S5900-24S4T2Q Switch Technical White Paper

After-sale Instructions for Error-prone Issues

Model: S5900-24S4T2Q

TECHNICAL WHITE PAPER

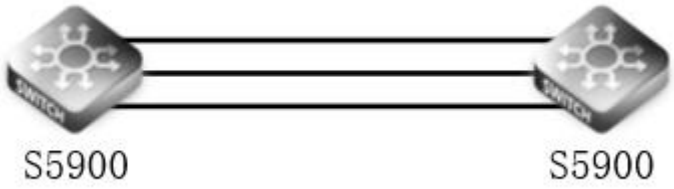
Contents

1. LACP Function Configuration Failure Issue

1.1 Issue Description

When the LACP function of the S5900 switch is configured, the LACP negotiation state is generated as the linedown state.

1.2 Topology Information



1.3 Handling Process

1.First use CRT software to connect to the device and create an aggregation group 1 on the device

```
S5900-1#config
S5900-1_config#interface port-aggregator 1
S5900-1_config_p1#quit
```

```
S5900-2#config
S5900-2_config#interface port-aggregator 1
S5900-2_config_p1#quit
```

2.Enter the interface configuration view and add the interface to the aggregation group to configure LACP mode. Both ends are configured in Passive mode.

```
S5900-1_config#int g0/1
S5900-1_config_g0/1#aggregator-group 1 mode lacp passive
S5900-1_config_g0/1#int g0/2
S5900-1_config_g0/2#aggregator-group 1 mode lacp passive
S5900-1_config_g0/2#int g0/3
S5900-1_config_g0/3#aggregator-group 1 mode lacp passive
```

```
S5900-2_config#int g0/1
S5900-2_config_g0/1#aggregator-group 1 mode lacp passive
S5900-2_config_g0/1#int g0/2
S5900-2_config_g0/2#aggregator-group 1 mode lacp passive
```

```
S5900-2_config_g0/2#int g0/3

S5900-2_config_g0/3#aggregator-group 1 mode lacp passive
```

3.Check the status of lacp on the device at this time, (UI) is not in the aggregation group, indicating that the negotiation is not successful.

```
S5900-1#show aggregator-group 1 brief

                        Aggregator-group brief infomation

                        --------------------------------

Group: 1              Speed: 1000       interval: 30

          AggregatedCount: 0       LastAggregated:

          LastDetached:

-----------------------------------------------------------

System ID : 32768 649D.9920.6C4B       Partner : 0 0000.0000.0000

 Group ID : 32768 649D.9920.6C4B          state : lineDown

Max Ports : 32                                ports : 3

-----------------------------------------------------------

Flags:   D - down             A - Use In port-aggregator

            U - Up               I - Not In port-aggregator

            d - default


g0/3(UI)       g0/1(UI)       g0/2(UI)
```

4.Change an end to active mode

```
S5900-1_config#interface g0/1

S5900-1_config_g0/1#no aggregator-group

S5900-1_config_g0/1#interface g0/2

S5900-1_config_g0/2#no aggregator-group

S5900-1_config_g0/2#interface g0/3

S5900-1_config_g0/3#no aggregator-group

S5900-1_config_g0/3#aggregator-group 1 mode lacp active

S5900-1_config_g0/3#interface g0/2

S5900-1_config_g0/2#aggregator-group 1 mode lacp active

S5900-1_config_g0/2#interface g0/1

S5900-1_config_g0/1#aggregator-group 1 mode lacp active
```

5.Check the status of LACP on the device at this time, (UA).

```
S5900-1#show aggregator-group 1 brief

                        Aggregator-group brief infomation

                        ------------------------------

Group: 1              Speed: 1000       interval: 30

          AggregatedCount: 1       LastAggregated: 01-01 00:03:30

          LastDetached:

-------------------------------------------------------

System ID : 32768 649D.9920.6C4B       Partner : 32768 649D.9921.54E2

 Group ID : 32768 649D.9920.6C4C          state : lineUp

Max Ports : 32                                ports : 3

-------------------------------------------------------

Flags:   D - down            A - Use In port-aggregator

            U - Up             I - Not In port-aggregator

            d - default


g0/3(UA)       g0/1(UA)       g0/2(UA)
```

1.4 Root Cause

In summary, in Active mode, the switch actively initiates the aggregation negotiation process, while Passive mode passively accepts the aggregation negotiation process. When selecting LACP aggregation, the aggregation will not succeed if both sides of the port aggregation use Passive mode, because both ends will wait for the peer to initiate the aggregation negotiation process. There is also a situation where, for the occasional phenomenon, when interfacing with a friend's device LACP, the aggregation group does not allow vlan 1, the state of valn 1 is down, the state of LACP is linedown, and after vlan 1, the state of LACP is lineup.

