

00

...

00

.....

....

....

0 0 0 60 0 0.0

......

.......

...

. ۲ ...

.

...

0.0

0 ...

۲ . . .

.

........

S8050-20Q4C Switch Technical White Paper

After-sale Instructions for Error-prone Issues

Model: \$8050-20Q4C

Contents

1. L/	ACP Function Configuration Failure Issue	1
	1.1 Issue Description	1
	1.2 Topology Information	1
	1.3 Handling Process	1
	1.4 Root Cause	5
	1.5 Solution	5
	1.6 Suggestions and Conclusions	5
2. M	LAG Function Configuration Failure Issue	6
	2.1 Issue Description	6
	2.2 Topology Information	6
	2.3 Handling Process	6
	2.4 Root Cause	.10
	2.5 Solution	.11
	2.6 Suggestions and Conclusions	.11
		••••
3. P	ort split Function Configuration Failure Issue	12
3. Po	2.0 Suggestions and Configuration Failure Issue	.12 .12
3. Po	2.0 Suggestions and Configuration Failure Issue	.12 .12 .12
3. P	2.0 Suggestions and Configuration Failure Issue 3.1 Issue Description 3.2 Topology information 3.3 Handling Process	12 .12 .12
3. P	2.0 Suggestions and Configuration Failure Issue	12 .12 .12 .12 .12
3. P	 2.0 Suggestions and Configuration Failure Issue	12 .12 .12 .12 .12 .16
3. P	 2.6 Suggestions and conclusions bort split Function Configuration Failure Issue	12 .12 .12 .12 .12 .16 .16
3. Po 4. V	2.0 Suggestions and Conclusions ort split Function Configuration Failure Issue 3.1 Issue Description 3.2 Topology information 3.3 Handling Process 3.4 Root Cause 3.5 Solution 3.6 Suggestion and Conclusions XLAN Function Configuration Failure Issue	12 .12 .12 .12 .12 .16 .16 .16
3. P¢ 4. V)	2.0 Suggestions and Conclusions	12 .12 .12 .12 .12 .16 .16 .16 .17
3. Po 4. V	2.0 Suggestions and conclusions	12 .12 .12 .12 .16 .16 .16 .17 .17
3. P(2.0 Suggestions and conclusions ort split Function Configuration Failure Issue 3.1 Issue Description 3.2 Topology information 3.3 Handling Process 3.4 Root Cause 3.5 Solution 3.6 Suggestion and Conclusions XLAN Function Configuration Failure Issue 4.1 Issue Description 4.3 Handling Process 4.4 Root Cause	12 .12 .12 .12 .12 .16 .16 .16 .17 .17 .21
3. P¢ 4. V	2.0 Suggestions and Configuration Failure Issue. 3.1 Issue Description. 3.2 Topology information. 3.3 Handling Process. 3.4 Root Cause. 3.5 Solution. 3.6 Suggestion and Conclusions. KLAN Function Configuration Failure Issue. 4.1 Issue Description. 4.3 Handling Process. 4.4 Root Cause. 4.5 Solution.	12 .12 .12 .12 .16 .16 .16 .17 .17 .21

FFS

5. VRRP Function Function Configuration Failure Issue	23
5.1 Issue Description	23
5.2 Topology Information	23
5.3 Handing Process	23
5.4 Root Cause	
5.5 Solution	26
5.6 Suggestion and Conclusion	26
6. ACL Function Configuration Failure Issue	27
6. ACL Function Configuration Failure Issue	27
6. ACL Function Configuration Failure Issue 6.1 Issue Description 6.2 Topology Information	27
6. ACL Function Configuration Failure Issue. 6.1 Issue Description. 6.2 Topology Information. 6.3 Handing Access.	27 27 27 27 27
6. ACL Function Configuration Failure Issue. 6.1 Issue Description. 6.2 Topology Information. 6.3 Handing Access. 6.4 Root Cause.	27 27 27 27 27 27 27 30
6. ACL Function Configuration Failure Issue. 6.1 Issue Description. 6.2 Topology Information. 6.3 Handing Access. 6.4 Root Cause. 6.5 Solution.	27 27 27 27 27 30 30

1. LACP Function Configuration Failure Issue

1.1 Issue Description

When the LINK AGGREGATION function of the S8050 series switches is configured, when the LINK AGGREGATION dynamic mo de is configured, the active interfaces selected by the devices at both ends are inconsistent, resulting in the inability to esta blish a link aggregation group.

1.2 Topology Information



1.3. Handling Process

Check the LACP status with the commands" show channel-group summary" and "show interface agg10", and find that the negotiation is not successful, the port is Down, and the aggregation port is also Down.

S8050_ES_1# chow	channel_arc							
50050-F3-1# SHOW	channel-gro	up summary						
port-channel load-	port-channel load-balance hash-arithmetic: xor							
port-channel load-	balance has	h-field-select:						
macsa								
port-channel group	o-mode: 56							
Flags: s - Suspend	k	T - Standby						
D - Down	/Admin dov	vn B - In bu	ndle					
R - Layer3	3	S - Layer2						
w - Wait		U - In use						
Mode: SLB - St	tatic load ba	lance						
DLB - D	ynamic load	l balance						
RR - Ro	ound robin l	oad balance						
RLB - Re	esilient load	balance						
Aggregator Name	Mode	Protocol	Ports					
+		+						
Agg20(SD)	SLB	LACP	eth-0-2(D)	eth-0-3(D)	eth-0-4(D)			
S8050-FS-1#S8050-	-20Q4C# sho	ow interface ag	Jg22					
Interface agg22								

Interface current state: DOWN
Hardware is AGGREGATE, address is 001e.080d.6e97 (bia 001e.080d.6e97)
Bandwidth 1000000 kbits
Index 2070 , Metric 1 , Encapsulation ARPA
Speed - 40Gb/s , Duplex - Full , Media type is Aggregation
Link type is force link
FEC config: DISABLE
FEC status: Unknown
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 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes
Received 0 unicast, 0 broadcast, 0 multicast
0 runts, 0 giants, 0 input errors, 0 CRC
0 frame, 0 overrun, 0 pause input
0 packets output, 0 bytes
Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output

Check the LACP configuration and find that the active interfaces selected by the devices at both ends of the S8050 switch are inconsistent.

