config)# interface eth-0-9
Switch-3(config-if)# no switchport
Switch-3(config-if)# ip address 11.11.9.2/24
Switch-3(config-if)# enable-ldp
Switch-3(config-if)# label-switching
Switch-3(config-if)# exit
Switch-3(config)#router ldp
Switch-3(config-router)# targeted-peer 1.1.1.1
```

Enable RIP routing (Switch-1, 2, and 3 have the same configuration)

```
Switch-1(config)# router rip
Switch-1(config-router)# network 11.11.1.1/16
Switch-1(config-router)# network 1.1.1.1/32
Switch-1(config-router)# exit
```

```
Switch-2(config)# router rip
Switch-2(config-router)# network 11.11.1.1/16
Switch-2(config-router)# network 2.2.2.2/32
Switch-2(config-router)# exit
```

```
Switch-3(config)# router rip
Switch-3(config-router)# network 11.11.1.1/16
Switch-3(config-router)# network 3.3.3.3/32
Switch-3(config-router)# exit
```

Check the LDP session status, the remote ldp session establishment fails.

Switch-1

```
Switch-1# show ldp session
```

Enable LDP enablement under Switch-2 globally.

Switch-2

```
Switch-2(config)# router ldp
Switch-2(config-router)# exit
```

Check the session status of LDP, the remote session of ldp is established successfully

Switch-1

```
Switch-1# show ldp session
Peer IP Address      IF Name      My Role     State              KeepAlive
3.3.3.3              eth-0-17     Passive     OPERATIONAL        30
```

Switch-2

```
Switch-2# show ldp session
```

Switch-3

```
Switch-3# show ldp session
Peer IP Address      IF Name      My Role     State              KeepAlive
1.1.1.1              eth-0-9      Active      OPERATIONAL        30
```

9.4 Root Cause

When the LDP remote session is configured, the LDP function is not enabled on the intermediate device, so that the messag e message for establishing the LDP session cannot be forwarded through the intermediate device.

9.5 Solution

When establishing an LDP remote session, the intermediate forwarding device also needs to configure related LDP functions.

9.6 Suggestions and Conclusions

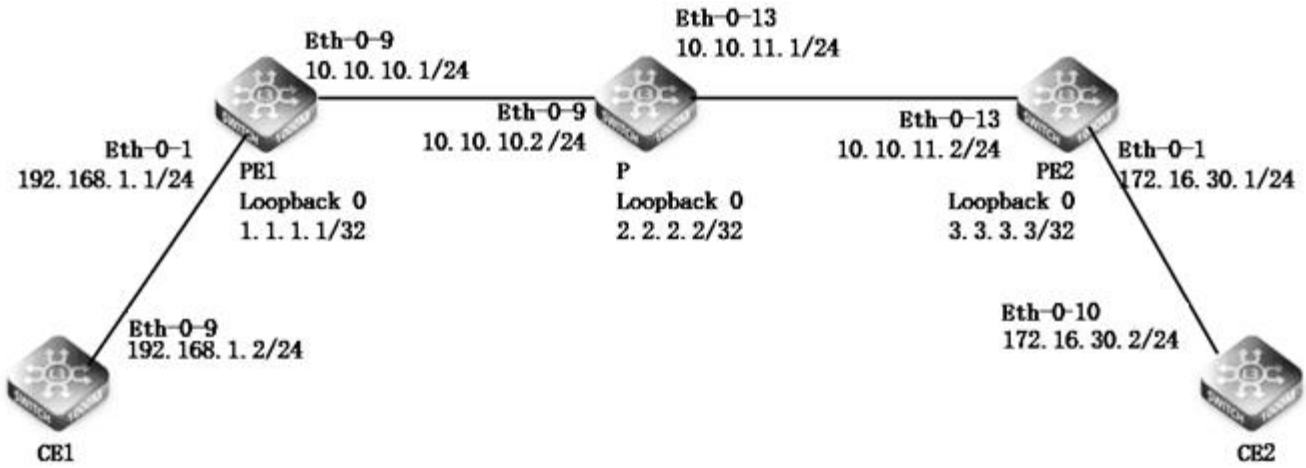
When configuring the LDP remote session fails, it is recommended to check whether the physical link is normal, then check whether the underlying network is reachable, and finally check whether the intermediate device enables the related LDP func tion.

10. Precautions for MPLS-VPN Function Configuration Considerations

10.1 Problem Description

S58 series switches in the deployment of MPLS-VPN business scenarios, the interface configuration is cleared, resulting in clie nt service traffic can not communicate.

10.2 Topology Information



10.3 Handing Access

1.Create a vrf instance on the PE device