1.5 Solution

When configuring LACP aggregation, avoid configuring Passive at both ends to ensure that at least one end is active.
When interfacing with a friend's device, the state of LACP is linedown, and the protocol-status state of vlan 1 is down. You can try to allow vlan1 under the aggregation group.

1.6 Suggestions and Conclusions

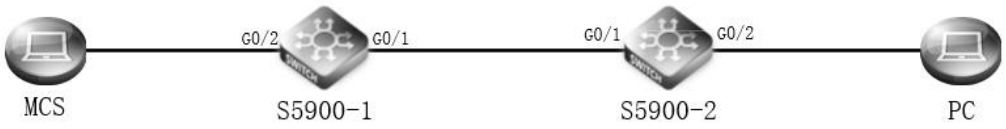
After the configuration fails, it is recommended to check the configuration first to see whether the configuration is configured according to the specified configuration template.

2. Multicast PIM-SM Configuration Failure Issue

2.1 Problem Description

When the multicast PIM-SM function of the S5900 switch is configured, the PC cannot receive multicast traffic. In the SSM model scenario, the multicast stream cannot be received.

2.2 Topology Information



2.3 Handing Access

1.First use CRT software to connect the devices and start global multicast on the two devices respectively

```
S5900-1_config#ip multicast-routing
```

```
S5900-2_config#ip multicast-routing
```

2.Create vlan2 on S5900-1 and configure the link type and allowed vlan.

```
S5900-1_config#vlan 2
S5900-1_config_vlan2#quit
S5900-1_config#int g0/1
S5900-1_config_g0/1#switchport mode trunk
S5900-1_config_g0/1#switchport trunk vlan-allowed 2
S5900-1_config_g0/1#quit
S5900-1_config#int g0/2
S5900-1_config_g0/2#switchport mode access
```

3.Create vlan2 on S5900-2 and configure the link type and allowed vlan.

```
S5900-2_config#vlan 2
S5900-2_config_vlan2#quit
S5900-2_config#int g0/1
S5900-2_config_g0/1#switchport mode trunk
S5900-2_config_g0/1#switchport trunk vlan-allowed 2
S5900-2_config_g0/1#int g0/2
S5900-2_config_g0/2#switchport mode access
```

4.Configure pim-sm under the vlan process of the two devices. If you do not configure the corresponding port, you cannot send and receive pim-sm protocol messages.

```
S5900-1_config#int vlan1
S5900-1_config_v1#ip address 192.168.1.1 255.255.255.0
S5900-1_config_v1#ip pim-sm
S5900-1_config_v1#quit
S5900-1_config#int vlan 2
S5900-1_config_v2#ip address 10.1.1.1 255.255.255.0
S5900-1_config_v2#ip pim-sm
```

```
S5900-2_config#int vlan 1
S5900-2_config_v1#ip address 10.1.2.1 255.255.255.0
S5900-2_config_v1#ip pim-sm
S5900-2_config_v1#int vlan 2
S5900-2_config_v2#ip address 10.1.1.2 255.255.255.0
S5900-2_config_v2#ip pim-sm
```

5.Configure the IP address of the loopback0 interface on S5900-1 and enable PIM-SM. Let S5900-1 be RP.

```
S5900-1_config#int l0
S5900-1_config_l0#ip address 6.6.6.6 255.255.255.255
S5900-1_config_l0#ip pim-sm
S5900-1_config_l0#quit
```

6.Configure OSPF dynamic routing protocol between the two devices to make routing interoperable.

```
S5900-1_config#router ospf 1
S5900-1_config_ospf_1#network 10.1.1.1 255.255.255.255 area 0
S5900-1_config_ospf_1#network 6.6.6.6 255.255.255.255 area 0
S5900-1_config_ospf_1#network 192.168.1.0 255.255.255.0 area 0
```

```
S5900-2_config#router ospf 1
S5900-2_config_ospf_1#network 10.1.1.2 255.255.255.255 area 0
S5900-2_config_ospf_1#network 10.1.2.0 255.255.255.0 area 0
```

7.Check the ospf neighbor information to see if the neighbor is established.

```
S5900-1#show ip ospf neighbor
--------------------------------------------------------------------------------
                                OSPF process: 1
```

```
                                    AREA: 0
Neighbor ID      Pri    State              DeadTime    Neighbor Addr    Interface
192.168.1.2      1      FULL/DR            31          10.1.1.2         VLAN2
----------------------------------------------------------------------------------------
```