S8050-FS-1 configuration commands:

port-channel load-balance hash-field-select macsa lacp system-priority 2000

interface eth-0-2 no switchport channel-group 1 mode active

interface eth-0-3 no switchport channel-group 1 mode passive

interface eth-0-4

no switchport

channel-group 1 mode active

S8050-FS-2 configuration commands:

port-channel load-balance hash-field-select macsa lacp system-priority 1000

interface eth-0-2 no switchport channel-group 1 mode active

interface eth-0-3 no switchport

channel-group 1 mode active

interface eth-0-4

no switchport

channel-group 1 mode passive

Modify the active ports at both ends, Active Member Ports: Eth/0/2, Eth/0/3, Passive Member Ports: Eth/0/4, the active and passive interfaces at both ends should be the same.

S8050-FS-1# configure terminal

S8050-FS-1(config)#int eth-0-2

S8050-FS-1(config)#no shutdown

S8050-FS-1(config)#channel-group 20 mode active

S8050-FS-1(config)#int eth-0-3

S8050-FS-1(config)#no shutdown

S8050-FS-1(config)#channel-group 20 mode active

S8050-FS-1(config)#int eth-0-4

S8050-FS-1(config)#no shutdown

S8050-FS-1(config)#channel-group 20 mode passive

S8050-FS-2# configure terminal

S8050-FS-2(config)#int eth-0-2

S8050-FS-2(config)#no shutdown

S8050-FS-2(config)#channel-group 20 mode active

S8050-FS-2(config)#int eth-0-3

S8050-FS-2(config)#no shutdown

S8050-FS-2(config)#channel-group 20 mode active

S8050-FS-2(config)#int eth-0-4

S8050-FS-2(config)#no shutdown

S8050-FS-2(config)#channel-group 20 mode passive

Check the configuration at this time, and use the show channe	l-group summary and show interface agg20 commands to see that LACP
has been negotiated successfully.	
S8050-FS-1# show interface agg20	
Interface agg20	
Interface current state: UP	
Hardware is AGGREGATE, address is 001e.080d.6d77 (bia 001e	.080d.6d77)
Bandwidth 80000000 kbits	
Index 2070 , Metric 1 , Encapsulation ARPA	
Speed - 40Gb/s , Duplex - Full , Media type is Aggregation	
Link type is force link	
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 512 bits/sec, 0 packets/sec	
5 minute output rate 129 bits/sec, 0 packets/sec	
714 packets input, 71320 bytes	
Received 0 unicast, 653 broadcast, 61 multicast	
0 runts, 0 giants, 0 input errors, 0 CRC	
0 frame, 0 overrun, 0 pause input	
79 packets output, 15276 bytes	
Transmitted 0 unicast, 16 broadcast, 63 multicast	
0 underruns, 0 output errors, 0 pause output	
S8050-FS-1# show channel-group summary	
port-channel load-balance hash-arithmetic: xor	
port-channel load-balance hash-field-select:	
macda	
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			
agg20(SU)	SLB	LACP	eth-0-2(B)	- eth-0-3(B)	eth-0-4(s)

1.4 Root Cause

In summary, when the LINK AGGREGATION dynamic function is used in the S8050 series switches, the negotiation of configuring the LINK AGGREGATION function fails because the selected active interfaces are inconsistent.

1.5 Solution

When configuring the LINK AGGREGATION dynamic function, configure the LINK AGGREGATION function according to the spec ifications. When configuring the LINK AGGREGATION dynamic function, the active interfaces selected by the devices at both e nds must be consistent, or they can be directly selected according to the LACP system priority. Active interface.

1.6 Suggestions and Conclusions

If the configuration of LINK AGGREGATION is abnormal, you should pay attention to check whether the physical line is norm al and whether the related configuration of link aggregation is correct. When configuring the LINK AGGREGATION function, pl ease refer to the relevant configuration manual for correct configuration.

2. MLAG Function Configuration Failure Issue

2.1 Issue Description

If the S8050 series switches enable the MLAG function when the spanning tree protocol is enabled, the MLAG function configuration will be abnormal.

2.2 Topology Information



2.3 Handling Process

Configure the MLAG function of S8050 two switches, create Vlan, create static AGG, configure the aggregate Peer link attribute in advance, and add the AGG port to MLAG. Unless otherwise specified, the configuration of the two S8050 devices is the same.





