Switch Troubleshooting Guide V1.0

Exemption Statement

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

This article provides a systematic approach to identifying and remedying problems that may arise as you use your RG-S8600E Switch over a period of time. This guide is not intended to replace configuration guide or to be an all-inclusive guide for every application. Rather, it is an attempt to provide you with the knowledge and skills necessary to correct the most common issues that you may encounter.

This article introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that may occur when you configure and use RG-S8600E serial switch.

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

- Ruijie Networks Websites : http://www.ruijienetworks.com
- Ruijie Service Portal : http://caseportal.ruijienetworks.com

Welcome to report error and give advice in any Ruijie manual to Ruijie Service Portal

Related Documents

- RG-S8600E Release Note
- RG-S8600E Hardware Installation and Reference Guide
- RG-S8600E Series Switch Configuration Guide
- RG-S8600E Series Switch RGOS Command Reference

Revision History

Date	Change contents	Reviser
2016.01	Initial publication V1.0	Amy

Contents

1. Troubleshooting high CPU&Memory

1.1 Troubleshooting high CPU utilization

1.1.1 Fault Symptom

The **show cpu** command output shows that the CPU utilization increases to 80% - 100%, which may cause slow CLI response, high ping loss or latency, and protocol flapping.

Note: If the CPU utilization is much higher than normal (for example, normal state range from 20% to 30%) but does not exceed 80% and services are not affected, check whether the CPU utilization keeps increasing. It is recommended to leave briefly increasing (for example, for 1s to 2s) unhandled. Instead, keep monitoring it.

1.1.2 Possible Causes

1) The CPU receives **a large number of** abnormal protocol packets (for example: packets with TTL value 1, ARP DoS attack packets, DHCP packets, IGMP packets,etc.).

2) **Protocol flapping frequently occurs**, such as routing protocols, Spanning Tree Protocol (STP), Virtual Router Redundancy Protocol (VRRP), and Bidirectional Forwarding Detection (BFD), and therefore the protocols need to recalculate which consumed CPU resources.

3) **A physical loop occurs.** A large number of packets are sent to the CPU of devices that do not support the CPU Protect Policy (CPP).

4) When a **process** is running, many CPU resources are consumed and cannot be released. (For example, the SNMP reads the MIB of the device, or the device prints many syslogs, or many users send requests for Web authentication simultaneously.)

5) After receiving some packets, the CPU responds with **many protocol packets**. (For example, a non-existing address in a VLAN is constantly scanned, causing the switch to send excessive ARP requests.)

1.1.3 Troubleshooting Procedure

Step 1 Check whether CPU process information is abnormal.

Step 2 Check whether CPP statistics are abnormal.

Step 3 Check whether IP scanning occurs.

Step 4 Check whether any loop occurs.

Step 5 Check whether protocol flapping occurs.

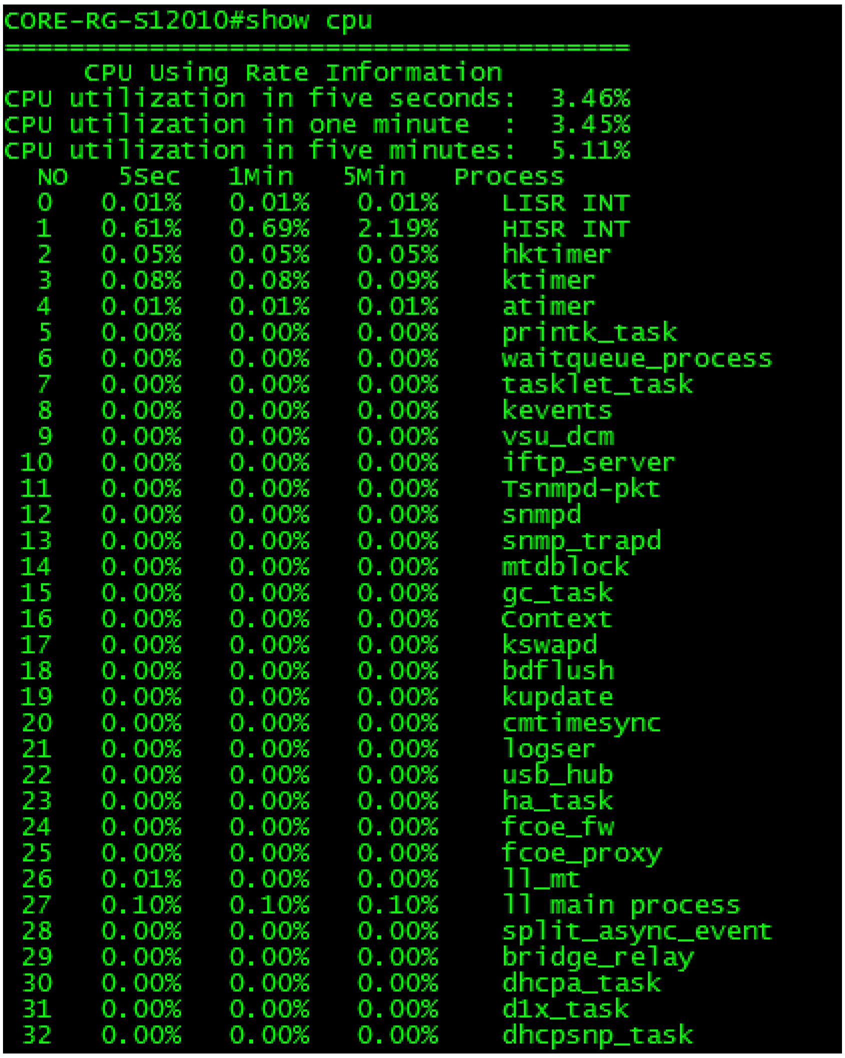
Step 6 Collect information and contact Ruijie technical support.

Step1: Check whether CPU process information is abnormal.

Display CPU process information to check whether any special process causes an increase in CPU utilization.

Procedure:

Excute the **show cpu** command for three times(every 5 seconds) to display CPU utilization.



```
CORE-RG-S12010#show cpu
=======================================
     CPU Using Rate Information
CPU utilization in five seconds:  3.46%
CPU utilization in one minute  :  3.45%
CPU utilization in five minutes:  5.11%
  NO    5Sec    1Min    5Min    Process
   0    0.01%   0.01%   0.01%     LISR INT
   1    0.61%   0.69%   2.19%     HISR INT
   2    0.05%   0.05%   0.05%     hktimer
   3    0.08%   0.08%   0.09%     ktimer
   4    0.01%   0.01%   0.01%     atimer
   5    0.00%   0.00%   0.00%     printk_task
   6    0.00%   0.00%   0.00%     waitqueue_process
   7    0.00%   0.00%   0.00%     tasklet_task
   8    0.00%   0.00%   0.00%     kevents
   9    0.00%   0.00%   0.00%     vsu_dcm
  10    0.00%   0.00%   0.00%     iftp_server
  11    0.00%   0.00%   0.00%     Tsnmpd-pkt
  12    0.00%   0.00%   0.00%     snmpd
  13    0.00%   0.00%   0.00%     snmp_trapd
  14    0.00%   0.00%   0.00%     mtdblock
  15    0.00%   0.00%   0.00%     gc_task
  16    0.00%   0.00%   0.00%     Context
  17    0.00%   0.00%   0.00%     kswapd
  18    0.00%   0.00%   0.00%     bdflush
  19    0.00%   0.00%   0.00%     kupdate
  20    0.00%   0.00%   0.00%     cmtimesync
  21    0.00%   0.00%   0.00%     logser
  22    0.00%   0.00%   0.00%     usb_hub
  23    0.00%   0.00%   0.00%     ha_task
  24    0.00%   0.00%   0.00%     fcoe_fw
  25    0.00%   0.00%   0.00%     fcoe_proxy
  26    0.01%   0.00%   0.00%     ll_mt
  27    0.10%   0.10%   0.10%     ll main process
  28    0.00%   0.00%   0.00%     split_async_event
  29    0.00%   0.00%   0.00%     bridge_relay
  30    0.00%   0.00%   0.00%     dhcpa_task
  31    0.00%   0.00%   0.00%     d1x_task
  32    0.00%   0.00%   0.00%     dhcpsnp_task
```

Check criterion:

Check whether any process occupies many CPU resources for 5 seconds in the **show cpu** command output for three consecutive times. (The CPU utilization above 20% is usually defined high.)

If you are not clear about the definition of processes with high CPU utilization, contact Ruijie technical support.

Solution:

When the CPU process is running, a large number of CPU resources are consumed and cannot be released, causing an increase in CPU utilization.

Solutions are listed as follows:

1) Temporarily disable a function (Ensure this action does not affect the services and you have confirmed with the customer): For example, if services become abnormal due to 100% CPU utilization of the Simple Network Management Protocol (SNMP) process, disable the SNMP agent; if the CPU utilization of the **rl_con** process is high, disable console logging.

2) Use the Access Control List (ACL) to filter process-related packets: For example, associate the ACL with Secure Shell (SSH) and SNMP to rectify high CPU utilization caused by abnormal SSH and SNMP packets.

3) If the CPU is high, check whether CPU Protect Policy (CPP) statistics are abnormal (CPP statistics usually change with CPU utilization). If yes, go to Step 2.

4) If the CPU utilization persists at a high level, go to Step 2.

【Additional】

Common solutions to High CPU Utilization:

Common solutions to high CPU utilization are described as follows: (Note: If you are not clear about the definition of processes with high CPU utilization, contact Ruijie technical support for more information.)

tnet/tnet6: a process for receiving IPv4/IPv6 packets. If the CPU utilization of this process is high, it is possibly because many ARP/ND packets or IPv4/IPv6 packets are sent to the CPU.

Solution: Check CPP statistics and configure the optimization policy according to Step 2.

ssp_flow_rx_task: a process for receiving data packets. If the CPU utilization of this process is high, it is mostly because many data packets are sent to the CPU. Check CPP information to obtain the information about the packets sent to the CPU.

Solution: Check CPP statistics and configure the optimization policy according to Step 2.

snmpd: SNMP process. If the CPU utilization of this process is high, it is usually because many SNMP packets are sent to the CPU or the SNMP consumes many CPU resources when obtaining a MIB node of the device.

Solution:

1) Excute **no enable service snmp-agent** command to temporarily disable the SNMP agent.

//If SNMP is disabled, the administrator may fail to manage devices. Besides, it may cause 802.1X/WEB authentication failure. Therefore, confirm with the customer before this operation.

2) Use the ACL to allow access of legal SNMP servers only.

Configure the ACL to allow access of specified SNMP servers only:

```
ip access-list standard trust-snmp

10 permit 172.18.252.0 0.0.0.255

20 permit 172.18.126.0 0.0.0.255
```

Apply the ACL to SNMP:

```
Ruijie(config)#snmp-server community ruijie rw trust-snmp
```

rl_con: a process for console logging. If the CPU utilization of this process is high, it is usually because many logs are generated.

Solution:

Run the **no logging console** command to disable the console logging.

For example：Ruijie(config)#no logging console

Or run the **logging rate-limit all 10 except emergencies** command to limit the output rate of the log.

For example：Ruijie(config)# logging rate-limit all 10 except emergencies

pimd/pim6d: a process for receiving IGMP/PIM multicast packets. If the CPU utilization of this process is high, it is usually because many unknown multicast packets are sent to the CPU.

Solution:
1) Modify the rate limits of the unknown multicast packets which send to CPU.

```
Ruijie(config)#cpu-protect type unknown-ipmc pps 30

Ruijie(config)#cpu-protect type unknown-ipmcv6 pps 30
```

2) Deploy multicast optimization policy , configure an ACL for avoiding multicast source spoofing (to filter illegal multicast packets from enduser)

There is no security policy for multicast by default. Currently, a large amount of software installed on a PC can send multicast packets, which may cause multicast packets flooding on the entire network and consume multicast resource entries and CPU resources of the switch. Therefore, deploy the multicast optimization policy on all multicast-enabled networks.