8.Check the routing table on S5900-2 to see if you learned the routing information of S5900-1.

```
S5900-2#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2, IA - ISIS inter-level
       I - IPSEC type

VRF ID: 0

S       0.0.0.0/0           [1,0] via 10.32.133.254(on GigaEthernet0/0)
O       6.6.6.6/32          [110,2] via 10.1.1.1(on VLAN2)
C       10.1.1.0/24         is directly connected, VLAN2
C       10.1.2.0/24         is directly connected, VLAN1
C       10.32.132.0/23      is directly connected, GigaEthernet0/0
O       192.168.1.0/32          [110,2] via 10.1.1.1(on VLAN2)
```

9.To enable static RP on both devices, you need to specify the RP address on each PIM route. This address must be reachable on each device.

```
S5900-1_config#router pim-sm
S5900-1_config_ps#static-rp 6.6.6.6
```

```
S5900-2_config#router pim-sm
S5900-2_config_ps#static-rp 6.6.6.6
```

10.View the pim-sm neighbor information on the switch.

```
S5900-2#show ip pim-sm neighbor
```

```
PIM-SMv2 Neighbor Table
Neighbor              Interface                Uptime/Expires      DR
Address                                                            Prior
10.1.1.1              v2                       00:05:32/00:01:15   1
```

11. Enable the SSM function and configure the SSM group range. You can also use the default 232.0.0.0/8 as the SSM group range.

```
S5900-1_config#router pim-sm
S5900-1_config_ps#ssm range grp_range
S5900-1_config_ps#quit
S5900-1_config#ip access-list standard grp_range
S5900-1_config_std#permit 224.1.2.3 255.255.255.255
```

```
S5900-2_config#router pim-sm
S5900-2_config_ps#ssm range grp_range
S5900-2_config_ps#quit
S5900-2_config#ip access-list standard grp_range
S5900-2_config_std#permit 224.1.2.3 255.255.255.255
```

12.Use VLC to simulate multicast source

13.On the PC, select IGMPv3, select the multicast group and multicast source, and capture packets. The multicast stream can be seen as follows.

No.	Time	Source	Destination	Protocc	Lengt	Info
10255	556.453000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10256	556.766000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10257	556.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10258	556.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10259	556.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10260	556.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10261	556.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10262	557.109000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10263	557.281000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10264	557.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10265	557.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10266	557.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10267	557.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10268	557.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10269	557.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10270	557.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10271	557.766000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10272	557.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10273	557.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10274	557.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10275	557.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10276	557.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10277	557.938000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10278	558.266000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10280	558.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10281	558.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10282	558.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328
10283	558.438000	192.168.1.3	224.1.2.3	UDP	1370	4193 → 0 Len=1328

2.4 Root Cause

In summary, if pim-sm is not enabled on the interface, the port cannot receive pim protocol messages. In the SSM scenario, if the multicast

address is not within the specified SSM group range, the multicast source information cannot be passed to the receiver.

2.5 Solution

Before configuring basic pim-sm functions, you need to ensure the configuration of unicast routing to ensure that the network layer in the domain is reachable. When configuring the pim-sm protocol, it is recommended to enable pim-sm on all its non-border interfaces. If the multicast group is not within the default 232.0.0.0/8 group range, it is recommended to manually configure the SSM group range

2.6 Suggestions and Conclusions

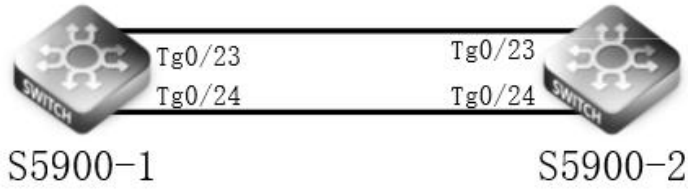
When configuring pim-ssm, the ssm group uses the manually configured group range.

3. BVSS Establishment failure Scenario Failure Issue

3.1 Problem Description

On S5900 switches, the stack is called BVSS, but during the configuration of the stack, the stack cannot be negotiated.