```
PE1(config)#ip vrf vpn1
PE1(config-vrf)# rd 1:1
PE1(config-vrf)# route-target both 2:2
```

```
PE2(config)#ip vrf vpn1
PE2(config-vrf)# rd 1:1
PE2(config-vrf)# route-target both 2:2
```

2.Configure the switch interface, configure the IP address, and bind the vrf instance,

```
PE1(config)#int eth-0-1
PE1(config-if)# no shutdown
PE1(config-if)# no switchport
PE1(config-if)# ip address 192.168.1.1/24
PE1(config-if)# ip vrf forwarding vpn1
PE1(config-if)# int eth-0-9
PE1(config-if)# no shutdown
PE1(config-if)# no switchport
PE1(config-if)# ip address 10.10.10.1/24
PE1(config-if)# int loopback 0
PE1(config-if)# ip address 1.1.1.1/32
```

```
P(config)# int eth-0-9
P(config-if)# no shutdown
P(config-if)# no switchport
P(config-if)# ip address 10.10.10.2/24
P(config-if)# int eth-0-13
P(config-if)# no shutdown
P(config-if)# no switchport
P(config-if)# ip address 10.10.11.1/24
P(config-if)# int loopback 0
P(config-if)# ip address 2.2.2.2/32
```

```
PE2(config)# int eth-0-13
PE2(config-if)# no shutdown
PE2(config-if)# no switchport
PE2(config-if)# ip address 10.10.11.2/24
PE2(config-if)# int eth-0-1
PE2(config-if)# no shutdown
PE2(config-if)# no switchport
PE2(config-if)# ip address 10.10.11.2/24
PE2(config-if)# ip vrf forwarding vpn1
PE2(config-if)# int loopback 0
PE2(config-if)# ip address 3.3.3.3/32
```

3.Enable ldp, and enable ldp and label forwarding under the interface

```
PE1(config)#router ldp
PE1(config-router)#exit
PE1(config)#int eth-0-9
PE1(config-if)#enable-ldp
PE1(config-if)#label-switching
```

```
P(config)#router ldp
P(config-router)#exit
P(config)#int eth-0-9
P(config-if)#enable-ldp
P(config-if)#label-switching
P(config-if)#int eth-0-13
P(config-if)#enable-ldp
P(config-if)#label-switching
```

```
PE2(config)#router ldp
PE2(config-router)#exit
PE2(config)#int eth-0-13
PE2(config-if)#enable-ldp
PE2(config-if)#label-switching
```

4.Configure ospf in the Mpls domain to communicate with each other in the mpls domain

```
PE1(config)#router ospf 1
PE1(config-router)#router-id 1.1.1.1
PE1(config-router)#network 1.1.1.1/32 area 0
PE1(config-router)#network 10.10.10.1/24 area 0
```

```
P(config)#router ospf 1
P(config-router)#router-id 2.2.2.2
P(config-router)#network 2.2.2.2/32area 0
P(config-router)#network 10.10.10.2/24 area 0
P(config-router)#network 10.10.11.1/24 area 0
```

```
PE2(config)#router ospf 1
PE2(config-router)#router-id 3.3.3.3
PE2(config-router)#network 3.3.3.3/32 area 0
PE2(config-router)#network 10.10.11.2/24 area 0
```

1.Establish mp-bgp neighbor relationship between PEs

```
PE1(config)#router bgp 1
PE1(config-router)#bgp router-id 1.1.1.1
PE1(config-router)#neighbor 3.3.3.3 remote-as 1
PE1(config-router)#neighbor 3.3.3.3 update-source loopback 0
PE1(config-router)#address-family vpnv4 unicast
PE1(config-router-af)#neighbor 3.3.3.3 activate
PE1(config-router-af)#neighbor 3.3.3.3 send-community both
PE1(config-router-af)#exit
PE1(config-router)#address-family ipv4 vrf vpn1
PE1(config-router-af)#redistribute connected
```

```
PE2(config)#router bgp 1
PE2(config-router)#bgp router-id 3.3.3.3
PE2(config-router)#neighbor 1.1.1.1 remote-as 1
PE2(config-router)#neighbor 1.1.1.1 update-source loopback 0
PE2(config-router)#address-family vpnv4 unicast
PE2(config-router-af)#neighbor 1.1.1.1 activate
PE2(config-router-af)#neighbor 1.1.1.1 send-community both
PE2(config-router-af)#exit
PE2(config-router)#address-family ipv4 vrf vpn1
PE2(config-router-af)#redistribute connected
```

2.Establish ospf neighbor relationship between PE and CE