Use a specific ACL to allow only multicast packets from valid sources to valid destinations to pass through. (Apply the ACL on the Trunk port or SVI.) Whether in PIM-DM or PIM-SM mode, deploy the

ACL on the entire network.

Optimization approach (e.g., IPv4):

```
Ruijie(config)#ip access-list extended deny_mc_source
```

```
Ruijie(config-ext-nacl)#10 permit igmp any any //Allow all IGMP packets to pass through.
```

```
Ruijie(config-ext-nacl)#20 permit ip 219.229.134.0 0.0.0.255 239.202.0.0 0.0.255.255
```

//Allow multicast packets from legal sources to legal destinations to pass through. (**The legal multicast source and destination should be according to the customer's network requirement.**)

```
Ruijie(config-ext-nacl)#30 deny ip any 224.0.0.0 15.255.255.255
```

//Deny all multicast packets.

```
Ruijie(config-ext-nacl)#40 permit ip any any
```

//Allow all IPv4 packets.

To integrate the above ACL with the old ACL applied on Trunk port or SVI, add ACE 10-30 to the old ACL.

If you are not clear about ACL integration, contact Ruijie technical support for assistance.

ef_res: A process for neighbor resolution. If the CPU utilization of this process is high, it is usually because IP scanning or frequent ARP aging and deletion occurs (mostly because STP receives TC packets).

Solution: If IP scanning occurs, enable IP-guard for the switch.

Step1 Ruijie(config)#nfpp // Run the **nfpp** command to enter the NFPP configuration mode.

Step2 Ruijie(config-nfpp)#ip-guard enable // Run the **ip-guard enable** command to enable anti-scanning globally. It is enabled by default.

Step3 Ruijie#show nfpp ip-guard hosts //Run the **show nfpp ip-guard hosts** command to display the attacked hosts.

Step 4 Ruijie(config-nfpp)#ip-guard isolate-period //Run the **ip-guard isolate-period** command to isolate the attacked hosts.

Caution

NFPP-based hardware isolation is disabled by default. If it is required, confirm with the customer before enabling it in the case of IP scanning. If PCs are found as attacker will be isolated, the communication fails (for 10 minutes by default).

To troubleshoot the attack source, you need to identify the attack source port (based on the IP address/ARP/MAC address/port mappings or mirror traffic).

Approach to Identifying Attack Source:

1) Display logs to check whether the syslog contains abnormal packet sources (IP address and MAC address).

2) Obtain source addresses (IP address and MAC address) of the abnormal packets by mirroring traffic on suspicious ports. If too many packets go through the port, use flow-based mirroring or Wireshark to filter the packets.

3) Check the ARP table and MAC address table of the switch to identify the port sending the abnormal packets.

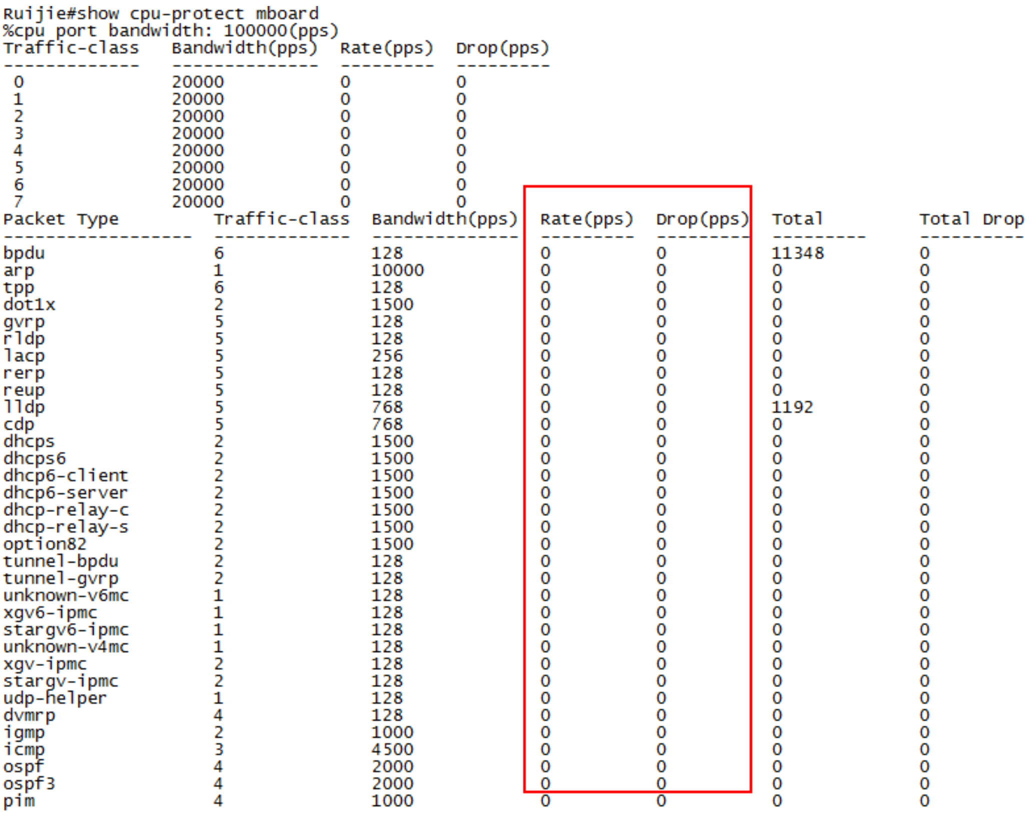
If the STP topology frequently changes, enable tc-guard or tc ignore on the port receiving TC packets and then identify the source of TC packets to rectify the fault. After the network is recovered, remove the temporary optimization configuration.

Ruijie(config-if)# spanning-tree tc-guard

Ruijie(config-if)# spanning-tree ignore tc

Step2: Check the status of protocol packets which sent to CPU

1.Run the **show cpu-protect mb** command for three to five times (every 5 seconds)

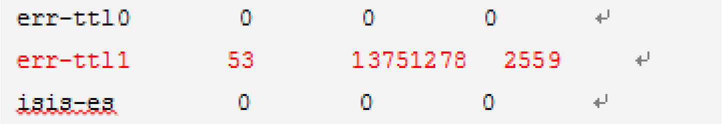


```
Ruijie#show cpu-protect mboard
%cpu port bandwidth: 100000(pps)
Traffic-class    Bandwidth(pps)  Rate(pps)  Drop(pps)
-------------    --------------  ---------  ---------
 0               20000           0          0
 1               20000           0          0
 2               20000           0          0
 3               20000           0          0
 4               20000           0          0
 5               20000           0          0
 6               20000           0          0
 7               20000           0          0
Packet Type          Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total      Total Drop
-------------------  -------------  --------------  ---------  ---------  ---------  ----------
bpdu                 6              128             0          0          11348      0
arp                  1              10000           0          0          0          0
tpp                  6              128             0          0          0          0
dot1x                2              1500            0          0          0          0
gvrp                 5              128             0          0          0          0
rldp                 5              128             0          0          0          0
lacp                 5              256             0          0          0          0
rerp                 5              128             0          0          0          0
reup                 5              128             0          0          0          0
lldp                 5              768             0          0          1192       0
cdp                  5              768             0          0          0          0
dhcps                2              1500            0          0          0          0
dhcps6               2              1500            0          0          0          0
dhcp6-client         2              1500            0          0          0          0
dhcp6-server         2              1500            0          0          0          0
dhcp-relay-c         2              1500            0          0          0          0
dhcp-relay-s         2              1500            0          0          0          0
option82             2              1500            0          0          0          0
tunnel-bpdu          2              128             0          0          0          0
tunnel-gvrp          2              128             0          0          0          0
unknown-v6mc         1              128             0          0          0          0
xgv6-ipmc            1              128             0          0          0          0
stargv6-ipmc         1              128             0          0          0          0
unknown-v4mc         1              128             0          0          0          0
xgv-ipmc             2              128             0          0          0          0
stargv-ipmc          2              128             0          0          0          0
udp-helper           1              128             0          0          0          0
dvmrp                4              128             0          0          0          0
igmp                 2              1000            0          0          0          0
icmp                 3              4500            0          0          0          0
ospf                 4              2000            0          0          0          0
ospf3                4              2000            0          0          0          0
pim                  4              1000            0          0          0          0
```

Check Standard:

1. Check whether there is any case of high packet drop with constant growth. For

example, in a fault case, the number of dropped packets with TTL value 1 keeps increasing, as shown in the following figure.



```
err-ttl0        0         0         0       ↵
err-ttl1       53         13751278  2559       ↵
isis-es         0         0         0       ↵
```

- If many types of protocol packets are dropped with an increasing rate and the RX rate (pps) is very large, it is usually because a loop occurs. Go to Step 4 to troubleshoot the fault.

- The fact that some types of protocol packets are dropped with an increasing rate proves that a large number of abnormal packets flood the network. Optimize the network according to the optimization policy in the following solution and check the result.

2. Check whether there is any case of high RX rate but less drop in the cpp statistics.

To cater to networks of different sizes, the default RX rate limit is set to an empirical value . For example, the default rate limit of unknown multicast packets is 128 pps.

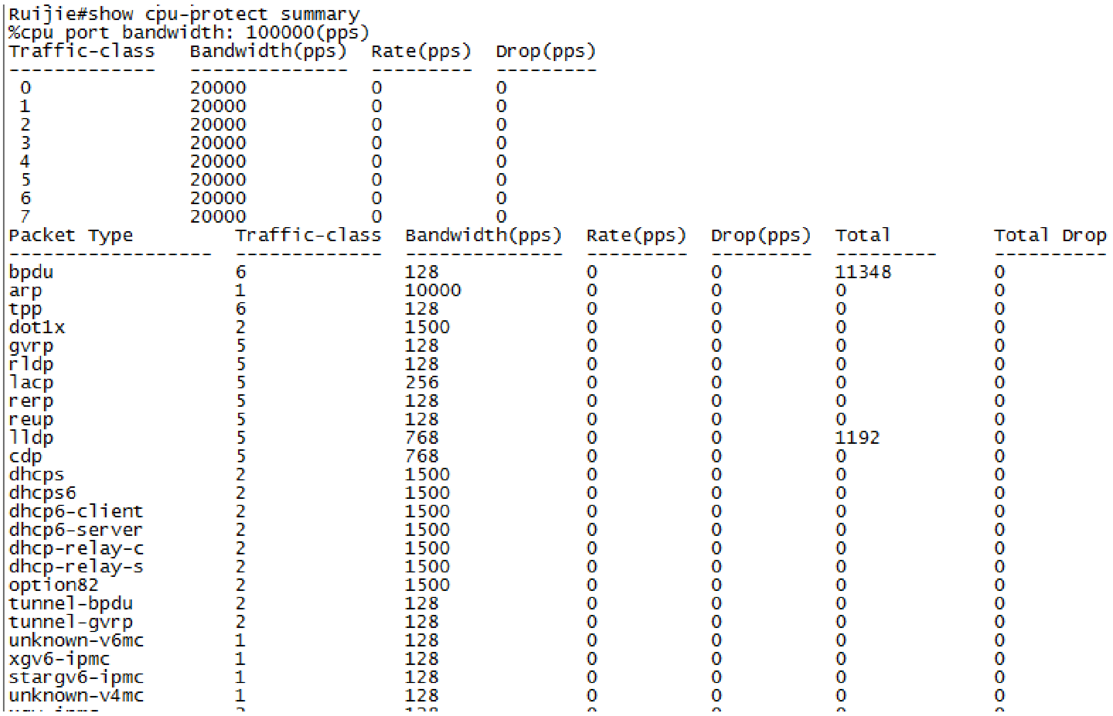
The rate of unknown multicast packets is very small (for example, 3 pps) on a healthy network. If it ranges from 30 pps to 100 pps, the CPU utilization will also increase even though no drop occurs.