3.2 Topology information



3.3 Handing Process

3.3.1 First connect the device using CRT software, and configure the virtualization ports on the two devices.

```
S5900-1_config#bvss
S5900-1_config_bvss#bvss interface 1 type tGigaEthernet port 23 group 1
S5900-1_config_bvss#bvss interface 2 type tgigaEthernet port 24 group 1
```

```
s5900-2_config#bvss
s5900-2_config_bvss#bvss interface 1 type tGigaEthernet port 23 group 2
s5900-2_config_bvss#bvss interface 2 type tGigaEthernet port 24 group 2
```

3.3.2 Configure the virtualization mode of the two devices separately.

There are two modes, Normal mode only supports 2 device virtualization, Enhanced mode supports up to 4 device virtualization, but currently the device only supports normal mode.

```
S5900-1_config#bvss
S5900-1_config_bvss#bvss mode normal
```

```
s5900-2_config#bvss
s5900-2_config_bvss#bvss mode normal
```

3.3.3 Configure the virtualization domain to which the two devices belong.

```
S5900-1_config_bvss#bvss domain-id 1
```

```
s5900-2_config_bvss#bvss domain-id 1
```

3.3.4 Configure the virtualized member numbers of the two devices separately.

```
S5900-1_config_bvss#bvss member-id 1
```

```
s5900-2_config_bvss#bvss member-id 2
```

3.3.5 Configure the virtualization priority of the two devices separately

```
S5900-1_config_bvss#bvss priority 150
```

```
s5900-2_config_bvss#bvss priority 100
```

3.3.6 Enable virtualization

```
S5900-1_config#bvss
```

```
S5900-1_config_bvss#bvss enable
```

```
S5900-2_config#bvss
S5900-2_config_bvss#bvss enable
```

3.3.7 Save the virtualization configuration and restart the device.

```
S5900-1#write bvss-config
S5900-1#reboot
```

```
S5900-2#write bvss-config
S5900-2#reboot
```

3.3.8 After the restart, the stack negotiation is established. You can use the command to view the port to see the stack establishment.

```
Switch>enable
Switch#show interface brief
Port       Description                    Status     Vlan       Duplex   Speed    Type
g0/0                                      up                    full     1000Mb   1000BASE-TX
g1/0/1                                    shutdown   1          auto     auto     Giga-TX
g1/0/2                                    shutdown   1          auto     auto     Giga-TX
g1/0/3                                    shutdown   1          auto     auto     Giga-TX
g1/0/4                                    shutdown   1          auto     auto     Giga-TX
g2/0/1                                    shutdown   1          auto     auto     Giga-TX
g2/0/2                                    shutdown   1          auto     auto     Giga-TX
g2/0/3                                    shutdown   1          auto     auto     Giga-TX
g2/0/4                                    shutdown   1          auto     auto     Giga-TX
tg1/0/1                                   shutdown   1          full     10000Mb  10Giga-FX
tg1/0/2                                   shutdown   1          full     10000Mb  10Giga-FX
tg1/0/3                                   shutdown   1          full     10000Mb  10Giga-FX
tg1/0/4                                   shutdown   1          full     10000Mb  10Giga-FX
tg1/0/5                                   shutdown   1          full     10000Mb  10Giga-FX
tg1/0/6                                   shutdown   1          full     10000Mb  10Giga-FX
tg1/0/7                                   shutdown   1          full     10000Mb  10Giga-FX
tg1/0/8                                   shutdown   1          full     10000Mb  10Giga-FX
tg1/0/9                                   shutdown   1          full     10000Mb  10Giga-FX
tg1/0/10                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/11                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/12                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/13                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/14                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/15                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/16                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/17                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/18                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/19                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/20                                  shutdown   1          full     10000Mb  10Giga-FX
tg1/0/21                                  shutdown   1          full     10000Mb  10Giga-FX
```

tg1/0/22	shutdown	1	full	10000Mb	10Giga-FX
tg1/0/23	up	1	full	10000Mb	10Giga-FX
tg1/0/24	up	1	full	10000Mb	10Giga-FX
tg2/0/1	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/2	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/3	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/4	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/5	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/6	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/7	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/8	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/9	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/10	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/11	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/12	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/13	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/14	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/15	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/16	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/17	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/18	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/19	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/20	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/21	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/22	shutdown	1	full	10000Mb	10Giga-FX
tg2/0/23	up	1	full	10000Mb	10Giga-FX
tg2/0/24	up	1	full	10000Mb	10Giga-FX
qtg1/0/1	shutdown	1	full	40000Mb	40Giga-FX
qtg1/0/2	shutdown	1	full	40000Mb	40Giga-FX
qtg2/0/1	shutdown	1	full	40000Mb	40Giga-FX
qtg2/0/	shutdown	1	full	40000Mb	40Giga-FX
v1	up				
n0	up				

3.3.9 View virtualization information through commands.

```
Switch#show bvss management
bvss member 1 management information:
 active member: 1, standby member: 2
 lgroup: 1-2, rgroup:
 orphan group:-1, normal group:-1
 HT[l]:, HT[r]: ,HT[a]:
 internal topology:0 , global topology: LINE-TOPO
 L to member 1: unknown R to member 1:unknown
 L to member 2: 1 R to member 2:unknown
 L to member 3: unknown R to member 3:unknown
```

```
 L to member 4: unknown R to member 4:unknown
hg route
 to member 1: local
 to member 2: l
 to member 3: unreachable
 to member 4: unreachable
```