S8050(config-if)# switchport mode trunk S8050(config-if)# switchport trunk allowed vlan all S8050(config-if)# static-channel-group 10 S8050(config-if)# no shutdown S8050(config-if)# int eth-0-16 S8050(config-if)# switchport mode trunk S8050(config-if)# switchport trunk allowed vlan all S8050(config-if)# static-channel-group 10 S8050(config-if)# no shutdown S8050(config-if)# no shutdown

S8050(config)# int agg 10 S8050(config-if)# switchport mode trunk S8050(config-if)# switchport trunk allowed vlan all S8050-(config-if)# exit

Configure the attributes of the vlan interface of two S8050s S8050-FS-1 configuration: S8050--FS-1(config)# int vlan 4094 S8050--FS-1(config-if)# ip add 12.1.1.1/24 S8050--FS-1(config-if)# exit

S8050-FS-2 configuration: S8050--FS-2(config)# int vlan 4094 S8050--FS-2(config-if)# ip add 12.1.1.2/24 S8050--FS-2(config-if)# exit

Configure the link aggregation port of the S5080 switch.

S5080(config)# vlan database S5080(config-vlan)# vlan 10 S5080(config-vlan)# exit S5080(config)# int eth-0-1 S5080(config-if)# static-channel-group 1 S5080(config-if)# no shutdown S5080(config-if)# int eth-0-2 S5080(config-if)# static-channel-group 1 S5080(config-if)# no shutdown S5080(config-if)# no shutdown

When entering the MLAG mode of the switch, an error will be reported when configuring peer-link related attributes. Since the interface is enabled by default with spanning tree protocol, the STP function under the interface needs to be disabled S8050(config)# mlag configuration

S8050(config-mlag)# peer-link agg 10

% Interface has enabled spanning-tree

Enter the interface mode first, cancel joining the aggregation port and then close the STP function, and then add it to the aggregation port, because you cannot configure the port separately after joining the aggregation port.

S8050(config)# int eth-0-15

S8050(config-if)# spanning-tree port disable

% Can't configure on interface eth-0-15

S8050-20Q4C(config-if)# no static-channel-group

S8050(config-if)# spanning-tree port disable

S8050(config-if)# static-channel-group 10

S8050(config-if)# exit

S8050(config)# int eth-0-16

S8050(config-if)# no static-channel-group

S8050(config-if)# spanning-tree port disable

S8050(config-if)# static-channel-group 10

S8050(config-if)# exit.

Then enter the aggregation port mode, turn off the STP function.

S8050(config)# int agg 10

S8050(config-if)# spanning-tree port disable

S8050(config-if)# exit

Configure peer link related attributes S8050-FS-1 configuration: S8050-FS-1(config)# mlag configuration S8050-FS-1(config-mlag)# peer-link agg 10 S8050-FS-1(config-mlag)# peer-address 12.1.1.2 S8050-FS-1(config-mlag)# end

S8050-FS-2 configuration:

S8050-FS-2(config)# mlag configuration S8050--FS-2(config-mlag)#peer-link agg 10 S8050--FS-2(config-mlag)# peer-address 12.1.1.1

S8050--FS-2(config-mlag)# end

Verify the configuration results and view the MLAG status information on the two \$8050s.

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

S8050-FS-1# show mlag MLAG configuration:

role : Slave

local_sysid : 001e.080d.6d62 remote_sysid : 001e.080d.6e88

mlag_sysid : 001e.080d.6e88

local_syspri : 32768

remote_syspri: 32768

mlag_syspri : 32768

peer-link : agg10

peer conf : Yes

reload-delay : Auto(300s)

S8050-FS-2# show mlag

MLAG configuration:

role : Master local_sysid : 001e.080d.6e88 remote_sysid : 001e.080d.6d62 mlag_sysid : 001e.080d.6e88 local_syspri : 32768 remote_syspri : 32768 mlag_syspri : 32768 peer-link : agg10 peer conf : Yes reload-delay : Auto(300s)

View mlag interface status information

S8050#	show m	lag interface	
mlagid	local-if	local-state	remote-state
1	agg1	up	up

View the MAC table of the device:

8050-FS-1# show mac address-table						
Mac Address Table						
(*) C	A construction of the second sec		Frater			
(^) - 56	ecurity Entry (N	(I) - MLAG	Entry			
(MO) - I	MLAG Output Entry	(MI) - ML	AG Input Entry			
(E) - E'	VPN Entry	(EO) - EVPN	l Output Entry			
(EI) - EV	/PN Input Entry					
Vlan	Mac Address	Туре	Ports			
1	001e.0810.e0bd	dynamic	agg1(MI)			
1	001e.080d.6e88	static	agg10			
4094	001e.080d.6e88	static	agg10			

S8050-FS-2# show mac address-table Mac Address Table (*) - Security Entry (M) - MLAG Entry (MO) - MLAG Output Entry (MI) - MLAG Input Entry (E) - EVPN Entry (EO) - EVPN Output Entry (EI) - EVPN Input Entry Vlan Mac Address Туре Ports 001e.0810.e0bd dynamic agg1(MO) 001e.080d.6d62 static agg10 1 4094 001e.080d.6d62 static agg10

View MLAG neighbor information

S8050-FS-1# show mlag peer MLAG neighbor is 12.1.1.2, MLAG version 1 MLAG state = Established, up for 01:05:42 Last read 00:00:17, hold time is 240, keepalive interval is 60 seconds Received 8669 messages, Sent 97 messages Open : received 1, sent 1 KAlive : received 76, sent 76 Fdb sync : received 8581, sent 14 Failover : received 1, sent 1 Conf : received 1, sent 1 Syspri : received 1, sent 1 Peer fdb : received 1, sent 1 STP Total: received 7, sent 2 Global : received 3, sent 2 Packet : received 0, sent 0 Instance: received 0, sent 0 State : received 4, sent 0 Connections established 1; dropped 0 Local host: 12.1.1.1, Local port: 61001 Foreign host: 12.1.1.2, Foreign port: 61000 remote_sysid: 001e.080d.6e88

2.4 Root Cause

Due to the characteristics of S8050 series switches, spanning tree protocol and MLAG cannot be used at the same time, oth erwise it will cause abnormal MLAG function.