- The fact that some types of protocol packets with an increasing rate proves that a large number of abnormal packets flood the network. Optimize the network according to the optimization policy in the following solution and check the result.

- If a CPU process is abnormal without CPP statistics exception (or such statistics cannot be independently analyzed), go to Step 4.3 for troubleshooting.

Notes

Run the **show cpu-protect summary** command to display the default RX rate limit of a device.



```
Ruijie#show cpu-protect summary
%cpu port bandwidth: 100000(pps)
Traffic-class     Bandwidth(pps)  Rate(pps)  Drop(pps)
-------------     --------------  ---------  ---------
 0                20000           0          0
 1                20000           0          0
 2                20000           0          0
 3                20000           0          0
 4                20000           0          0
 5                20000           0          0
 6                20000           0          0
 7                20000           0          0
Packet Type         Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total      Total Drop
------------------  -------------  --------------  ---------  ---------  ---------  ----------
bpdu                6              128             0          0          11348      0
arp                 1              10000           0          0          0          0
tpp                 6              128             0          0          0          0
dot1x               2              1500            0          0          0          0
gvrp                5              128             0          0          0          0
rldp                5              128             0          0          0          0
lacp                5              256             0          0          0          0
rerp                5              128             0          0          0          0
reup                5              128             0          0          0          0
lldp                5              768             0          0          1192       0
cdp                 5              768             0          0          0          0
dhcps               2              1500            0          0          0          0
dhcps6              2              1500            0          0          0          0
dhcp6-client        2              1500            0          0          0          0
dhcp6-server        2              1500            0          0          0          0
dhcp-relay-c        2              1500            0          0          0          0
dhcp-relay-s        2              1500            0          0          0          0
option82            2              1500            0          0          0          0
tunnel-bpdu         2              128             0          0          0          0
tunnel-gvrp         2              128             0          0          0          0
unknown-v6mc        1              128             0          0          0          0
xgv6-ipmc           1              128             0          0          0          0
stargv6-ipmc        1              128             0          0          0          0
unknown-v4mc        1              128             0          0          0          0
```

Solution:

1. Adjust the RX rate limit based on the protocol type.

If the rate limit is too small, packet exchanges will be affected. It is recommended to adjust the RX rate limit as follows:

1) First reduce the rate limit by 50%. For example, if the original default rate limit is 128 pps, it is recommended to change it to 64 pps and check for optimization. After the CPU utilization drops to below 50%, it is recommended to identify the root cause rather than adjust the rate limit again. CPP rate limiting is only a preventive measure, and the solution is to identify abnormal packet sources.

2) Some types of packets are too important to reduce the original rate limit, such as ARP packets, BPDU packets, and OSPF packets. The reason is that setting a rate limit too small may cause protocol packet drop.

Approach to Adjusting the CPP Rate Limit:

Ruijie(config)#cpu-protect type local-ipv4 bandwidth 50   //Take the command for example

If the fault persists, go to Step 3.

Common Solutions:

Common causes and solutions to high RX rate are listed as follows:

1. nd-snp-ns-na: After a switch receives routing/neighbor resolution packets from an IPv6 host, its CPU utilization is high. It is usually because a fault occurs to the host such as virus attack.

Solution: Reduce the rate limit of the preceding packets and identify the packet sources (see the following description).

For example:

```
Ruijie(config)#cpu-protect type nd bandwidth 200
```

Approach to identifying abnormal packet sources:

1) Display logs to check whether the syslog contains abnormal packet sources (IP address and MAC address).

2) Obtain source addresses (IP address and MAC address) of the abnormal packets by mirroring traffic on suspicious ports. If too many packets go through the port, use flow-based mirroring or Wireshark to filter the packets.

3) Check the ARP table and MAC address table of the switch to identify the port sending the abnormal packets.

2. unknown-ipmc/unknown-ipmcv6: After a switch receives abnormal multicast packets, its CPU utilization is high .

Solution: Reduce the rate limits of the preceding packets and configure an ACL for anti multicast source spoofing.

```
Ruijie(config)#cpu-protect type unknown-v4mc bandwidth 30

Ruijie(config)#cpu-protect type unknown-v6mc bandwidth 30
```

Configure an ACL (to filter invalid multicast packets on the PC)

There is no security policy for multicast by default. Currently, a large amount of software installed on a PC can send multicast packets, which may cause multicast floods on the entire network and consume multicast resource entries and CPU resources of the switch. Therefore, deploy the multicast optimization policy on all multicast-enabled networks.

Multicast source anti-spoofing (implementation process): Use a specific ACL to allow only multicast packets from valid sources to valid destinations to pass through. (Apply the ACL on the Trunk port or SVI.) Whether in PIM-DM or PIM-SM mode, deploy the ACL on the entire network.

Optimization approach:

```
Ruijie(config)#ip access-list extended deny_mc_source

Ruijie(config-ext-nacl)#10 permit igmp any any //Allow all IGMP packets to pass through.

Ruijie(config-ext-nacl)#20 permit ip 219.229.134.0 0.0.0.255 239.202.0.0 0.0.255.255
```

//Allow multicast packets from valid sources to valid destinations to pass through. (**Update the ARP entry according to the customer's requirement.**)

```
Ruijie(config-ext-nacl)#30 deny ip any 224.0.0.0 15.255.255.255
```

//Deny all multicast packets.

```
Ruijie(config-ext-nacl)#40 permit ip any any
```

//Allow all IPv4 packets.

To integrate the above ACL with the old ACL applied on Trunk port or SVI, add ACE 40 to the old ACL.

If you are not clear about ACL integration, contact Ruijie technical support for assistance.

3. ip4-packet-other/ip6-packet-other: IPv4 packets not specified in the CPP are usually scanning packets.

Solution: Reduce the rate limits of the preceding packets and identify the packet sources (See above).

```
Ruijie(config)#cpu-protect type ip4-packet-other bandwidth 50

Ruijie(config)#cpu-protect type ip6-packet-other bandwidth 50
```

Or configure NFPP IPv6 guard as follows:

```
Ruijie(config)#nfpp

Ruijie(config-nfpp)#define ipv6_guard

Ruijie(config-nfpp-define)#match etype 0x86dd

Ruijie(config-nfpp-define)#global-policy per-src-ip 10 20

Ruijie(config-nfpp-define)#exit

Ruijie(config-nfpp)#define ipv6_guard enable
```

Step3: Check whether IP scanning occurs.

1. Run the show arp and show arp counter commands.

```
Ruijie#show arp
  Internet   125.39.113.32     <--->      <Incomplete>     arpa     GigabitEthernet 0/22
  Internet   125.39.113.35     <--->      <Incomplete>     arpa     GigabitEthernet 0/22
  Internet   125.39.113.37     <--->      <Incomplete>     arpa     GigabitEthernet 0/22
  Internet   125.39.113.38     <--->      <Incomplete>     arpa     GigabitEthernet 0/22
  Internet   125.39.113.34     <--->      <Incomplete>     arpa     GigabitEthernet 0/22

Ruijie#show arp counter
Count of static entries:   1
Count of dynamic entries: 3486 (complete: 3607   incomplete: 221)
Total:                              3487
```

Check Criterion:

1.Check whether there are many incomplete ARP entries containing continuous IP addresses.

If yes, IP scanning occurs in the network. In this case, it is recommended to connect one trunk interface to a PC to capture packets and check whether the switch sends a large number of ARP request packets.

Solution:

If IP scanning occurs, enable IP-guard for the switch.

IP-guard is enabled by default. If it is disabled, re-enable it.

- Step1 Run the Ruijie(config)#nfpp command // enter the NFPP configuration mode.
- Step2 Run the Ruijie(config-nfpp)#ip-guard enable // enable anti-scanning globally. It is enabled by default.
- Step3 Run the Ruijie#show nfpp ip-guard hosts // display the attacked hosts.

NFPP-based hardware isolation is disabled by default. If it is required, confirm with the customer before enabling it in the case of IP scanning. If PCs are found attacked, the communication fails (for 10 minutes by default).

To troubleshoot the attack source, you need to identify the attack source port (based on the IP address/ARP/MAC address/port mappings or SPAN packet capturing).

1). Display logs to check whether the syslog contains abnormal packet sources (IP address and MAC address).

2). Obtain source addresses (IP address and MAC address) of the abnormal packets by mirroring traffic on suspicious ports. If too many packets go through the port, use flow-based mirroring or Wireshark to filter the packets.

3).Check the ARP table and MAC address table of the switch to identify the port sending the abnormal packets.

If the fault persists, go to Step 4.

Step4: Check whether any loop occurs.

Identify a loop according to the following symptoms:

1. Many interface indicators on the switch rapidly flash at the same time.

2. After connected to the switch through a Trunk port, the PC receives a large number of packets repeatedly.

3. The **show interfaces counters rate** command output shows that the traffic on the Trunk port is very high and consistent.

4. When the **show mac-address-table** command is run for three consecutive times, the MAC address may move to different ports.

Check Standard:

1. The flashing frequency of indicators is related to the transmission rate of the interface. If a loop occurs, Layer-2 ports will transmit and receive a large number of packets, and the interface indicators will rapidly flash with the same frequency.

2. A loop means that broadcast packets are flooded in a VLAN. After accessing a Trunk port, the PC receives packets from the loop. If a large number of packets are captured repeatedly, a loop must have occurred.

3. Check whether the broadcast traffic is abnormal on a port. If the broadcast traffic suddenly increases to a volume higher than the unicast traffic, a loop must have occurred.
4. Check whether the MAC address of any port frequently changes. If yes, a loop may have occurred.

Solution:

In the network environment where a loop occurs, eliminate the loop by automatically blocking loop ports through protocol (Loop avoidance) or manually disabling ports. Perform the following operations:

1. Enable loop detection on the access-layer switch.

Optional solution 1: Enable RLDP loop detection and check whether the port is automatically disabled and shut down.

```
Ruijie(config)#rldp enable    //Globally enable RLDP.

Ruijie(config-if-range)#rldp port loop-detect shutdown    //Enable rldp on the Access port.

Ruijie(config-if-range)#spanning-tree bpdufilter enable    //Enable BPDU filtering on an STP port to prevent the port from sending or receiving BPDUs.
```

Optional Solution 2: Enable PortFast and BPDU guard.

```
Ruijie(config-if-range)#spanning-tree portfast     //Enable STP loop guard on the Access port.

Ruijie(config-if-range)#spanning-tree bpduguard enable    //Enable STP loop guard on the Access port.
```

2. Enable broadcast storm control on the Access port to mitigate the broadcast storm problem caused by the loop. (Not required on the uplink port.)

```
Ruijie(config-if-range)#storm-control broadcast
```

3. Shut down or unplug cables from suspicious ports one by one to see whether the problem is solved.

If the fault persists, go to Step 5.

Step5: Check whether protocol flapping occurs.

1. Run the **show log** and **show ip ospf nei** commands to check whether the OSPF/BFD neighbor relationship is frequently down.

2. Run the **show spanning-tree summary** command (every 5 seconds) three times to check whether the topology changes frequently.