3.3.10 Display the status information of RNP through commands, and you can view the role of each member device negotiated in the virtualization domain.

```
Switch#show bvss rnp

  RNP is running. CfgPri 150, SwitchType 0x10eb, Slot 0
  System started, ignoreTimeoutCnt 0
  DomainId 1, MemberId 1, LoopTopology 0, Merge 0, Master State
  MasterMemId 1, BackupMemId 2, MasterGlbMacAddr 649d.9920.6c4b
  OldMasterMemberId 0, OldMasterWhile 0, txAdvPduCnt 75
  lacpMad: OldActiveId 0, OldActiveWhile 0, ActiveWhile 0

  bvss link group 1 is usable, bvss link group 2 is not usable.

  Pri info for member 1 (SwitchType 10eb, slot 0):
     Priority 150, RunningTime 442, MAC 649d.9920.6c4b

  Pri info for member 2 (SwitchType 10eb, slot 0):
     Priority 100, RunningTime 437, MAC 649d.9921.54e2
```

3.4 Root Cause

1. The configuration virtualization mode is incorrect. Currently, the device only supports normal mode, and supports up to two devices stacked.
2. BVSS uses a virtual domain to manage the same set of virtualized devices. Devices in the same virtual domain are virtualized, and each member device in the virtual domain has a different number.
3. After the BVSS configuration is ok, you must save the BVSS configuration before restarting the switch to take effect.

3.5 Solution

1. It is currently recommended that up to two devices do BVSS.
2. Two devices with different numbers in the same domain.
3. The switch version must be consistent.

3.6 Suggestions and Conclusions

When using the BVSS function on an S5900 device, it is recommended to use up to two devices and the mode is normal. The current running configuration of virtualization refers to the running virtualized configuration of the device. The current virtualized configuration is a configuration that the user may modify or add during the running of the virtualization. These configurations do not take effect. You need to save and restart the device to take effect. Keep in mind that the software version must be consistent when configuring BVSS. If they are inconsistent, a device will restart infinitely or the stack will not be established.

4. 802.1x Authentication Failure Issue

4.1 Problem Description

On the S5900 switches, when the dot1x function is used, the interaction between the AAA server and the device is normal, and the PC authentication fails.

4.2 Topology Information

4.3 Handing Process

1.First use CRT software to connect the device, specify the radius server address and pre-shared key, so that the device can pass the authentication information to the AAA server.

```
S5900_config#radius-server host 10.32.133.248
S5900_config#radius-server key Aa123456
```

2. Enable 802.1x authentication globally and enable authentication on the port connected to the PC.

```
S5900_config#dot1x enable
S5900_config#int g0/2
S5900_config_g0/2#dot1x port-control auto
```

3.Configure AAA authentication parameters.

```
S5900_config#aaa authentication dot1x fs-g0/2 group radius
S5900_config#aaa accounting network fs_acc start-stop group radius
```

4.Configure 802.1x re-authentication and authentication cycle to ensure the legitimacy of the authentication client.

```
S5900_config#dot1x re-authentication
S5900_config#dot1x timeout re-authperiod 10
```

5.Enabling 802.1x guest-vlan will give the corresponding port limited access rights when the client does not respond.

Initially, the guest-vlan id of each port is 0. At this time, even if the global guest-vlan function is turned on, it will not work. Only in the port configuration mode, after the guest-vlan id is configured, the guest-vlan works

```
S5900_config#dot1x guest-vlan
```

6.Call the AAA authentication parameters under the interface and set the authentication type to eap.

```
S5900_config#int g0/2
S5900_config_g0/2#dot1x authentication method fs-g0/2
S5900_config_g0/2#dot1x accounting enable
S5900_config_g0/2#dot1x accounting method fs_acc
```

```
S5900_config_g0/2#dot1x authentication type eap
```

7.Use 802.1x authentication on the PC, enter the username and password of the AAA server resource pool, and the authentication is successful.