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 resta rted after the configuration is complete, and the forwarding decisions are all local. Normally, traffic does not need to take th e interconnection path between devices, avoiding the interconnection path Bandwidth becomes a bottleneck while reducing I atency.

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. Port Split Function Configuration Failure Issue

3.1 Issue Description

When the S8050 series switch port is split and the four-port DAC is connected to the four ports of the S5080 series switch and aggregated, the port aggregation operation cannot be performed.

3.2 Topology information



3.3 Handling Process

Check the port status of the S8050 switch, and find that the port for port aggregation with the peer switch is the Eth-0-1 port, and the S8050 switch has a feature. The four ports split by the Eth-0-1 port are the first four unique to the S8050 device. 10G ports; so the first method is to change the cable on the four 10G ports of the S8050 switch and perform port aggregation with the peer switch, and the second method is to switch to the Eth-0-2 port and the peer to perform port aggregation.

The following uses the second method as an example to split the Eth-0-2 port into 4*10G ports, save the configuration, and then restart the switch.

S8050-FS-1# configure terminal S8050-FS-1(config)# split interface eth-0-2 10giga S8050-FS-1# write Building configuration... [OK] S8050-FS-1# reboot Building configuration... Reboot system? [confirm]y

Note: After performing the port split operation, you must save the configuration and restart the switch for the configuration to take effect.

Check the port status of the S8050 and S5080 switches respectively. On the S8050 switch, some ports are down, and the po

rt status of the S5080 switch is also Err-disable.

S8050-FS-	-1# show inte	erface sta	tus			
Port	Status	Duplex	Speed	Mode	Туре	Description
eth-0-1	down	auto	auto	ACCESS	Unknown	
eth-0-2/1	up	a-full	a-10000	ACCESS	40GBASE_CR4	
eth-0-2/2	down	auto	auto	ACCESS	5 40GBASE_CR4	
eth-0-2/3	down	auto	auto	ACCESS	5 40GBASE_CR4	
eth-0-2/4	up	a-full	a-10000	ACCESS	40GBASE_CR4	
eth-0-3	down	full	40000	TRUNK	Unknown	
eth-0-4	down	full	40000	TRUNK	Unknown	
S50801# Port	show interf Status	ace status Duplex	Speed	Mode	Туре	Description
eth-0-20	down	auto	auto	ACCE	SS Unknown	
eth-0-21	down	auto	auto	ACCE	SS Unknown	
eth-0-22	down	auto	auto	ACCE	SS Unknown	
eth-0-23	down	auto	auto	ACCE	SS Unknown	
eth-0-24	down	auto	auto	ACCE	SS Unknown	
eth-0-25	errdisable	auto	auto	ACCESS	Unknown	
eth-0-26	errdisable	auto	auto	ACCESS	Unknown	
eth-0-27	up	a-full	a-10000	ACCESS	10GBASE_PASSIVE_COPPER	
eth-0-28	up	a-full	a-10000	ACCESS	10GBASE_PASSIVE_COPPER	

Check the cause and find that the S5080 switch port connected to the S8050 switch is a layer 2 port, and the layer 2 port has a loop problem, so some ports are in Errdisable state. Change the layer 2 port to a layer 3 port, and then check S8050 and S5080 The switch port status is found to be normal.

S5080-1(config)# interface eth-0-25 S5080-1(config-if)# no switchport S5080-1(config-if)# no shutdown S5080-1(config-if)#exit S5080-1(config)# interface eth-0-26 S5080-1(config-if)# no switchport S5080-1(config-if)# no shutdown S5080-1(config-if)#exit S5080-1(config)# interface eth-0-27 S5080-1(config-if)# no switchport S5080-1(config-if)# no shutdown S5080-1(config-if)# no shutdown S5080-1(config)# interface eth-0-28 S5080-1(config-if)# no switchport S5080-1(config-if)# no shutdown

S5080-1(config-if)#exit

S8050-FS-1# show interface status

Port	Status	Duplex	Speed	Mode	Туре		Description
eth-0-1	down	auto	auto	ACCESS	Unknown		
eth-0-2/1	up	a-full	a-10000	ACCESS	40GBASE_CR4		
eth-0-2/2	up	a-full	a-10000	ACCESS	40GBASE_CR4		
eth-0-2/3	up	a-full	a-10000	ACCESS	40GBASE_CR4		
eth-0-2/4	up	a-full	a-10000	ACCESS	40GBASE_CR4		
eth-0-3	down	full	40000	TRUNK	Unknown		
eth-0-4	down	full	40000	TRUNK	Unknown		
S50801#	show inter	face status	;				
Port	Status	Duplex	Speed	Mode	Туре		Description
eth-0-20	down	auto	auto	ACCE	SS Unknown		
eth-0-21	down	auto	auto	ACCE	SS Unknown		
eth-0-22	down	auto	auto	ACCE	SS Unknown		
eth-0-23	down	auto	auto	ACCE	SS Unknown		
eth-0-24	down	auto	auto	ACCE	SS Unknown		
eth-0-25	up	a-full	a-10000	ACCESS	10GBASE_PASSIV	E_COPPER	
eth-0-26	up	a-full	a-10000	ACCESS	10GBASE_PASSIV	E_COPPER	
eth-0-27	up	a-full	a-10000	ACCESS	10GBASE_PASSIV	E_COPPER	
eth-0-28	up	a-full	a-10000	ACCESS	10GBASE_PASSIV	E_COPPER	

Enter the split port of the switch to perform the aggregation operation. After the operation is complete, check the configura tion and the aggregation port is successfully established.

