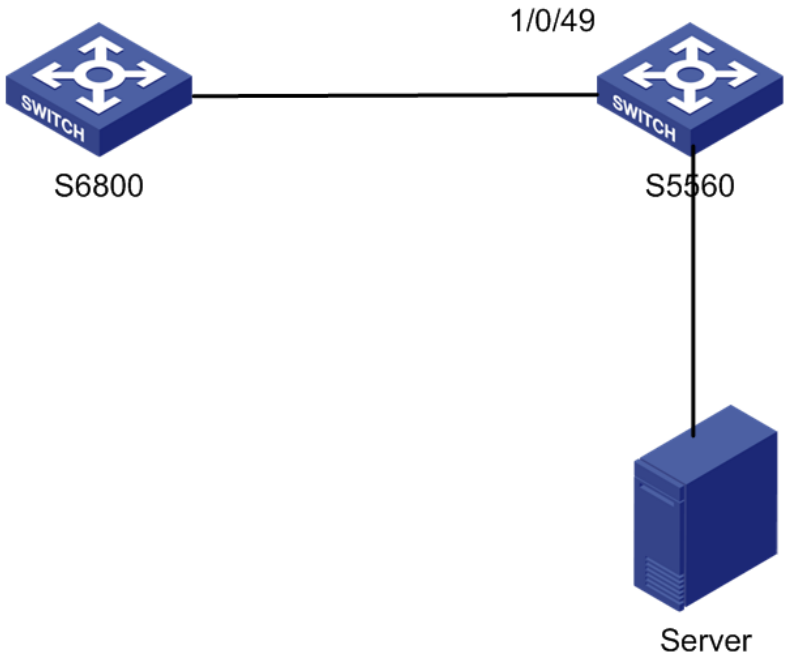
The problem that a Layer 3 routing port on a site switch can only mirror packets in one direction

Switches 周天 2020-03-21 Published

Network Topology

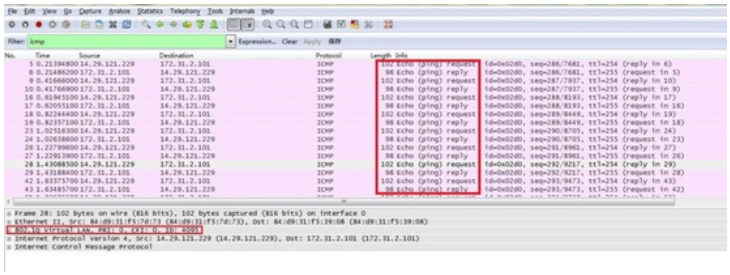
The customer topology is as follows. The customer wants to send bidirectional traffic from certain ports on the S6800 device to the server through mirroring.



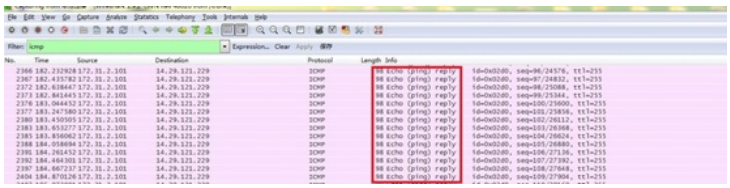
Problem Description

However, after the configuration is complete, the server can only receive inbound packets in one direction and cannot receive outbound packets.

By analyzing the configuration to see that there is no problem with the configuration on the device, the configuration on the field device is reproduced in the laboratory, and the problem on site occurs. Connect the pc directly to the outbound interface of the S6800 device, and can capture bidirectional packets on the pc. But the captured outbound packets are tagged with vlan tag 4095:



After the S5560 switch is transparently transmitted, capturing packets on the PC can only capture unidirectional packets in the inbound direction:



Process Analysis

By analyzing the configuration on the S6800 and S5560 switches, the on-site customer first mirrors the bidirectional traffic on the port of the S6800 device to the port of the S5560 device, and then transmits the mirrored data to the server by broadcasting on the mirrored VLAN on the S5560 switch.

Looking at the configuration on the two devices, the source port on the S6800 switch is a routing port and the destination port is an aggregation port. The default configuration under the aggregation port is as follows:

#
mirroring-group 1 local
#
interface Ten-GigabitEthernet1/0/48
port link-mode route
description ISP_TEL_S12510_T0/0/24_14.29.121.229_Up-Link
flow-interval 5
ip address 14.29.121.230 255.255.255.252
sflow flow collector 1
sflow sampling-rate 16000
sflow counter collector 1
sflow counter interval 60
packet-filter 3457 inbound
mirroring-group 1 mirroring-port both
#
interface Bridge-Aggregation1
description to ADS-mirror
mirroring-group 1 monitor-port
#

On the S5560, the interface connected to the S6800 is a Layer 2 interface. The port access the vlan3001, and the MAC learning function is disabled.