8.Use commands on the device to view dot1x information.

```
Switch#show dot1x


   802.1X Parameters
reAuthen              Yes
reAuth-Period      10
quiet-Period       60
Tx-Period             30
Supp-timeout       30
Server-timeout     30
reAuth-max          5
max-request         3
authen-type         Eap


IEEE 802.1x on port g0/2 enabled
defVlanID: 1
currentVlanID: 1
formerVlanID: 0
voice_vlanID: 0


IEEE 802.1x accounting on port g0/2 enabled
   Authen Type                    Eap
   Authen Method                  fs-g0/2
   Account Method                 fs_acc
   Accounting                     True
   Permit Users                   All Users
   Permit Macs                    All Macs
   Multiple Auth                  Disallowed(current 0)
   Multiple hosts                 Disallowed
```

```
Current Supplicant                  fs(8cec.4bad.036b)
    Authorized                          Yes
    Current Identifier                  154

    Authenticator State Machine
        State                           Authenticated
        Reauth Count                    0
        auth vlan                       1
    Backend State Machine
        State                           Idle
        Request Count                   0
        Identifier (Server)             153
    Port Timer Machine
        Auth Tx While Time              27
        Backend While Time              177
        Backend accWhile Time           147
        Backend updateWhile Time        0
        reAuth Wait Time                7
        Hold Wait Time                  0
        Misc Mab AgingWhile             0
        Last Time After Rx Packet from Supplicant3
```

9.View log information on the AAA server.

RADIUS Authentication Details

Generated At: 2020-04-09 11:39:22.361

Authentication Summary	
Logged At:	2020-04-09 11:38:59.631
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	fs
MAC/IP Address:	8C-EC-4B-AD-03-6B
Network Device:	alex-sw1
Access Service:	Default Network Access
Identity Store:	Internal Users
Authorization Profiles:	Permit Access
CTS Security Group:	
Authentication Method:	MSCHAPV2
Authentication Result	
	{User-Name=fs; Class=CACS:ACS/375606312/170; }
Session Events	
	2020-04-09 11:38:59.631
	Radius authentication passed for USER: fs MAC: 8C-EC-4B-AD-03-6B AUTHTYPE: PEAP(EAP-MSCHAPv2)
	Radius authentication passed
Authentication Details	
Logged At:	2020-04-09 11:38:59.631
ACS Time:	2020-04-09 11:38:59.615
ACS Instance:	ACS
Authentication Method:	MSCHAPV2
EAP Authentication Method:	EAP-MSCHAPv2

4.4 Root Cause

In summary, when the pre-shared key configured on the device is inconsistent with the pre-shared key added on the AAA server, the device cannot pass the authentication information to the AAA server, resulting in authentication failure. Inconsistent eap-type between the PC and the AAA server can also cause authentication failure.

4.5 Solution

When the PC authentication fails, the following factors may be considered:

4.5.1 Whether the parameters configured on the device are ok and whether the pre-shared key is consistent with the server.

4.5.2 Whether the authentication protocol on the PC side is allowed to pass on the AAA server, and whether there is the user name and password entered during the authentication on the PC side. Whether the Eap-type is consistent with the PC.

4.6 Suggestions and Conclusions

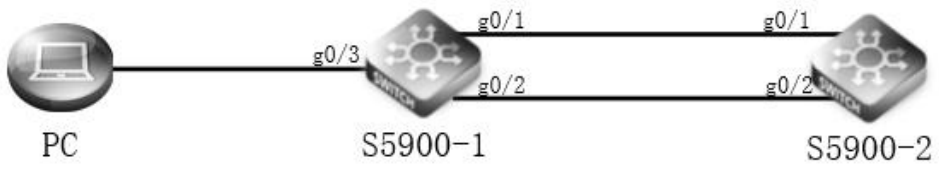
First of all, we must ensure that the interaction between the device and the AAA server is normal. You can read the log information of the AAA server during the process to obtain the cause of the problem.

5. Network Loop-MAC Address Drift Processing Issue

5.1 Problem Description

During the operation of the S5900 switch, a loop in the network caused the device memory, cpu to fill up, and the PC to freeze.

5.2 Topology Information



5.3 Handing Process

5.3.1 Use CRT software to connect the devices first, and close the spanning tree globally on the two devices.

```
S5900-1_config#no spanning-tree
```

```
S5900-2_config#no spanning-tree
```