Note: At this time, you need to enter the split port for operation.

S8050-FS-1(config)# interface eth-0-2/?
<1-4> Sub-port number
S8050-FS-1(config)# interface eth-0-2/1
S8050-FS-1(config-if)# static-channel-group 2
S8050-FS-1(config-if)# no shut
S8050-FS-1(config-if)# int eth-0-2/2
S8050-FS-1(config-if)# static-channel-group 2
S8050-FS-1(config-if)# no shut



S8050-FS-1(config-if)# int eth-0-2/3
S8050-FS-1(config-if)# static-channel-group 2
S8050-FS-1(config-if)# no shut
S8050-FS-1(config-if)# int eth-0-2/4
S8050-FS-1(config-if)# static-channel-group 2
S8050-FS-1(config-if)# no shut
S8050-FS-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
DLD Desilient lead belance
RED - Resilient load Dialance
r_{r}
$agg_{2(30)}$ SLD Static ettr-0-2/1(b) ettr-0-2/2(b) ettr-0-2/3(b)
S5080-1# show chappel-group supmary
nort-channel load-balance bach-arithmetic: vor
nort-channel load-balance hash-field-select.
macda macsa insa inda
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
SHLB - self-healing load balance
RR - round robin load balance

Aggregator	Name	Mode	Protocol	Ports		
agg2(RU)		SLB	Static	eth-0-25(B)	eth-0-26(B)	eth-0-27(B)
				eth-0-28(B)		

3.4 Root Cause

The split operation of the Eth-0-1 port of the S8050 device is the first four 10G ports of the device, and the S5080 switch port connected to the S8050 switch is a layer 2 port, which will cause loop problems.

3.5 Solution

On the S8050 switch, change the Eth-0-2 port and the peer switch for port aggregation, or change the cable to operate the first four 10G ports of the S8050 switch and the peer switch, and modify the Layer 2 port of the peer switch to three Laye r port will perform port aggregation, and there will be no loop at this time.

3.6 Suggestion and Conclusions

After the port split operation, save the configuration and restart the switch. In addition, when configuring the port operation, the port DOWN is a relatively common problem. The troubleshooting should start with the basic configuration. When the ph ysical line is normal, check the detailed status of the port. Troubleshoot the problem.

Note:

Features of S8050 switch: The four 10G ports on the front of the S8050 device are split on the Eth-0-1 port. After the split operation on the Eth-0-1 port, the 40G port cannot be used.

4. VXLAN Function Configuration Failure Issue

4.1 Issue Description

Use distributed routing to establish a VXLAN tunnel to achieve private network communication. The VXLAN tunnel is establis hed successfully but the tenants under the private network cannot communicate.

4.2 **Topology Information**



4.3 Handling Process

The two VMs establish a vxlan tunnel through the S8050 switch. The command shows that the vxlan tunnel can be successfully established, but the tenants of the two parties cannot communicate with each other. Checking the configuration reveals that the tenant routing cannot be learned on the S8050-FS-2.

```
Check the tunnel establishment of S8050-FS-1
```

S805(8050-FS-1# show overlay						
ECMF	9 Mode	: 1	Normal				
Sourc	e VTEP	: 2.2	.2.2				
Vlan	Vni	Туре	Remote-vtep	IP-Address	Src-Address	Head-end-flooding F	rotocol
20	20000	VxLAN	1	3.3.3.3	2.2.2.2	Enable	Static

Check the tunnel establishment of S8050-FS-2: S8050-FS-2# show overlay

					-		
ECMP	Mode	: 1	lormal				
Sourc	e VTEP	: 3.3	.3.3				
Vlan	Vni	Туре	Remote-vtep	IP-Address	Src-Address	Head-end-flooding	Protocol
					-		
20	20000	VxLAN	1	2.2.2.2	3.3.3.3	Enable	Static

View the vrf routing of S8050-FS-1:

S8050-FS-1# show ip route vrf tenant1
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

View the vrf routing of S8050-FS-2:

S8050-FS-2# show ip route vrf tenant1
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
C 2.2.2.0/24 is directly connected, vlan20
C 2.2.2.222/32 is in local loopback, vlan20

First check whether the underlying network is interoperable, and it is found that the conflict between the IP address of VM2 and the loopback 0 port of S8050-FS-1 is 2.2.2.2. The underlying network cannot communicate. After changing the IP address of VM2, it is 2.2.2.4/ After 32, the tenants of the two parties still cannot communicate. At this time, the tunnels of both sides are successfully established, but neither side can learn the vrf routing situation.

VM2# ping 2.2.2.1

connect: Network is unreachable

S8050-FS-1#	show	qi	interface	brief	
500501511	511011	ı۲	miceriace	oner	

View the vrf routing of S8050-FS-1:

Interface	IP-Address	Status	Protocol
eth-0-3	9.9.9.1	up	up
vlan1	unassigned	up	up
vlan20	2.2.2.111	up	up
loopback0	2.2.2.2	up	up

S8050-FS-1# show ip route vrf tenant1
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

View the vrf routing of S8050-FS-2:

```
S8050-FS-2# show ip route vrf tenant1
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
```

Check the configuration of the VXLAN tunnel establishment of the two switches of S8050, and find that both parties specified the wrong destination address when configuring the static static route of the vxlan distributed route. The destination address refers to the IP of the VM, and the destination address is modified to S8050. loopback address.