Check Standard:

1. Check whether the neighbor relationship based on a routing protocol (OSPF/BFD)

flaps up or down and whether logs similar to the following are displayed:

OSPF logs

```
*Aug  9 10:26:10: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/24, changed state to up.

*Aug  9 10:26:20: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.1-GigabitEthernet 0/24 from Down to Init, HelloReceived.

*Aug  9 10:26:50: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.1-GigabitEthernet 0/24 from Exchange to Full, ExchangeDone.

*Aug  9 10:27:44: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.1-GigabitEthernet 0/24 from Full to Init, 1-WayReceived.

*Aug  9 10:27:55: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.1-GigabitEthernet 0/24 from Exchange to Full, ExchangeDone.
```

BFD logs

```
140092: *Sep 29 19:21:23: %BFD-6-SESSION_STATE_UP: BFD session to neighbor 10.242.237.82 on interface TenGigabitEthernet 0/21 is up

140093: *Sep 29 19:21:35: %BFD-6-SESSION_STATE_DOWN: BFD session to neighbor 10.242.237.82 on interface TenGigabitEthernet 0/21 has gone down. Reason: Control Detection Time Expired
```

If there are many logs about neighbor relationship flapping, the protocol frequently goes up or down.

2. Check whether STP frequently receives topology changes. Focus on the count and duration of topology changes (information in red font).

```
Ruijie#show spanning-tree

StpVersion : MSTP <---Current STP mode

SysStpStatus : ENABLED

MaxAge : 20

HelloTime : 2

ForwardDelay : 15

BridgeMaxAge : 20

BridgeHelloTime : 2

BridgeForwardDelay : 15

MaxHops: 20

TxHoldCount : 3
```

```
###### mst 0 vlans map : ALL          <---All VLANs are mapped to Instance 0.

BridgeAddr : 001a.a915.5984           <---Local MAC address

Priority: 4096

TimeSinceTopologyChange : 0d:0h:0m:12s     //Check whether the last topology lasts for a short time.

TopologyChanges : 1182 //Check whether the count of topology changes rapidly increases.

DesignatedRoot : 1000.001a.a915.5984   <---MAC address of Root Bridge for all regions

RootCost : 0

RootPort : 0                           <---Root port selected by the local host in Instance 0. If the Root Bridge is the local host, this value is 0.

CistRegionRoot : 1000.001a.a915.5984   <---MAC addresses of the Root Bridge for Instance 0 in the local region.
```

If the topology change count rapidly increases and the last change lasts for a short time, TC packets (STP topology changes) must have been generated in the network. For details about troubleshooting, see the "Troubleshooting STP" Section

Solution:

1. If a protocol flapping occurs due to the link fault on a port, you can temporarily shut down the port or disable the dynamic routing protocol to see whether the fault is rectified. If not, troubleshoot the link fault on the port.

2. If the topology frequently changes, you can enable TC guard or TC ignorance on the port receiving TC packets and then identify the source of TC packets (described in Step4). After the network is recovered, remove the makeshift configuration.

tc-guard:

Ruijie(config-if)# spanning-tree tc-protection tc-guard //Enable TC guard on the port receiving TC packets. The port is connected to an access/convergence switch.

tc ignore:

Ruijie(config-if)# spanning-tree ignore tc (an optimization to TC guard) // Enable TC ignorance on the port receiving TC packets. The port is connected to an access/convergence switch.

3. If the fault persists, go to Step 6 to collect information and then contact Ruijie technical support for assistance.

Step6: Collect information for further analyzing

1) Collect key information about high CPU utilization.

```
show debugging

show cpu

show cpu-protect mb

show cpu-protect

show cpu

show cpu-protect mb

show cpu-protect

Ruijie#debug su

Ruijie(support)#tech-support package

exit

show cpu

show cpu-protect mb

show cpu-protect
```

----

2) Collect auxiliary information about high CPU utilization.

```
show version

show version slots

show run

show log

show ip interface brief

show interface status

show interface counter

show interfaces counters rate

show interface count summary

show interfaces counters rate

show interface count summary

show arp counter
```

show arp detail

show mac-address-table

show spanning-tree

show spanning-tree summary

show vrrp brief

show cpu-pro

show cpu-pro mb

show cpu-protect slot X //X indicates the slot number. For example, run **show cpu-pro slot 4** to display information about slot 4 on a standalone S8600E series switch; Run **show cpu-pro slot 2/4** to display information about slot 4 on chassis 2 of an S8600E Virtual Switching Unit (VSU).

show arp counter

show arp detail

show mac-address-table

3) Capture packets on the network for 2 to 3 minutes, and enable port mirroring, with the mirror source being a typical service port. (It is recommended that packets be captured every 10 seconds. If the traffic is very large, capture the packets for 1 to 2 seconds multiple times)

Configuration on switches

Ruijie(config)#monitor session 1 source interface gigabitEthernet 0/Y //gigabitEthernet 0/Y indicates a service interface. Multiple service interfaces need to be selected.

Ruijie(config)#monitor session 1 destination interface gigabitEthernet 0/X //gigabitEthernet 0/X indicates an interface connected to the PC.

☑ Gathering troubleshooting information and then submit a case in the service portal (case.ruijienetowrks.com), and contact the Ruijie Technical Assistance Center (TAC) for assistance and further instructions.

1.2 Troubleshooting for the “mstp.elf” process with very high cpu utilization

1.2.1 Fault Symptom

The Spanning Tree Protocol (STP) is disabled on a core switch. However, the **show cpu** command output shows high CPU utilization and the CPU Protect Policy (CPP) statistics show that a large number of Bridge Protocol Data Unit (BPDU) packets are sent to the

CPU.

```
Switch#show cpu
=======================================
        CPU Using Rate Information
CPU utilization in five seconds: 87%
CPU utilization in one minute   : 65%
CPU utilization in five minutes: 16%
   NO     5Sec     1Min     5Min     Process
      1     0.00%     0.00%     0.00% init
      2     0.00%     0.00%     0.00% kthreadd
      3     0.00%     0.00%     0.00% migration/0
      4     0.00%     0.00%     0.00% ksoftirqd/0
      5     0.00%     0.00%     0.00% migration/1
      6     0.00%     0.00%     0.00% ksoftirqd/1
     11     0.00%     0.00%     0.00% events/0
     12     0.00%     0.00%     0.00% events/1
     15     0.00%     0.00%     0.00% khelper
..........................................
1021       80%       60%       15%    mstp.elf
```

1.2.2 Possible Causes

1) A loop occurs on the Spanning Tree Protocol (STP) network. On the STP-enabled network, ports are not blocked due to incorrect calculation on some switches, thereby forming a loop.
2) Due to BPDU attacks by humans or other devices, the switch receives a large number of BPDU packets in a short time.
3) STP and some other security functions (such as 802.1X) are enabled on some switches but errors occur to software processing on these devices. As a result, blocked ports forward EAPOL packets, causing a loop and high CPU utilization.

1.2.3 Troubleshooting procedure

Troubleshooting Procedure
Step 1 Check the CPU utilization of the switch.
Step 2 Check parameters related to the task and timer processes.
Step 3 Check whether BPDU attacks are initiated by humans.
Step 4 Check the configurations of convergence switches connected to the core switch.

If the fault persists, collect fault information and contact Ruijie technical support for assistance.

Step1: Check CPU process information to see whether any special process causes an increase in CPU utilization.

1.Run the **show cpu** command multiple times to display the CPU utilization of the switch. If the high CPU utilization is caused by the BPDU receiving process, save the logs of the following operations.
(Note: The BPDU packets sent to an STP-disabled switch consume its CPU resources. That is, discarding excessive BPDU packets may also cause an increase in CPU utilization.)

```
Switch#sho cpu
========================================
       CPU Using Rate Information
CPU utilization in five seconds: 87%
CPU utilization in one minute   : 65%
CPU utilization in five minutes: 16%
  NO     5Sec      1Min      5Min      Process
     1    0.00%     0.00%     0.00% init
     2    0.00%     0.00%     0.00% kthreadd
     3    0.00%     0.00%     0.00% migration/0
     4    0.00%     0.00%     0.00% ksoftirqd/0
     5    0.00%     0.00%     0.00% migration/1
     6    0.00%     0.00%     0.00% ksoftirqd/1
    11    0.00%     0.00%     0.00% events/0
    12    0.00%     0.00%     0.00% events/1
    15    0.00%     0.00%     0.00% khelper
............................................
1021      80%       60%       15%    mstp.elf
............................................
```

Check Standard:
1. Check whether the CPU utilization of the mstp.elf process is high for 5 seconds in the show cpu command output for three consecutive times. (The CPU utilization above 15% is usually assumed high)
Note: The mstp.elf process is used to process STP-related events, for example, BPDU packet receiving and transmission, interface event, and state machine processing. If STP is disabled, the process may also cause high CPU utilization due to BPDU packet drop. You can run the **show cpu-protect mboard** command to check the CPU utilization of the MSTP.

2. Run the **show cpu-protect mboard** command to display the numbers of received and dropped BPDU packets.

```
Ruijie#show cpu-protect mboard
%cpu port bandwidth: 100000(pps)
Traffic-class    Bandwidth(pps)   Rate(pps)   Drop(pps)
-------------    --------------   ---------   ---------
  0                 20000             0           0
  1                 20000             0           0
  2                 20000             0           0
  3                 20000             0           0
  4                 20000             0           0
  5                 20000             0           0
  6                 20000             0           0
  7                 20000             0           0
Packet Type   Traffic-class   Bandwidth(pps)   Rate(pps)   Drop(pps)   Total    Total Drop
-----------------   -------------   --------------      ---------     ---------     ---------   ----------
bpdu              6             128               0              0          206099      101088
arp               1             10000             0              0          0           0
```

Check criterion:

If the BPDU packet drop is high, it indicates that the switch receives a large number of BPDU packets, of which some are discarded by the CPP hardware and some are discarded by the software.

If the statistics of STP-related process in the **show cpu** and **show cpu-protect mboard** command output are small, go to Step 2.

Step2: Check whether high CPU utilization is caused by man-made BPDU attacks

A core switch receives a large number of BPDU packets for either of the following reasons:
1. A large number of BPDU packets are sent due to man-made attacks or device faults.
2. BPDU packets from a large number of access switches are transparently transmitted to the core switch.
To exclude the above possibility, identify BPDU packet sources by mirroring-based packet capture:
Perform port mirroring on the Access ports of the core switch one by one, analyze the captured BPDU packets, and determine the source MAC addresses of these BPDU packets. It is recommended to identify the switches sending these abnormal BPDU packets based on the source MAC addresses and perform rate limiting on BPDU packets.
If the possibility is excluded, go to Step 3.

Step3: Check the configurations of all convergence switches connected to the core switch

1. If the possibility of man-made attacks or device faults is excluded, check the configurations of convergence switches. If convergence switches do not filter BPDU packets, BPDU packets will be transparently transmitted to the core switch, causing high CPU utilization.

1) Log in to a convergence switch connected to the core switch, and check whether BPDU filtering is enabled on the port connecting the switch to the core switch or a PC. If not, it is recommended to enable BPDU filtering on the port connecting the switch to the PC.

```
Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree bpdufilter enable
```

//Ensure that no loop occurs among the devices connected to this port.

2. Check configurations of other security functions than STP on the switch, especially security-related packets forwarding on the blocked ports. If abnormal forwarding occurs, a loop may have occurred among the devices.

1.3 Troubleshooting high memory utilization

1.3.1 Fault symptom

1) A switch works properly. However, the **show memory** command output shows that the memory utilization ranges from 80% to 90% or even higher and increases continuously. (As the available memory is decreasing, the memory utilization is increasing.)