#
interface Ten-GigabitEthernet1/0/49 ---------- Interface connected to S6800
port link-mode bridge
port access vlan 3001
flow-interval 5
undo mac-address mac-learning enable
#
interface Ten-GigabitEthernet1/0/50 ---------- Interface connected to the server
port link-mode bridge
port access vlan 3001
stp edged-port
#

Through analysis and confirmation, after the Layer 3 routing port is enabled on the port of the switch, the underlying implementation is still implemented through the Layer 3 virtual interface (vlan 4095). When the packet is sent from the Layer 3 port, the outer 4095 label is stripped However, in the implementation of mirroring: the action of de-labeling the packets in the outbound direction of the routing port and access port is after the mirroring action, so the packets in the out direction are mirrored with the VLAN tag (4095), and the packets are mirrored to 5560 When the interface is connected, because the interface access vlan 3001, the VLAN check fails and is thrown away.

Solution

According to the above analysis, it can be seen that the outbound packet cannot be sent to the server because the packet mirrored by the Layer 3 routing port has tag4095, which causes the VLAN check on the S5560 device interface to fail and is discarded. Therefore, what needs to be resolved is to check the packets passing the outgoing direction on the S5560 interface. This can be achieved in two ways:

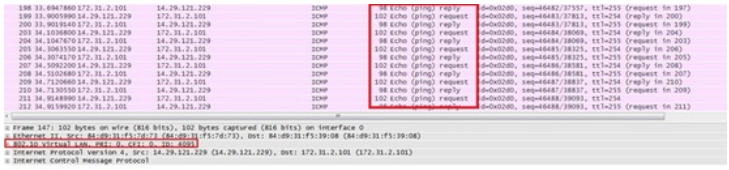
(1) Remote port mirroring on S6800

On the S6800, mirrored packets can be sent to the vlan, transparently transmitted in vlan3001, 3001 transparently transmitted on 5560, mac learning on 3001 disabled, and server interface access 3001. The implementation of this method is equivalent to tagging the packet with the outer layer 3001 on the S6800 device. When the packet enters the S5560 device interface, the outer label is already 3001, and the port can pass the packet through. Remove the outer layer 3001 label on the port connected to the server.

Two-way packets can be captured, but due to the problem of the layer 3 interface and the implementation of mirroring, the out-direction packets in the two-way packets are labeled 4095, which cannot be removed. This problem does not exist on the layer 2 port. The configuration on the 6800 is as follows. The configuration on the S5560 is unchanged.

#

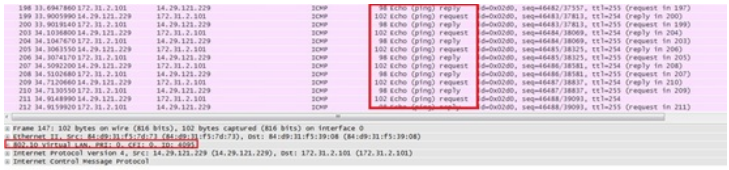
mirroring-group 1 remote-source
mirroring-group 1 remote-probe vlan 3001
#
interface Ten-GigabitEthernet3/0/16
port link-mode bridge
mirroring-group 1 reflector-port
#



(2) Implemented by the QINQ function on the S5560 switch

This method does not modify the configuration on the S6800 switch, and only enables the qinq function on the port of the S5560 switch. When a packet enters the port of the S5560 switch, qinq will first mark the outer tag 3001. Packets tagged with 3001 will be released by the port, and the outer 3001 tag will be removed from the port connected to the server. The port configuration on the S5560 switch is as follows. The configuration on the S6800 switch is not modified.

#
interface Ten-GigabitEthernet1/0/49 ---------- Interface connected to S6800
port link-mode bridge
port access vlan 3001
flow-interval 5
qinq enable
undo mac-address mac-learning enable
#



Analysis summary

The implementation of the Layer 3 routing interface on the switch is also implemented through the VLAN virtual interface (4095) at the bottom. Mirroring is implemented on the Layer 3 interface before the label is stripped, which causes this problem. Since the logical order of mirroring cannot be changed, it can be avoided by other methods.