S8050-FS-1# show running-config

Building configuration...

.

ip route 3.3.3.0/24 9.9.9.2 ip route vrf tenant1 2.2.2.2/32 remote-vtep 1 vni 20000 inner-macda 0003.0003.0003

S8050-FS-2# show running-config

Building configuration...

.

ip route 2.2.2.0/24 9.9.9.1

ip route vrf tenant1 2.2.2.1/32 remote-vtep 1 vni 20000 inner-macda 0001.0001.0001

Modify the destination address of the overlay static route to be the IP address of the switch at both ends of the tunnel instead of the VM.

S8050-FS-1# configure terminal

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

S8050-FS-1(config)# no ip route vrf tenant1 2.2.2.2/32 remote-vtep 1 vni 20000 inner-macda 0003.0003.0003 S8050-FS-1(config)# ip route vrf tenant1 3.3.3.3/32 remote-vtep 1 vni 20000 inner-macda 0003.0003.0003

S8050-FS-2# configure terminal

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

S8050-FS-2(config)# no ip route vrf tenant1 2.2.2.1/32 remote-vtep 1 vni 20000 inner-macda 0003.0003.0003

S8050-FS-2(config)# ip route vrf tenant1 2.2.2.2/32 remote-vtep 1 vni 20000 inner-macda 0003.0003.0003

At this time, check the tunnel establishment and vrf routing of both parties. The tunnel is successfully established and the v rf routing is successfully learned; the tenants of both parties can communicate through the vxlan tunnel.

S8050-FS-1# show ip route vrf tenant1 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 С 2.2.2.0/24 is directly connected, vlan20 С 2.2.2.111/32 is in local loopback, vlan20 S 3.3.3.3/32 [1/0] is in overlay remote vxlan vtep:2.2.2.2->3.3.3.3, vni:20000 S8050-FS-2# show ip route vrf tenant1 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 С 2.2.2.0/24 is directly connected, vlan20 С 2.2.2.222/32 is in local loopback, vlan20 2.2.2.2/32 [1/0] is in overlay remote vxlan vtep:3.3.3.3->2.2.2.2, vni:20000 VM-2# ping -a 2.2.2.4 2.2.2.1 PING 2.2.2.1 (2.2.2.1) from 2.2.2.4 : 56(84) bytes of data. 64 bytes from 2.2.2.1: icmp_seq=1 ttl=64 time=2.39 ms 64 bytes from 2.2.2.1: icmp_seq=2 ttl=64 time=1.90 ms 64 bytes from 2.2.2.1: icmp_seq=3 ttl=64 time=1.88 ms 64 bytes from 2.2.2.1: icmp_seq=4 ttl=64 time=1.89 ms 64 bytes from 2.2.2.1: icmp_seq=5 ttl=64 time=2.40 ms --- 2.2.2.1 ping statistics ---5 packets transmitted, 5 received, 0% packet loss, time 4004ms rtt min/avg/max/mdev = 1.888/2.096/2.404/0.251 ms

4.4 Root Cause

When configuring the network, if the network IP address conflicts, the underlying network cannot communicate. The VXLAN t unnel must be configured to ensure that the Underlay network must be interoperable. When configuring the Overlay networ k, errors in the endpoints of both ends of the Vxlan tunnel will cause the route to not be learned.

4.5 Solution

Modify the conflicting network IP address; specify the destination address when modifying the static route of the vxlan distributed routing configuration overlay, and the destination network segment and subnet mask must be consistent with the configuration under the interface.

4.6 Suggestion and Conclusion

When establishing a VXLAN tunnel, you should pay attention to the combination of the Underlay network and the Overlay n etwork. When ensuring the interconnection of the Underlay underlying network, you must also ensure that the VXLAN config uration parameters are correct. When configuring commands, you should sort out the logical thinking and then configure.

Configure the VXLAN distributed gateway in static mode, which requires a lot of manual work and has low flexibility. It is n ot suitable for large-scale networking environments. It is recommended to use BGP EVPN to deploy distributed gateways; in addition, the logical thinking should be clarified when deploying the network , Plan the network according to the configurati

on document and follow the standard steps to avoid simple errors.

5. VRRP Function Function Configuration Failure Issue

5.1 Issue Description

When VRRP technology is used to configure a redundant gateway, when the master device fails, the Backup device cannot quickly switch between the master and backup to continue to carry traffic.

5.2 Topology Information



5.3 Handing Process

In the above network, S8050-FS-1 is configured with a priority of 100 to become a master device, and S8050-FS-2 is configur ed with a priority of 90 to become a backup device. When the uplink fails, the status of the master device will be In Initiali ze state, when the link state is restored, the device will first switch back to Backup state and then wait for the preemption delay time to switch back to Master state, during which the waiting time is too long.