2) If the memory utilization increases till the memory is exhausted, the following symptom appears:

When you type characters on the console port, the switch does not respond and a log indicating insufficient memory is displayed.

```
Ruijie>en
not enough memory! cli execute fail!
```

Or *Sep 6 08:54:14: %SCHED-0-NOSTACK: Could not allocate 40960 bytes for stack from memory.

Note: Some Ruijie switches have a small memory. After they are started, memory utilization ranges from 50% to 75%. When switches are running, the memory utilization may even exceed 80%. As long as the switches work properly and the memory does not increase to 90% or above sharply, no fault occurs.

Check whether the memory utilization increases continuously. If the network management software shows that the memory utilization increases sharply, a memory leak may have occurred.

1.3.2 Possible Causes

1) Due to software faults, the memory space occupied by a function cannot be released, causing rapid or slow memory leak. If a switch has been working properly for a long time but rapid memory leak occurs on it after a new function is applied, it is mostly because the new function is abnormal.

2) In the case of function changes such as the increasing of new unicast route entries and multicast entries, the memory utilization usually increase stably. You need to analyze the fault based on real network.

1.3.3 Troubleshooting procedure

Step1: Check whether the memory utilization increases continuously.

In the case of function changes such as new unicast route entries and multicast entries, the memory utilization usually increase stably. (For example, 1,000 routes occupy about 2 MB in the memory. Due to network expansion and reconstruction, the switch learns 1,000 more routes, and therefore the memory space is reduced by about 2 MB.) This is normal.

Therefore, if you doubt whether memory leak occurs, check for a continuous increase in memory utilization.

1. Run the **show memory** command every 2 seconds for three times.

2. Check whether **Used Rate** (memory utilization) increases continuously and **Current Free Memory** (available memory space in KB) decreases continuously.

For example:

```
Ruijie#show memory

System Memory Statistic:

Free pages: 2898

watermarks : min 433, lower 866, low 1299, high 1732
```

System Total Memory : 128MB, **Current Free Memory : 14580KB**

Used Rate : 89%

- If **Current Free Memory** decreases sharply (by about 2 KB each time), run the **show memory** command every 5 to 10 minutes.
- If **Current Free Memory** changes slightly, run the **show memory** command every couple of hours or every day. If it still changes slightly, run the **show memory** command every week or month.

3.

1) No fault occurs if **Current Free Memory** changes slightly in a long time.
2) If **Current Free Memory** decreases steadily (whether rapidly or slowly), run the following commands again and contact Ruijie technical support.

1) Run the **show memory** command every 5 seconds for three times.
2) Run the **show memory protocols** command every 5 seconds for three times.
3) Run the **show version**, **show version slots**, **show running**, **show interface status**, **show arp counter**, **show mac-address-table count**, **show ip route**, **show vlan**, **show log** commands once to collect regular information.

Notes

If the memory utilization exceeds 90% and continues to increase, you can negotiate with the customer on the time to restart the switch to minimize the effect on the customer's services. After the switch is restarted, collect information according to Step 3 and contact Ruijie technical support.

Step2: Check whether the memory is exhausted

1.Log in to the switch and obtain the memory information (using either of the following methods).

- Connect to the switch through the console port and type characters to see whether input is echoed on the SecureCRT or Hyper Terminal. If yes, log in to the switch and run the **show memory** command twice.
- Remotely log in to the switch through Telnet or SSH and run the **show memory** command twice.

2. Check the memory utilization of the switch.

- If the switch displays either of the following logs, a severe memory leak has occurred and the system cannot allocate memory properly. In this case, the switch fails to work and services are interrupted.

```
log1:not enough memory! cli execute fail!

log2:*Sep   6 08:54:14: %SCHED-0-NOSTACK: Could not allocate 40960 bytes
        for stack from memory.
```

In this case, go to Step 3 to collect information and recover services in emergency.

- If the **show memory** command displays an output as follows, it indicates that there is enough available memory for normal operation of the system.

  For example:

```
Ruijie#show memory

System Memory Statistic:

Free pages: 2898

watermarks : min 433, lower 866, low 1299, high 1732

System Total Memory : 128MB, Current Free Memory : 14580KB

Used Rate : 89%
```

If the memory utilization is high (over 70% for example) but the switch works properly, or the memory utilization is low (below 70% for example) but you are concerned about faults, go to step3 to collect information.

Step3: Collect information and recover services in emergency

⚠ Caution

1) Risks: Collection poses high risks. Due to high priority and frequent interruption, collection may affect customer service, or even interrupt the customer's network (in this case, you need to restart the switch to recover services).

⚠ Caution

2) If the switches work as a VSU group, collect information on each standby device (see the "Note" above), (If there are more than three VSU members, collect information on any three members.)

⚠ Caution

3) Enter @@@@C on the standby device to enable console printing.

Notes

- Collect information as follows if the customer wants to restart the switch for service recovery immediately but the switch cannot be managed through console, telnet or SSH.
- If the customer agrees to collect information after being informed of the risks, you can restart the switch.
- Information collection must be complete within the downtime of the customer's services. If not, you should restart the switch as well.
- Before restarting the switch, confirm with the customer on the restart time so that the customer can be well prepared.

1. Connect to the faulty switch through the console port.

Run the following commands in sequence. If the customer wants to recover services, restart the switch whether the collection is complete or not. (4Esc indicates pressing the Esc button for four times.)

4Esc + d : debug_show_all_locks

4Esc + c : open and close console

4Esc + f : dump tech-support info

4Esc + h : help

4Esc + i : dump cli debug info

4Esc + j : dump irq info

4Esc + k + pid + # : kill pid proc

4Esc + l : dump start process

4Esc + m : dump mem info

4Esc + n : start hrtimer

4Esc + o : stop hrtimer

4Esc + p : close logging message(same as: no logging on)

4Esc + q : dump context switches and runtime

4Esc + r : dump other cpu dump_stack

4Esc + s : show 5@ info

4Esc + t : show task states

4Esc + x : start dot task

4Esc + y : stop dot task

2. If the switches work as a VSU group, collect information on each standby device: (If there are more than three VSU members, collect information on any three members.)

Enter @@@@C on the standby device to enable console printing.

Ruijie#debug su

Ruijie(support)#tech-support package

Notes

- If console printing fails while no fault occurs to console cable connection, contact Ruijie technical support.
- Ensure that the **show** command outputs are automatically logged in the SecureCRT (See the "8.1.1 Configure SecureCRT automatic logging" section)

3. After information collection is complete, power off and restart the switch based on the customer's demand. When the device is restarted, the console cable should be connected to the device. Observe the logs on the device and ensure that the device is restarted properly.

4. After the device is properly restarted, run the following commands to collect information and report the information to Ruijie technical support for analysis. You can rapidly identify the fault by comparing the information collected during proper running of the switch with that collected in emergency during failure of the switch.

1) Run the **show memory** command every 5 seconds for three times.
2) Run the **show memory protocols** command every 5 seconds for three times.
3) Run the **show version**, **show version slots**, **show running**, **show interface status**, **show arp counter**, **show mac-address-table count**, **show ip route**, **show vlan**, **show log** commands once to collect regular information.

Perform the preceding steps to collect information, and contact Ruijie technical support for assistance.

1.4 Troubleshooting the device abnormal restarted

1.4.1 Fault symptom

The switch or line card is abnormally restarted.

1.4.2 Possible causes

1) Power supply system fault
2) Software defect
3) Hardware fault

1.4.3 Troubleshooting procedure

Step1: Check the environment of the switch

1) Check whether the power cable is inserted tightly. If the power cable is loose, the power supply may be unstable and the switch may be abnormally restarted. If possible, take pictures of the power supply and socket.

For example:

Run the **show log** command to check whether the following information is displayed:

"The power not enough, current system is in danger."

Check whether the input power is sufficient.

2) Check whether the input power matches the rated input power. If the switch is a chassis device with dual power supplies, connect the cables to sockets based on the cable type to prevent insufficient input for the single system.

Step2: Check whether the device has been manually restarted.

Run the **show log** command to check whether the device has been manually restarted.

2. Troubleshooting STP

2.1 Troubleshooting Forwarding Loops

2.1.1 Fault Symptom

In a Spanning Tree Protocol (STP)-enabled network with dual core switches, a loop occurs in the originally stable network. It is observed that the port status LEDs keep blinking at the same frequency. Run the **show interface counters** command on interconnected interfaces. It is shown that the counters are very large, most of which are of increased broadcast packets.

2.1.2 Possible Causes

1) STP is not configured on certain switches, which causes errors in STP algorithm.

2) STP standards run on switches are incompatible, which causes troubles in STP.

3) The BPDU filter is incorrectly configured on switches, which causes STP packets to be filtered out.

4) Errors occur when switches process BPDU packets, which causes the failure of forwarding BPDU packets.

2.1.3 Troubleshooting Procedure

Overview：

Step 1: Check the STP configuration of the switches.

Step 2: Check the STP compatibility between the switches.

Step 3: Check the STP configuration of the interfaces.

Step 4: Check the transmission of BPDU packets by the switches.

Step 5: Collect fault information and submit cases to Ruijie Service Portal.

Step1: Check the STP configuration of the switches

1. Certain switches do not support STP or cannot forward BPDU packets when not enabled with STP. Check whether the switches involved in STP are enabled with STP (including

whether the devices are configured with the same STP mode, such as STP/MSTP/RSTP) and can normally process BPDU packets. Check whether all related devices are enabled with STP.

Verification:

```
Ruijie(config)#show spanning-tree
StpVersion : MSTP
SysStpStatus : ENABLED
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops: 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : Disabled
BPDUFilter : Disabled
LoopGuardDef    : Disabled

###### mst 0 vlans map : ALL

BridgeAddr : 001a.a916.11b6
Priority: 32768
TimeSinceTopologyChange : 0d:0h:5m:26s
TopologyChanges : 0
DesignatedRoot : 32768.001a.a916.11b6
RootCost : 0
RootPort : 0
CistRegionRoot : 32768.001a.a916.11b6
CistPathCost : 0
```

2. If a switch does not support STP, check whether the switch transparently transmits BPDU packets. Conduct experiment if necessary.

Step2: Check the STP compatibility between the switches

If some of the switches in a network run non-standard STP, you need to check whether the local loop is caused by STP incompatibility. Based on the network deployment, check the status of STP and the STP-enabled interfaces. Ensure that the blocking and forwarding of STP between switches is compliant with the deployment requirements, so as to avoid the discarding of BPDU packets due to the local loop.

Run the **show spanning-tree**, **show spanning-tree summary** and **show spanning interface xx** commands to check the roles of the switches and interfaces in STP. Run the following commands to display the information:

1. show spanning-tree interface

```
ruijie#show spanning-tree

StpVersion : MSTP                    <---Current STP mode

SysStpStatus : ENABLED

MaxAge : 20

HelloTime : 2

ForwardDelay : 15

BridgeMaxAge : 20

BridgeHelloTime : 2

BridgeForwardDelay : 15

MaxHops: 20

TxHoldCount : 3

PathCostMethod : Long

BPDUGuard : Disabled

BPDUFilter : Disabled

###### mst 0 vlans map : 1, 3-4094             <----VLAN 1, 3 to 4094 are associated with Instance0.

BridgeAddr : 00d0.f822.3caa                    <-------MAC address of the local switch.

Priority: 32768

TimeSinceTopologyChange : 0d:3h:43m:21s

TopologyChanges : 3

DesignatedRoot : 8000.00d0.f822.3caa     <---MAC address of the root bridge in all domains, so-called the CIST (Common and Internal Spanning Tree)root

RootCost : 0

RootPort : 0          <----RP selected in Instance0 of the local switch. If the root bridge is the local switch, this value is 0.

CistRegionRoot : 8000.00d0.f822.3caa      <-----MAC address of the root bridge of instance0 in this domain.

CistPathCost : 0

###### mst 1 vlans map : 2

BridgeAddr : 00d0.f822.3caa                 <------MAC address of the local switch
```

Priority: 0

TimeSinceTopologyChange : 0d:3h:42m:40s

TopologyChanges : 3

DesignatedRoot : 0001.00d0.f822.3caa <-----MAC address of the root bridge selected by Instance1.