5.3.2 Add the G0/1 and G0/2 interfaces of the S5900-1 device to VLAN 10, add the G0/1 and G0/2 interfaces of the S5900-2 device to VLAN 10, and add the IP addresses of the S5900-1 and S5900-2 to the VLAN 10 interface Configured on the same network segment, PC1 connects to the g0/3 interface of the S5900-1 switch.

```
S5900-1_config#vlan 10
S5900-1_config_vlan10#quit
S5900-1_config#interface vlan 10
S5900-1_config_v10#ip address 192.168.1.1 255.255.255.0
S5900-1_config_v10#quit
S5900-1_config#interface g0/1
S5900-1_config_g0/1#switchport mode access
S5900-1_config_g0/1#switchport pvid 10
S5900-1_config_g0/1#interface g0/2
S5900-1_config_g0/2#switchport mode access
S5900-1_config_g0/2#switchport pvid 10
S5900-1_config_g0/2#interface g0/3
S5900-1_config_g0/3#switchport mode access
S5900-1_config_g0/3#switchport pvid 10
```

```
S5900-1_config_g0/3#quit
```

```
S5900-2_config#vlan 10
S5900-2_config_vlan10#quit
S5900-2_config#interface vlan 10
S5900-2_config_v10#ip address 192.168.1.2 255.255.255.0
S5900-2_config_v10#quit
S5900-2_config#interface g0/1
S5900-2_config_g0/1#switchport mode access
S5900-2_config_g0/1#switchport pvid 10
S5900-2_config_g0/1#interface g0/2
S5900-2_config_g0/2#switchport mode access
S5900-2_config_g0/2#switchport pvid 10
S5900-2_config_g0/2#quit
```

5.3.3 Configure the IP to 192.168.1.3 on the PC. At this time, the PC is abnormally stuck and the network has a loop. Check the MAC address table of the S5900-1 device and find that the MAC address drifts.

```
S5900-1#show mac address-table
            Mac Address Table (Total 1)
------------------------------------------


Vlan      Mac Address           Type            Ports
----      -----------           ----            -----
10        8cec.4bad.036b        DYNAMIC   g0/2
S5900-1#show mac address-table
            Mac Address Table (Total 1)
------------------------------------------


Vlan      Mac Address           Type            Ports
----      -----------           ----            -----
10        8cec.4bad.036b        DYNAMIC   g0/1
```

5.3.4 Start spanning tree under global configuration on both switches.

```
S5900-1_config#spanning-tree
```

```
S5900-2_config#spanning-tree
```

5.3.5 At this time, the MAC address drift ends and the network returns to normal. View spanning tree information.

```
S5900-1#show spanning-tree

Spanning tree enabled protocol RSTP(2004)

RSTP
  Root ID      Priority    32768
               Address     649D.9920.6C4B
               This bridge is the root
               Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID    Priority    32768
               Address     649D.9920.6C4B
               Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface          Role Sts Cost      Pri.Nbr  Type
---------------- ---- --- --------- -------- --------------------
g0/1               Desg FWD 20000     128.17   P2p
g0/2               Desg FWD 20000     128.18   P2p
g0/3               Desg FWD 200000    128.19   Edge
```

```
S5900-2#show spanning-tree

Spanning tree enabled protocol RSTP(2004)

RSTP
  Root ID      Priority    32768
               Address     649D.9920.6C4B
               Port        GigaEthernet0/1
               Cost        20000
```

```
                Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec


  Bridge ID    Priority       32768

                Address        649D.9921.54E2

                Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec


Interface              Role Sts Cost          Pri.Nbr    Type

---------------- ---- --- --------- -------- ------------------------

g0/1                   Root FWD 20000         128.17     P2p

g0/2                   Altn BLK    20000      128.18     P2p
```

5.3.6 It can be seen that the g0/2 interface of S5900-2 is blocked, and the network loop has been released.

5.3.7 There is no drift in the MAC address table on the switch, and the results also correspond to each other.

```
S5900-1#show mac address-table

            Mac Address Table (Total 2)

------------------------------------------


Vlan       Mac Address            Type            Ports

----       ---------------          ----            -----

10          8cec.4bad.036b       DYNAMIC     g0/3

10          649d.9921.54e2       DYNAMIC     g0/1
```

5.4 Root Cause

In summary, a loop occurs on the bottom network of the device, causing ARP broadcast storms, causing PC-side stalls and MAC address drift.

5.5 Solution

1. Turn on protocols such as spanning tree to prevent loops.
2. Shut down or unplug the link port.
3. Add the link to the aggregation group so that the two links are logically one link.

5.6 Suggestions and Conclusions

When the MAC address drift phenomenon occurs in the service environment, you can choose the appropriate solution to deal with the needs of the business; when the MAC address drift phenomenon occurs, the sooner the better, otherwise the memory of the switch device will be consumed unrestricted, causing cards Phenomenon such as lag or network shock.

6. DHCP-Snooping Processing Scenario

6.1 Problem Description

The DHCP-Snooping function is configured during the operation of the S5900 switch, but when the PC obtains the IP address, it cannot obtain the IP address.