S8050-FS-1# sh vrrp	
vrrp session count: 1	I contraction of the second
VRID <100>	
State	: Initialize(Interface down)
Virtual IP	: 10.10.10.1(Not IP owner)
Interface	: vlan30
VMAC	: 0000.5e00.0164
VRF	: Default
Uniform-mac	:-
Advt timer	: 5 second(s)
Preempt mode	: TRUE
Conf pri	: 100 Run pri : 100
Increased pri	: 0
Master router ip	: 0.0.0



Master priority	: Unknown
Master advt timer	: Unknown
Master down timer	: Unknown
Preempt delay	: 20 second(s)
Learn master mode	e : FALSE
BFD session state	: UNSET
S8050-FS-1# con t	
Enter configuration	commands, one per line. End with CNTL/Z.
S8050-FS-1(config)#	
222222	
S8050-FS-2# sh vrrp	
vrrp session count:	1
VRID <100>	
State	: Master
Virtual IP	: 10.10.10.1(Not IP owner)
Interface	: vlan30
VMAC	: 0000.5e00.0164
VRF	: Default
Uniform-mac	:-
Advt timer	: 5 second(s)
Preempt mode	: TRUE
Conf pri	: 90 Run pri : 90
Increased pri	: 0
Master router ip	: 10.10.10.40
Master priority	: 90
Master advt timer	: 5 second(s)
Master down timer	: 16 second(s)
Preempt delay	: 0 second(s)
Learn master mode	e : FALSE
BFD session state	: UNSET
S8050-FS-2#	

In order to realize the VRRP link failure detection function, when the main link fails, the Backup device quickly switches to Master to carry traffic. When the main link recovers, the original Master device can quickly switch back to Master to carry tr affic, so the uplink monitoring interface configuration A priority-delta value, the original priority is 100, when the failure occu rs, the priority is automatically reduced to 20, when the failure is restored, the priority is restored to 100 to become the Ma ster device, operate on the S8050-FS-1S device, the configuration command is as follows:

S8050-FS-1(config)# track 10 int vlan 30 linkstate

S8050-FS-1(config-track)# exit

S8050-FS-1(config)# router vrrp 100

S8050-FS-1(config-router)# disable

S8050-FS-1(config-router)# track 10 decrement 20

S8050-FS-1(config-router)# enable

S8050-FS-1(config-router)# end

Note: When configuring VRRP, you must first disable the disable function, add the configuration command and then enable t he operation, the command will take effect.

Check the effect after the configuration: When the uplink fails, the Master device will automatically lower the priority by 20, so that the master and backup can be quickly switched.

S8050-FS-1# sh vrrp		
vrrp session count: 1	l	
VRID <100>		
State	: Master	
Virtual IP	: 10.10.10.1(Not IP owner)	
Interface	: vlan30	
VMAC	: 0000.5e00.0164	
VRF	: Default	
Uniform-mac	:-	
Advt timer	: 5 second(s)	
Preempt mode	: TRUE	
Conf pri	: 100 Run pri : 1	00
Increased pri	: 0	
Track Object	: 10	
Decre pri	: 20	
Master router ip	: 10.10.10.50	
Master priority	: 100	
Master advt timer	: 5 second(s)	
Master down timer	: 16 second(s)	
Preempt delay	: 20 second(s)	
Learn master mode	: FALSE	
BFD session state	: UNSET	
S8050-FS-1#		
S8050-FS-2# sh vrrp		
vrrp session count: 1	l	
VRID <100>		
State	: Backup	
Virtual IP	: 10.10.10.1(Not IP owner)	
Interface	: vlan30	
VMAC	: 0000.5e00.0164	
VRF	: Default	
Uniform-mac	: -	
Advt timer	: 5 second(s)	

Preempt mode	: TRUE		
Conf pri	: 90	Run pri	: 90
Increased pri	: 0		
Master router ip	: 10.10.10.50		
Master priority	: 100		
Master advt timer	: 5 second(s)		
Master down timer	: 16 second(s)		
Preempt delay	: 0 second(s)		
Learn master mode	e : FALSE		
BFD session state	: UNSET		
S8050-FS-2#			

5.4 Root Cause

When the VRRP redundant gateway is configured, the failure monitoring function is not configured, and when the network fa ils, the main and standby switching cannot be performed quickly.

5.5 Solution

Configure the VRRP master device to assume the default priority of 20, and configure the track connection monitoring functi on and application module. When the monitoring module senses the link transition and network performance changes, the tr ack status will change and notify the application at the same time. The module takes corresponding measures to avoid netw ork interruption.

5.6 Suggestion and Conclusion

When configuring a VRRP redundant gateway, pay attention to the configuration of the monitoring function to realize link fai lure monitoring and timely switch between the main and standby;

When configuring the priority of the VRRP device, the default priority of the device is 100. When configuring the priority-delt a value, it must be greater than the difference between the priority of the primary device and the backup device. The configuration of the priority-delta value will take effect.

6. ACL Function Configuration Failure Issue

6.1 Issue Description

Configure ACLs to restrict different users on the internal network from accessing the Internet. Sales departments that allow access to the

external network cannot access the external network.

6.2 Topology Information



6.3 Handing Access

Check whether the network can communicate with each other. Ping the IP address of the S5800 switch on the S8050 can be pinged, and the directly connected network segment can be pinged. On the S8050, ping 192.168.1.0 and the network segment 192.168.1.0 are both unable to ping.

```
S8050-FS-1# ping 100.100.100.3

PING 100.100.100.3 (100.100.100.3) 56(84) bytes of data.

64 bytes from 100.100.100.3: icmp_seq=1 ttl=64 time=1.66 ms

64 bytes from 100.100.100.3: icmp_seq=2 ttl=64 time=1.29 ms

64 bytes from 100.100.100.3: icmp_seq=3 ttl=64 time=1.29 ms

64 bytes from 100.100.100.3: icmp_seq=5 ttl=64 time=1.38 ms

--- 100.100.100.3 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4004ms

rtt min/avg/max/mdev = 1.288/1.385/1.667/0.150 ms

S8050-FS-1# ping 192.168.1.0

PING 192.168.1.0 (192.168.1.0) 56(84) bytes of data.

--- 192.168.1.0 ping statistics ---

5 packets transmitted, 0 received, 100% packet loss, time 4000ms
```

S8050-FS-1# ping 192.168.2.0

PING 192.168.2.0 (192.168.2.0) 56(84) bytes of data.