RootCost : 0

RootPort : 0 <-----RP selected by of the Local switch in Instance1. If the root bridge is the local switch, this value is 0.

Note: Instance 0 and other instances are different. Instance 0 plays a unique role in MSTP, which is involved in the topological calculation of both this domain and the entire switching network.

2. show spanning-tree interface

ruijie#sh spanning-tree int gi 0/24

PortAdminPortFast : Disabled

PortOperPortFast : Disabled

PortAdminLinkType : auto

PortOperLinkType : point-to-point

PortBPDUGuard : disable

PortBPDUFilter : disable

###### MST 0 vlans mapped :1, 3-4094

PortState : forwarding <----Forwarding state of the current interface in Instance0.

PortPriority : 128

PortDesignatedRoot : 8000.00d0.f822.3caa <----General root bridge (not a domain root bridge) of Instance0 learned by this interface.

PortDesignatedCost : 0

PortDesignatedBridge :8000.00d0.f822.3caa <---Bridge ID. If this interface is a DR, the value is the bridge ID of this interface. If this interface is RP, Alternate, or Backup, this value indicates the bridge ID of the uplink bridge in this instance.

PortDesignatedPort : 8018 <---Interface ID. If the interface is a DP, the value is the ID of this interface. If the interface is RP, Alternate, or Backup, this value indicates the bridge ID of the uplink interface in this instance.

This value consists of 16 bits; of which the first four bits indicate the priority 16 of the uplink interface and the last 12 bits indicate the index of the uplink interface. They are in the hexadecimal format. Run the **show interface** command to display the index of an interface. In the example, this value indicates that the priority of the uplink interface is 128 (decimal) and the index of the uplink interface is 24

```
(decimal).
PortForwardTransitions : 2
PortAdminPathCost : 200000
PortOperPathCost : 200000
PortRole : designatedPort   <-------Role of this interface in instance0.


###### MST 1 vlans mapped :2
PortState : forwarding   <--------Forwarding state of this interface in Instance1.
PortPriority : 128
PortDesignatedRoot : 0001.00d0.f822.3caa   <--------Root bridge (regional root) of this interface learned in Instance1.
PortDesignatedCost : 0
PortDesignatedBridge :0001.00d0.f822.3caa      <--------Uplink bridge ID.
PortDesignatedPort : 8018
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
PortRole : designatedPort     <------Role of this interface inInstance1.
```

Step3: Check the STP configuration of the interfaces.

1. Interfaces involved in STP must be enabled with it; otherwise, a loop cannot be blocked.

2. If the loop occurs in the access switches, check whether the BPDU filter is enabled. Run the **show interface counter** command to display the traffic passing through an interface:

```
Ruijie#show interface counter       //Check whether the input or output traffic is heavy on the interface and most increased packets are broadcast packets.
```

```
Ruijie#show running-config interface xx
```

3. If BPDU filter is configured, you need to disable the BPDU function on this interface. The command for disabling the BPDU filter is as follows:

Use the fa 0/1 interface for example:

```
Ruijie(config)#int f0/1
Ruijie(config-FastEthernet 0/1)#spanning-tree bpdufilter disabled
```

4. Check whether related switches can identify or normally forward BPDU packets. If you cannot confirm it, perform offline experiment for verification. If the fault is caused by STP incompatibility, you can modify the configuration or replace switches.

Step4: Check the transmission of BPDU packets by the switches.

1. If switches involved in STP cannot receive and send BPDU packets normally, STA errors may occur. This will cause a temporary loop which may deteriorate the network environment. There are various possible causes. One cause is that BPDU packets are discarded because excessive packets are sent to the CPU and BPDU packets have a lower priority in the CPP queue. The debugging command can be used for troubleshooting.

2. Check whether timeout occurs in BPDU packet transmission on an interface by enabling debugging.

Run the **debug mstp rx** command to check information including whether a non-root bridge receives BPDU packets normally from the RP, whether the packets are legitimate, and whether other interfaces receive BPDU packets.

Check whether the peer switch regularly sends BPDU packets. Run the **debug mstp tx** command to check the time when the local switch sends BPDU packets, and the source interface sending the packets.

3. If the root bridge does not receive BPDU packets regularly, the fault may be caused by timeout of BPDU packets. In this case, check whether the CPU usage of all switches involved in STP is too high. Being attacked by massive packets may cause high CPU usages and then abnormal packet reception and sending. You can run the following commands to display the BPDU packets in the CPP queue to check whether the CPU usage is too high and whether the CPU has Drop packets with the BPDU attribute.

```
Ruijie#show cpu
```

```
Ruijie#show cpu-protect mboard
```

4. High CPU usage may lead to the loss of BPDU packets. Check whether the high CPU usage is in normal range. If it is normal, adjust the priority of BPDU packets and the BPDU bandwidth value in the CPP queue on the switch. The commands are as follows:

```
ruijie(config)#cpu-protect type bpdu pps 400
```

```
ruijie(config)#cpu-protect type bpdu pri 7
```

⚠ Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time..

Step5:Collect fault information and submit cases to Ruijie Service Portal.

If the fault is not rectified through the preceding steps, collect the following information together with the analysis information obtained in steps 1 to 4. Submit cases to Ruijie Service Portal for further support.

Collect the network topology information on all STP-enabled devices.

```
show runnig-config

show spanning-tree

show spanning-tree summary

show spanning-tress interface xx (Switch interface)

show version

show version slot    //Chassis switch slot
```

2.2 Troubleshooting Excessive Topology Changes Causing Flooding

2.2.1 Fault symptom

In an STP-enabled network with dual core switches, the originally stable network becomes unstable. The Console prints the log "topochange:topology is changed" regularly. The network traffic is unstable and intermittent.

2.2.2 Possible causes

1). The core switches encounter STP protocol flapping, causing the STP topology continually changes.

2). Certain switches in the STP network malfunction due to hardware faults or cabling problems, causing the constant change of interface status

3). Interfaces on certain switches in the STP network experience frequent role change.

4). The core switches receive TC packets.

2.2.3 Troubleshooting Procedure

Before you start to troubleshoot, you must obtain this information:

- An actual topology diagram that details all of the switches and bridges
- Their corresponding (interconnecting) port numbers
- STP configuration details, such as which switch is the root and backup root, which links have a non-default cost or priority, and the location of blocking ports

Generally, troubleshooting involves these steps (depending on the situation, some steps may not be necessary):

Step 1: Check whether the core switches encounter STP protocol flapping.
Step 2: Check whether the switch interface status changes.
Step 3: Check whether the switch roles change.
Step 4: Check whether the core switches receive TC packets.
Step 5: Collect fault information and submit cases to Ruijie Service Portal.

Step1: Check whether the core switches continuously encounter STP protocol flapping.

STP flapping usually has the largest impact on core switches. Therefore, check the core switches first. Perform the following operations on the core gateway:

Run the **show spanning-tree** command to check whether the switches continuously encounter STP protocol flapping.

```
Ruijie#show spanning-tree

StpVersion : MSTP

SysStpStatus : ENABLED

MaxAge : 20

HelloTime : 2

ForwardDelay : 15

BridgeMaxAge : 20

BridgeHelloTime : 2

BridgeForwardDelay : 15

MaxHops: 20

TxHoldCount : 3

PathCostMethod : Long
```

```
BPDUGuard : Disabled

BPDUFilter : Disabled

###### mst 0 vlans map : 1, 3-4094

BridgeAddr : 00d0.f822.3caa

Priority: 32768

TimeSinceTopologyChange : 0d:3h:43m:21s

TopologyChanges : 3

DesignatedRoot : 8000.00d0.f822.3caa

RootCost : 0

RootPort : 0

CistRegionRoot : 8000.00d0.f822.3caa

CistPathCost : 0
```

If the value of TopologyChanges continuously increases, it indicates that the topology flaps more and more frequently. When the topology change occurs on the local switch or other switches in the network, the MAC address table of the local switch will be cleared.

Common causes are as follows: Switch interfaces undergo status change between Up and Down, role change such as from RP to Alternate, and receive TCN packets or TC BPDU packets from other switches.

Note: Clearing MAC address tables of layer-2 switches has no impact on users' communication, because unknown unicast packets are flooded as broadcast within a VLAN after the clearance of MAC address tables. However, it will burden the CPU because the switches must re-learn the MAC addresses. Clearing MAC addresses of layer-3 switches may interrupt the layer-3 forwarding for 2 to 10 seconds (because the layer-3 forwarding function needs to delay ARP learning) and bring massive MAC address learning (because layer-3 switches are often used as gateways which learn many MAC addresses). Frequent clearing of MAC address tables will severely interrupt users' communication, especially the streams forwarded by the layer-3 switches.

2. Run the **show log** command to check whether the "topochange:topology is changed" log exists. If yes, it indicates that STP flaps as the local topology changes. If not, the topology change may be caused by TC packets.

&Note: The meaning of "topochange:topology is changed" is that the current switch topology changes.

To simplify, port roles change, for example, changing from Disabled to DR, or from Alternate to DR. Possible causes for the topology changes are as follows: An interface changes from the forwarding state to the discarding state (forwarding->discarding), or from the discarding state to the forwarding state (discarding->forwarding). There are two possibilities for displaying this information: One is that the link status of certain interface changes. The information will be displayed when the interface goes up or down. The other one is that no interface link status changes but STP Algorithm changes the roles of certain interfaces, for example changing from RP to Alternate.

Step2: Check whether the switch interface status changes.

TC should be a rare event in a well-configured network. When a link on a switch port goes up or down, there is eventually a TC, once the STP state of the port is changing to or from forwarding. When the port is flapping, this would cause repetitive TCs and flooding.

1. Check whether the status of interfaces on the core switches frequently change (port goes up or down) and whether the interfaces are directly connected to PCs or single-link switches. If yes, configure the BPDU filter or Portfast on the switches to rectify the fault for normal status change. Ports with the STP portfast feature enabled will not cause TCs when going to or from the forwarding state. The configuration of portfast on all end-device ports (such as printers, PCs, and servers) should limit TCs to a low amount and is highly recommended.

2. Troubleshoot links frequently go up or down with other cause, include bad transceivers or Gigabit Interface Converters (GBICs), cabling issues, or hardware failures on the port, the linecard, or the Supervisor engine).

Step3: Check whether the switch roles change.

1. Check whether the switch roles frequently change. Run the **show spanning-tree interface vid** command.

The following information is displayed by using the **show spanning-tree interface** command onGi0/24 for example:

```
Switch#show spanning-tree int gi 0/24

PortAdminPortFast : Disabled

PortOperPortFast : Disabled

PortAdminLinkType : auto

PortOperLinkType : point-to-point    <-----p2p indicates full duplex whereas shared indicates half duplex.

PortBPDUGuard : disable

PortBPDUFilter : disable
```

###### MST 0 vlans mapped :1, 3-4094

PortState : forwarding <----Forwarding state of the current interface in Instance 0.

PortPriority : 128

PortDesignatedRoot : 8000.00d0.f822.3caa <----General root bridge (not a domain root bridge) learned by this interface in Instance 0.

PortDesignatedCost : 0

PortDesignatedBridge :8000.00d0.f822.3caa <----Uplink bridge of this interface in Instance 0.