```
PE1(config)#router ospf 2 vrf vpn1
PE1(config-router)#network 192.168.1.0 0.0.0.255 area 1
PE1(config-router)#redistribute bgp
PE1(config-router)#redistribute connected
```

```
PE2(config)#router ospf 2 vrf vpn1
PE2(config-router)#network 172.16.30.0 0.0.0.255 area 2
PE2(config-router)#redistribute bgp
PE2(config-router)#redistribute connected
```

```
CE1(config)#int eth-0-9
CE1(config-if)#no shutdown
CE1(config-if)#no switchport
CE1(config-if)#ip address 192.168.1.2/24
CE1(config-if)#exit
CE1(config)#router ospf 2
CE1(config-router)#network 192.168.1.2/24 area 1
```

```
CE2(config)#int eth-0-10
CE2(config-if)#no shutdown
CE2(config-if)#no switchport
CE2(config-if)#ip address 172.16.30.2/24
CE2(config-if)#exit
CE2config)#router ospf 2
CE2(config-router)#network 176.16.30.2/24 area 2
```

3.Check the PE1 device, interface IP configuration information, and find that the interface ip bound to the vrf instance has been cleared

```
PE1(config)#int eth-0-1
PE1(config-if)#no shutdown
PE1(config-if)#no switchport
PE1(config-if)#ip address 192.168.1.1/24
PE1(config-if)# ip vrf forwarding vpn1
```

View the IP address under the interface (after binding the VRF instance table, the IP address under the interface will be cleared by default)

```
PE1# show ip interface brief
Interface                IP-Address      Status                Protocol
eth-0-1                  unassigned      up                    up
eth-0-9                  10.10.10.1      up                    up
vlan1                    unassigned      down                  down
loopback0                1.1.1.1         up                    up
```

Reconfigure the IP address under the interface.

```
PE1(config)#int eth-0-1
PE1(config-if)#ip address 192.168.1.1/24
```

Check the configuration under the interface again. At this time, the interface IP is not cleared.

```
PE1(config-if)# show this
interface eth-0-1
 no switchport
 ip vrf forwarding vpn1
 ip address 192.168.1.1/24
```

Reconfigure the IP address under the interface of the PE1 and PE2 devices, and send the ping packet on the CE1 device to the CE2 device. At this time, the ping can be the same, indicating that the MPLS-VPN service can communicate normally.

```
CE1# ping -a 192.168.1.2 172.16.30.2
PING 172.16.30.2 (172.16.30.2) from 192.168.1.2 : 56(84) bytes of data.
64 bytes from 172.16.30.2: icmp_seq=1 ttl=61 time=1.34 ms
64 bytes from 172.16.30.2: icmp_seq=2 ttl=61 time=1.37 ms
64 bytes from 172.16.30.2: icmp_seq=3 ttl=61 time=1.22 ms
64 bytes from 172.16.30.2: icmp_seq=4 ttl=61 time=1.23 ms
64 bytes from 172.16.30.2: icmp_seq=5 ttl=61 time=1.17 ms
--- 172.16.30.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.173/1.268/1.373/0.076 ms
```

View the routing table of the CE device

```
CE1# 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
       Dc - DHCP Client
       [*] - [AD/Metric]
       * - candidate default
O E2     172.16.30.0/24 [110/1] via 192.168.1.1, eth-0-9, 00:30:38
C        192.168.1.0/24 is directly connected, eth-0-9
C        192.168.1.2/32 is in local loopback, eth-0-9
```

10.4 Root Cause

When the interface IP address is first configured on the PE device, and then the interface is bound to the VPN instance, the interface information is cleared, causing the underlying network to be unreachable, which ultimately affects the interruption 0 f client service flow.

10.5 Solution

When configuring MPLS-VPN service scenarios for S58 series switches, follow the configuration sequence, and configure the IP information of the interface after the interface is bound to the VPN instance.

10.6 Suggestions and Conclusions

When configuring the MPLS-VPN service scenario fails, it is recommended to check whether the physical link is connected fir st, and then check whether the configuration is correct. In summary, when configuring the MPLS-VPN business scenario, plea se follow the configuration manual for standard operation.

Note:

S58 series switches include S5850 model switches and S5800 model switches. Currently, only S5850 model switches support MPLS-VPN services, and S5800 model switches do not currently support them.

https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.