--- 192.168.2.0 ping statistics ---

5 packets transmitted, 0 received, 100% packet loss, time 4000ms

S8050-FS-1#

Ping 192.168.1.0 and 192.168.2.0 on the S5800 switch can be pinged, indicating that there is no problem on the PC access s ide network.

\$5800# ping 192.168.1.50 PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data. 64 bytes from 192.168.1.50: icmp_req=1 ttl=128 time=0.381 ms 64 bytes from 192.168.1.50: icmp_req=2 ttl=128 time=0.354 ms 64 bytes from 192.168.1.50: icmp_req=3 ttl=128 time=0.463 ms 64 bytes from 192.168.1.50: icmp_req=4 ttl=128 time=0.465 ms 64 bytes from 192.168.1.50: icmp_req=5 ttl=128 time=0.387 ms --- 192.168.1.50 ping statistics ---5 packets transmitted, 5 received, 0% packet loss, time 3998ms rtt min/avg/max/mdev = 0.354/0.410/0.465/0.045 ms S5800# ping 192.168.2.50 PING 192.168.2.50 (192.168.2.50) 56(84) bytes of data. From 192.168.2.1 icmp_seq=1 Destination Host Unreachable From 192.168.2.1 icmp_seq=2 Destination Host Unreachable From 192.168.2.1 icmp_seq=3 Destination Host Unreachable From 192.168.2.1 icmp_seq=4 Destination Host Unreachable From 192.168.2.1 icmp_seq=5 Destination Host Unreachable --- 192.168.2.50 ping statistics ---5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4024ms pipe 3 S5800#

Check whether the ACL rule configuration is correct: Check the configuration file of the S8050 switch, and locate the proble m in the ACL configuration rule. The 20 deny rule is in front of the 30 permit rule, so rule 30 cannot take effect. S8050-FS-1# show running-config

ip access-list ipv4
10 permit any 100.100.100.0 0.0.0.255 any
20 deny any any any
30 permit any 192.168.1.0 0.0.0.255 any



class-map match-any cmap1 match access-group ipv4

!

policy-map pmap1 class cmap1

router ospf 100 network 20.20.20.20 0.0.0.0 area 0 network 100.100.100.0 0.0.0.255 area 0 network 200.200.200.0 0.0.0.255 area 0

interface eth-0-2/1 no switchport service-policy input pmap1 ip address 100.100.100.1/24

interface eth-0-7 no switchport ip address 200.200.200.1/24

Modify the configuration: delete the ACL rule ip access-list ipv4, and reconfigure the ACL rule ip access-list ipv4, the configur ation is as follows:

S8050-FS-1# configure terminal Enter configuration commands, one per line. End with CNTL/Z. S8050-FS-1(config)# no ip access-list ipv4 S8050-FS-1(config)# ip access-list ipv4 S8050-FS-1(config-ip-acl)# permit any 100.100.100.0 0.0.0.255 any S8050-FS-1(config-ip-acl)# permit any 192.168.1.0 0.0.0.255 any S8050-FS-1(config-ip-acl)# deny any any any S8050-FS-1(config-ip-acl)# exit S8050-FS-1(config)# class-map cmap1 S8050-FS-1(config-cmap)# match access-group ipv4 S8050-FS-1(config-cmap)# exit S8050-FS-1(config)# policy-map pmap1 S8050-FS-1(config-pmap)# class cmap1 S8050-FS-1(config-pmap)# class cmap1 S8050-FS-1(config-pmap)# class cmap1 S8050-FS-1(config-if)# service-policy input pmap1 S8050-FS-1(config-if)# exit

Check the effect after configuration, the sales department can access the external network normally, and the testing departm ent restricts the access to the external network: S8050-FS-1# ping 192.168.1.55 PING 192.168.1.55 (192.168.1.55) 56(84) bytes of data. 64 bytes from 192.168.1.55: icmp_seq=1 ttl=127 time=2.79 ms 64 bytes from 192.168.1.55: icmp_seq=2 ttl=127 time=2.45 ms 64 bytes from 192.168.1.55: icmp_seq=3 ttl=127 time=2.42 ms 64 bytes from 192.168.1.55: icmp_seq=4 ttl=127 time=2.47 ms 64 bytes from 192.168.1.55: icmp_seq=5 ttl=127 time=2.45 ms --- 192.168.1.55 ping statistics ---5 packets transmitted, 5 received, 0% packet loss, time 4006ms rtt min/avg/max/mdev = 2.429/2.522/2.796/0.141 ms S8050-FS-1# ping 192.168.2.50 PING 192.168.2.50 (192.168.2.50) 56(84) bytes of data. --- 192.168.2.50 ping statistics ---5 packets transmitted, 0 received, 100% packet loss, time 3999ms

6.4 Root Cause

After the ACL access control policy takes effect due to incorrect ACL rule configuration, the internal network is denied access to the external network.

6.5 Solution

Modify the ACL configuration rules, configure the S80 switch to allow the sales department 192.168.1.0 network segment to access the external network first, deny access to all other hosts later, if the deny access rule comes first, then all other allow rules can not take effect.

6.6 Suggestion and Conclusion

When configuring ACL, you should pay attention to check the configuration rules, pay attention to the configuration effectiv order, whether the destination address of the configuration rule corresponds to the network segment to be configured.

When applying ACLs, pay attention to whether to apply policies in the traffic inbound or outbound directions. If they are co nfused, the ACL will not take effect.



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.