PortDesignatedPort : 8018: The ID of the uplink interface of this interface in Instance0. This value consists of 16 bits; of which the first four bits indicate the priority 16 of the uplink interface and the last 12 bits indicate the index of the uplink interface. They are in the hexadecimal format. Use the **show interface** command to display the index of an interface. In the example, this value indicates that the priority of the uplink interface is 128 (decimal) and the index of the interface is 24 (decimal).

PortForwardTransitions : 2

PortAdminPathCost : 200000

PortOperPathCost : 200000

PortRole: designatedPort----→ Role of this interface in instance0.

###### MST 1 vlans mapped :2

PortState: forwarding: Forwarding state of this interface inInstance1.

PortPriority : 128

PortDesignatedRoot: 0001.00d0.f822.3caa ----→Root bridge of this interface in Instance1.

PortDesignatedCost : 0

PortDesignatedBridge :0001.00d0.f822.3caa ---→ Uplink root bridge of this interface in Instance1.

PortDesignatedPort : 8018

PortForwardTransitions : 1

PortAdminPathCost : 200000

PortOperPathCost : 200000

PortRole: designatedPort----→Role of this port in instance1.

2. If interface roles change frequently, it is recommended that you run the **debug mstp**

topology command to enable debugging and collect related information for analysis and further fault locating.

Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time..

Debug mstp topochange:

Debug information about MSTP topology changes. Use the debugging command to trace MSTP topology changes on the current switch. Traceable topology changes include role and forwarding state changes of interface, MAC address table clearance, instance changes, and the interfaces that receive TC BPDU packets.

For example, connect a PC directly to the Gi0/24 interface of a switch that is enabled with MSTP. When the **debug mstp topochange** command is executed, the following information is displayed:

```
1:14:58:56 S2924G: %7:mstp topo:GigabitEthernet 0/24   select role DesignatedPort in msti 0! <-----
This interface is selected as the DPin Instance0.
1:14:58:56 S2924G:%7:mstp topo:ssp port state notify.set port GigabitEthernet 0/24 state 2,mstid 0   <--
---Set the forwarding state of the interface in Instance0 to 2, which indicates the learning state.
1:14:58:56 S2924G:%7:mstp topo:ssp port state notify.set port GigabitEthernet 0/24 state 2,mstid 1   <--
----The forwarding state of this interface in Instance1 is learning.
1:14:59:11 S2924G:%7:mstp topo:port[GigabitEthernet 0/24] change state discarding to forwarding   <--
---This interface enters the forwarding state.
1:14:59:11 S2924G:%7:mstp topo:ssp port state notify.set port GigabitEthernet 0/24 state 3,mstid 0   <--
---3 indicates the forwarding state.
1:14:59:11 S2924G: %7:mstp topo:port[GigabitEthernet 0/24] change state discarding to forwarding
1:14:59:11 S2924G: %7:mstp topo:ssp port state notify.set port GigabitEthernet 0/24 state 3,mstid 1
1:14:59:12 S2924G: %7:2007-1-12 10:28:40 topochange:topology is changed   <-----Topology changes
are displayed here.
```

Step4: Check whether the core switches receive TC packets.

1. Check whether the network flapping on core switches is due to TC BPDU packets received from other switches. If the flapping occurs not on the local switch, the TC BPDU packets received are the fuse. There are two solutions to this case:

Perform interface mirroring on all access interfaces of the core switches one by one to check which of them receive TC BPDU packets.

Run the **debug mstp topology** command to check which interfaces receive TC BPDU packets in the debugging information.

3. By port mirroring or the **debug mstp topology** command, if the TC BPDU packet are confirmed from non-core switches, track the involved interfaces on these switches further. Repeat the methods (steps 1 to 4) to locate the source interfaces. Then, enable the BPDU filter on the STP-enabled switches or troubleshoot link faults.

⚠ Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time..

Step5: Collect fault information and submit cases to Ruijie Service Portal.

If the fault is not rectified through the preceding steps, collect the following information and the analysis information obtained in steps 1 to 4. Submit cases to Ruijie Service Portal for further handling.

Collect the network topology information on all STP-enabled devices.

```
show runnig-config
show spanning-tree
show spanning-tree summary
show spanning-tress interface xx (Switch interface)
show version
show version slot //Chassis switch slot
```

2.3 Troubleshooting end-user can’t ping gateway successfully

2.3.1 Fault Symptom

In an STP-enabled network with dual core switches, a client accessing the network cannot ping the gateway successfully.

2.3.2 Possible Causes

1) STA between the core and access switches is incorrect.

2) The MSTP domain configuration between the core and access switches is incorrect.

3) The allowed VLANs configured for interfaces between switches are different, which causes abnormal data communication.

4) Other functions (such as RLDP and BPDU Guard) are configured for interfaces between switches, which causes that the interfaces are shut down and in non-forwarding status.

2.3.3 Troubleshooting Procedure

Step 1: Check the STP status between the access and core switches.

Step 2: Check the link configurations between the access and core switches.

Step 3: Check the VLAN interconnectivity between the access and core switches.

Step 4: Check whether the interfaces of the access and core switches are in the forwarding state.

Step 5: Check the MAC addresses of the clients connecting the access and core switches.

Step 6: Collect fault information and submit cases to Ruijie Service Portal.

Step1: Check the STP status between the access and core switches.

1. Check the status of the interfaces between the access and core switches (including the convergence switches) and ensure that the instances to which the member VLANs of the interfaces belong are in the forwarding state.

```
show spanning-tree interface xx
```

If the instances to which the member VLANs of the interfaces belong are not in the forwarding state, go to Step 2.

Step2: Check the link configurations between the access and core switches.

1. Check whether the VLAN instances of the interfaces between the access and core switches are consistent. If the VLAN instance configurations in MSTP are incorrect, STA cannot be conducted in the same MSTP domain. If different STP modes are configured on different switches, certain unexpected results may occur.

The checking method is as follows:

1) Run the **show run** command to check instance-related content in the STP configuration.

2) Check the MSTP configurations of all switches in the topology and ensure that the MSTP domain configurations are consistent.

Step3: Check the VLAN interconnectivity between the access and core switches.

1. Check whether the interfaces between the access and core switches allow member VLANs, that is, whether there is data of allowed VLANs passing the dual uplink links.

show run interface xxx //Display the VLAN configuration of an interface.

2. Check the configurations of VLAN allowed by an interface. Incorrect configurations may cause that the actual data forwarding is incompliant with the VLAN-instance mapping rule.

For example, in a dual-core topology, based on MSTP, the interface of a VLAN corresponding to an instance on an access-layer convergence switch is in the forwarding state. However, the VLAN has not been configured, which blocks data flowing.

3. Set the spanning-tree cost of interfaces to modify the shape of the spanning tree, and ensure that the VLAN configurations on the interfaces and the forwarding state are consistent.

Step4: Check whether the interfaces between the access and core switches are in the forwarding state.

1. Check whether the interfaces between the access and core switches are in the forwarding state. Because of RLDP or BPDU Guard, the interfaces may be blocked or shut down. Particularly, check whether certain functions supported block the interfaces.

Run the following command for checking: show interface status.

Notes

To ensure that RSTP or MSTP on Ruijie switches and H3C switches are compatible, you need to configure the packet format on H3C switch interfaces as compliant with the 802.1S standard by using the **stp compliance** command. In addition, you need to configure the default path cost to be calculated according to the IEEE 802.1t standard by using the **dot1t** command. If the above are not configured, the H3C switches will shut down the interfaces connecting to Ruijie switches.

Step5: Check the MAC addresses of clients connecting the access and core switches.

Check the MAC addresses of the clients connecting the access and core switches by running the **show mac-address-table** command. If the MAC addresses of the clients are all displayed, and the MAC addresses can still be learned after the **clear mac-address-table** command is executed, the fault may not be caused by STP.

If the MAC addresses of the clients are not displayed on the core switches but available on the access switches, unplug either of the dual links. If the fault remains, go to Step 6.

Step6: Collect fault information and submit cases to Ruijie Service Portal.

If the fault is not rectified through the preceding steps, collect the following information and the analysis information obtained in steps 1 to 4. Submit cases to Ruijie Service Portal for further handling.

Collect the network topology information on all STP-enabled devices.

```
show runnig-config

show spanning-tree

show spanning-tree summary

show spanning-tress interface xx (Switch interface)

show version

show version slot //Chassis switch slot
```

2.4 Compatibility Problems between the switches of Ruijie and Cisco

2.4.1 Fault Symptom

In STP deployment, Ruijie switches are often used together with Cisco switches for networking. However, the default Cisco-proprietary PVST cannot be interoperable with the standard STP applied by Ruijie. Therefore, Ruijie switches cannot collaborate with Cisco switches normally.

Note that PVST can send both standard and private BPDU packets, which may cause misjudgments by clients. For example, some spanning-tree instance (Instance 0) calculations seem correct, but certain spanning-tree instance (not instance 0) calculations are incorrect. Therefore, in hybrid networking with both Ruijie devices and

Cisco devices, the spanning-tree configurations of all Cisco switches must be checked first. For similar compatible faults, see the following troubleshooting procedure.

2.4.2 Possible Causes

1) STP standards of Ruijie and Cisco switches are different. Cisco uses PVST while Ruijie applies standard STP.

2) The software release of Cisco switches is of a lower version (lower than IOS 12.25SE), which causes inconsistency in STP packet fields and incorrect STA results.

3) Switch configurations are incorrect, especially in an MSTP-enabled network. The mappings between STP instances and VLANs are incorrect.

4) A loop or STP flapping occurs in the network, which causes the timeout of receiving and processing BPDU packets and then the failure of STP algorithm.

2.4.3 Troubleshooting Procedure

Step 1: Unify the STP modes on all switches in the network.

Step 2: Check the software releases of Cisco switches in the network.

Step 3: Check the VLAN activation on Cisco switches.

Step 4: Check the configurations of interfaces accessed by clients on Cisco switches.

Step 5: Check whether STP flapping or a loop occurs.

Step 6: Collect fault information and submit cases to Ruijie Service Portal.

Step1: Unify the STP modes on all switches in the network.

1. Check the STP configurations of all switches in the network. If both MSTP and PVST (Cisco-proprietary) are used in the layer-2 network, unify the STP modes on Cisco switches to the MSTP mode.

Step2: Check the software releases of Cisco switches in the network.

1. Check the software releases of Cisco switches configured with MSTP. The software releases of Cisco switches must be higher than IOS 12.2 (25) SEC.

Notes

Cisco switches of releases lower than IOS12.2(25)SEC use a private algorithm for the **digest** field in BPDU packets. This causes such a problem: Even though the same MSTP configurations are used on Ruijie and Cisco switches, the switches assume they are in different domains, which then causes incorrect calculations so that they all regard themselves as the root bridge.

Step3: Check the VLAN activation on Cisco switches.

1. Check the configuration of VLAN instances enabled with MSTP on Cisco switches. Ensure that the VLANs in the instances have been configured and the member interfaces of the VLANs are in the Upstate. Ensure that interfaces on Cisco switches connecting to Ruijie switches belong to valid VLANs in all instances configured in a domain. The simplest way is to configure these interfaces as Trunk interfaces that allow all VLANs.

For example: A user configures three instances on a Cisco switch but BPDU packets sent by the switch may not carry all the three instances. The instance information can be sent only after being activated. Otherwise, even though the Cisco switch is connected to Ruijie switches over MSTP, the MSTP tree of the Cisco switch is thought in another domain, which causes incorrect STA. A solution is to activate the instances. The conditions for activating an instance in MST on a Cisco switch are as follows: The VLAN mapped to the instance must be available on the device; at least one interface on the switch that belongs to this VLAN; the VLAN mapped to the instance has at least one interface that is in the Up state.