6.2 Topology Information

6.3 Handing Process

1.First use CRT software to connect to the device, configure the dhcp service and address pool on the S58 switch, and enable dhcp on the interface.

```
Switch(config)# service dhcp enable
Switch(config)# dhcp server
Switch(config)# dhcp pool pool1
Switch(config-dhcp)# network 172.16.30.0/24
Switch(config-dhcp)# gateway 172.16.30.1
Switch(config-dhcp)# quit
Switch(config)# int eth-0-1
Switch(config-if)# ip address 172.16.30.1/24
Switch(config-if)# dhcp server enable
```

2.The DHCP-Snooping function must be enabled on the S5900 device.

```
S5900_config#ip dhcp-relay snooping
```

3.Create a vlan on the S5900 device and configure the interface link type.

```
S5900_config#vlan 2
S5900_config_vlan2#quit
S5900_config#int g0/1
S5900_config_g0/1#switchport mode access
S5900_config_g0/1#switchport pvid 2
S5900_config_g0/1#quit
S5900_config#int g0/2
S5900_config_g0/2#switchport mode access
S5900_config_g0/2#switchport pvid 2
```

4.Start the DHCP-Snooping function on the VLAN, and perform legalization check on the DHCP messages received by all untrusted physical ports belonging to the entire VLAN.

```
S5900_config#ip dhcp-relay snooping vlan 2
```

5.Enable the DHCP anti-attack function on the vlan. When the number of users in the vlan reaches the configured maximum allowable value, new clients are not allowed to allocate.

```
S5900_config#ip dhcp-relay snooping vlan 2 max-client 10
```

6.If the interface is configured as a DHCP trusted interface, the DHCP messages received by the interface will not be checked.

```
S5900_config#interface g0/1
S5900_config_g0/2#dhcp snooping trust
```

7.Configure the interface ARP detection function. For the ARP monitoring trust interface, the ARP monitoring function is not enabled. The interface defaults to an untrusted interface.

```
S5900_config#int g0/2
S5900_config_g0/2#arp inspection trust
```

8.Start the IP source address detection function on the vlan to detect the binding relationship between the MAC and the IP address.

```
S5900_config#ip verify source vlan 2
```

9.Use commands to view DHCP-Snooping configuration information.

```
S5900#show ip dhcp-relay snooping

ip dhcp-relay snooping
ip dhcp-relay snooping vlan    2
ip verify source vlan    2
ip dhcp-relay snooping vlan 2 max-client 10
DHCP Snooping trust interface:
    g0/1

ARP Inspect trust interface:
    g0/2

IP source guard trust interface:
DHCP Snooping deny interface:

ip dhcp-relay snooping db-file /dhcpr-database
```

10.At this time, start the network card on the PC to obtain the IP address automatically, for getting the IP address.

11.Use the command to view the address binding entries that take effect on the interface.

```
S5900#show    ip dhcp-relay snooping binding
Hardware Address    IP Address          Surplus Time     Type          VLAN Intf
------------------      --------------        ------------      -------         ---- --------
8c:ec:4b:ad:03:6b     172.16.30.2          86220             DHCP_SN    2       g0/2
```

6.3.12 Check the assigned IP address in DHCP-Server as follows.

```
Switch## show dhcp server binding all
 IP address          Client-ID/                  Lease expiration                      Type
                        Hardware address
 172.16.30.2         8c:ec:4b:ad:03:6b         Fri      2020.04.10 12:38:03       Dynamic
```

6.4 Root Cause

In summary, after the DHCP-Snooping function is enabled, the PC cannot obtain an IP address or obtain an illegal IP address. The reasons are as follows

1. The trusted port is not enabled on the DHCP-Server port.

2. The number of clients exceeds the maximum number of clients, and the device will not allocate new clients.

3. I use dynamic binding here. If it is static binding, the assigned IP address is not the bound IP address, and the PC cannot obtain the IP

address.

6.5 Solution

1. Configure the port connected to the switch on the DHCP-Server as a trusted port. The DHCP messages received by the untrusted interface on the interface will be checked.
2. If the terminal is a dumb terminal, the IP address is relatively fixed, it is recommended to manually configure the static binding table.
3. The IP address cannot be obtained on the PC side. It is also possible that the network server and the client are on the same network segment, and there is no DHCP relay. There should be no proxy field prompt. DHCP SNOOPING has the option option enabled by default, resulting in the failure to obtain the IP address.

6.6 Suggestions and Conclusions

When configuring the DHCP-Snooping function, when the device is connected to the correct DHCP Server, the interface must be configured as a trusted interface. Prevent illegal IP addresses from being obtained on untrusted interfaces.

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.

Copyright © 2009-2022 FS.COM All Rights Reserved.