Step4: Check the configurations of interfaces accessed by clients on Cisco switches.

1. Check whether BPDU is configured on the interfaces on Cisco switches connecting PCs. If the BPDU filter function is configured, Port Fast must also be configured.

Notes

The BPDU filter function enabled on Cisco switches can only filter BPDU packets on interfaces, but cannot prevent the generation of TCN packets when the interfaces are in Up state. The BPDU filter function enabled on Ruijie switches can filter both BPDU packets and TCN packets when the interfaces are in Up state. Network flapping may occur when Ruijie switches receive TCN packets from Cisco switches. Therefore, both the BPDU filter and the Port Fast functions need to be configured on interfaces of Cisco switches.

Step5: Check whether STP flapping or a loop occurs.

1. After the compatible cause is excluded by the preceding operations, the network may still flaps and STP interface roles are mistaken. In this case, troubleshoot the faults by using general methods. For details, see the troubleshooting guides in sections "Broadcast Storm Occurring in a Topology Where Layer-2 Access Switches Are Connected to Dual Core Switches" and "STP Flapping Continually Occurring in a Topology Where Layer-2 Access Switches Are Connected to Dual Core Switches".

Step6: Collect fault information and submit cases to Ruijie Service Portal.

1. If the fault is not rectified through the preceding steps, you can log in to Ruijie Service Portal for support after collect the following information and the analysis information obtained in steps 1 to 4.

Collect the network topology information on all STP-enabled devices.

show runnig-config

show spanning-tree

show spanning-tree summary

show spanning-tress interface xx (Switch interface)

show version

show version slot //Chassis switch slot

2.5 Troubleshooting Service intermittence based on the network of MSTP&VRRP

2.5.1 Fault Symptom

Service intermittence occurs based on the network of MSTP&VRRP.

2.5.2 Possible Causes

1) A switch receives massive TC packets and frequently clear address tables, which causes network flapping.

2) The CPU usage on a switch is too high, which causes that protocol packets cannot be processed in time and then causes network flapping.

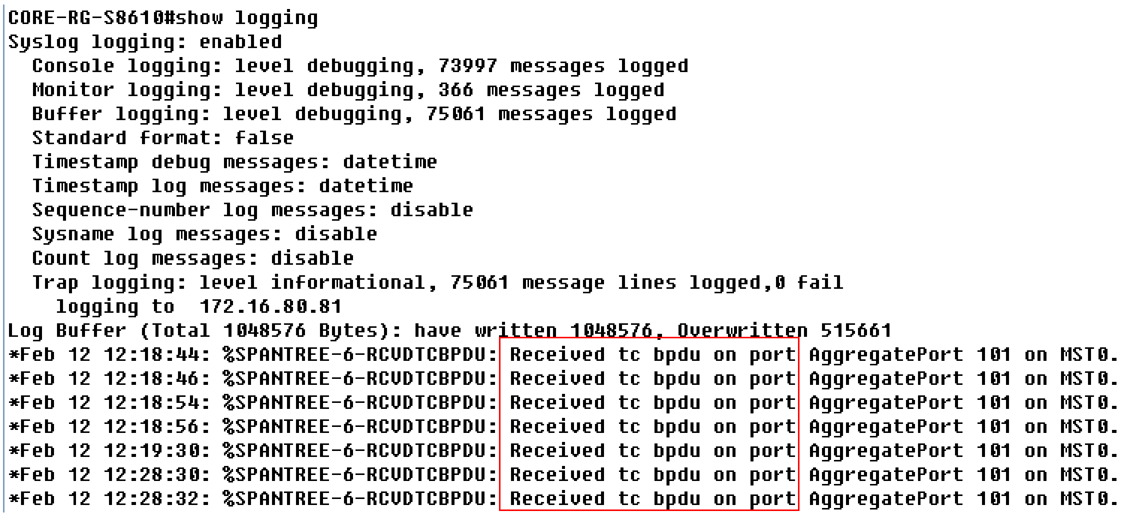
3) BPDU packets sent to the CPU of a switch are lost, which causes network flapping.

4) VRRP packets sent to the CPU of a switch are lost, which causes network flapping.

2.5.3 Troubleshooting Procedure

Step1:Check whether a switch receives massive TC packets.

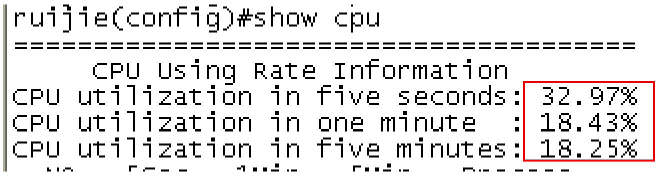
Run the **show logging** command to check whether the switch receives massive TC packets.



```
CORE-RG-S8610#show logging
Syslog logging: enabled
  Console logging: level debugging, 73997 messages logged
  Monitor logging: level debugging, 366 messages logged
  Buffer logging: level debugging, 75061 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Count log messages: disable
  Trap logging: level informational, 75061 message lines logged,0 fail
    logging to  172.16.80.81
Log Buffer (Total 1048576 Bytes): have written 1048576, Overwritten 515661
*Feb 12 12:18:44: %SPANTREE-6-RCVDTCBPDU: Received tc bpdu on port AggregatePort 101 on MST0.
*Feb 12 12:18:46: %SPANTREE-6-RCVDTCBPDU: Received tc bpdu on port AggregatePort 101 on MST0.
*Feb 12 12:18:54: %SPANTREE-6-RCVDTCBPDU: Received tc bpdu on port AggregatePort 101 on MST0.
*Feb 12 12:18:56: %SPANTREE-6-RCVDTCBPDU: Received tc bpdu on port AggregatePort 101 on MST0.
*Feb 12 12:19:30: %SPANTREE-6-RCVDTCBPDU: Received tc bpdu on port AggregatePort 101 on MST0.
*Feb 12 12:28:30: %SPANTREE-6-RCVDTCBPDU: Received tc bpdu on port AggregatePort 101 on MST0.
*Feb 12 12:28:32: %SPANTREE-6-RCVDTCBPDU: Received tc bpdu on port AggregatePort 101 on MST0.
```

--->>If massive TC packets are received in network flapping, the network flapping may be caused by the TC packets. You need to configure TC protection by using the **spanning-tree tc-protection** command on the switch and identify the source of the TC packets.

Step2: Check whether the CPU usage of a switch is too high.

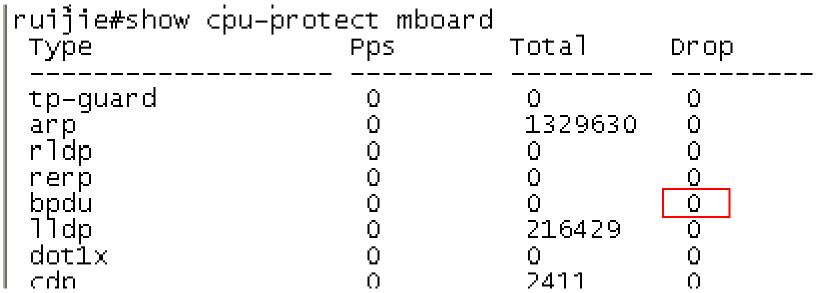


```
ruijie(config)#show cpu
=======================================
      CPU Using Rate Information
CPU utilization in five seconds: 32.97%
CPU utilization in one minute   : 18.43%
CPU utilization in five minutes: 18.25%
```

--->> If the CPU usage exceeds 90%, the network flapping may be caused by the high CPU usage. Because of that corresponding protocol packets cannot be processed in time and then causes network flapping. You need to check the processes that cause the high CPU usage.

Step3: Check whether BPDU packets sent to the CPU of a switch are lost.

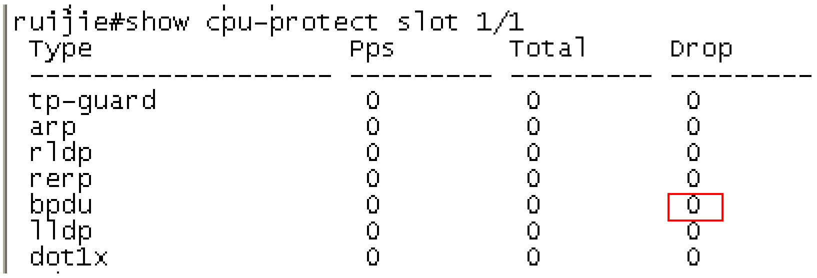
(1) Check whether the BPDU packets sent to the CPU of the management board are lost.



```
ruijie#show cpu-protect mboard
 Type                 Pps        Total      Drop
 -------------------- ---------- ---------- ----------
 tp-guard              0          0          0
 arp                   0          1329630    0
 rldp                  0          0          0
 rerp                  0          0          0
 bpdu                  0          0          0
 lldp                  0          216429     0
 dot1x                 0          0          0
 cdp                   0          2411       0
```

--->> If this value is greater than 0 and increases, it indicates that BPDU packets sent to the CPU of the management board are lost, which may be the cause for network flapping.

(2) Check whether the BPDU packets sent to the CPU of the line card are lost.



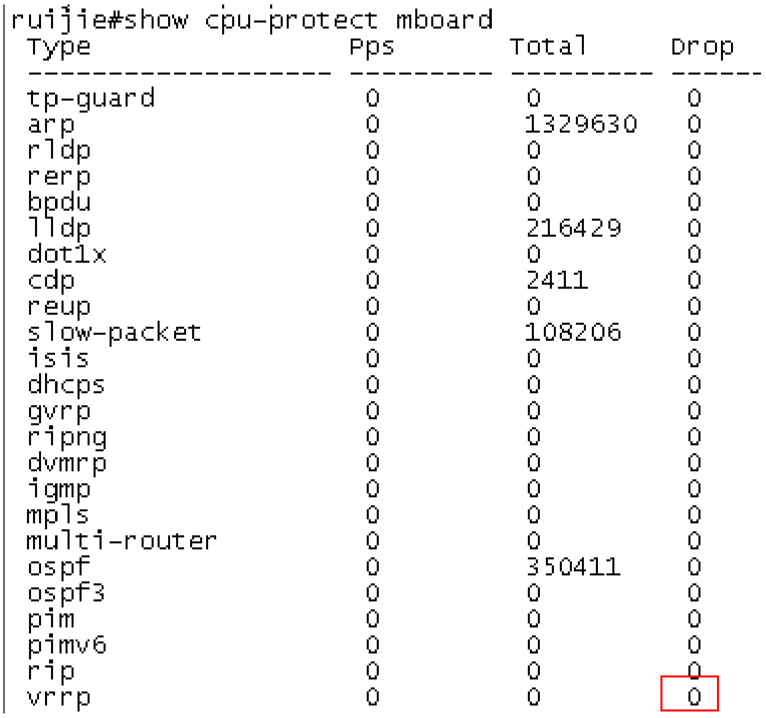
```
ruijie#show cpu-protect slot 1/1
 Type                 Pps        Total      Drop
 -------------------- ---------- ---------- ----------
 tp-guard              0          0          0
 arp                   0          0          0
 rldp                  0          0          0
 rerp                  0          0          0
 bpdu                  0          0          0
 lldp                  0          0          0
 dot1x                 0          0          0
```

--->> If this value is greater than 0 and increases, it indicates that BPDU packets sent to the CPU of the line card are lost, which may be the cause for network oscillation.

If the BPDU packets sent to the CPU are lost, it is recommended to set the CPP threshold for BPDU packets to a larger value. In addition, you need to check whether the number of BPDU packets in the environment meets the expectation.

Step4: Check whether VRRP packets sent to the CPU of a switch are lost.

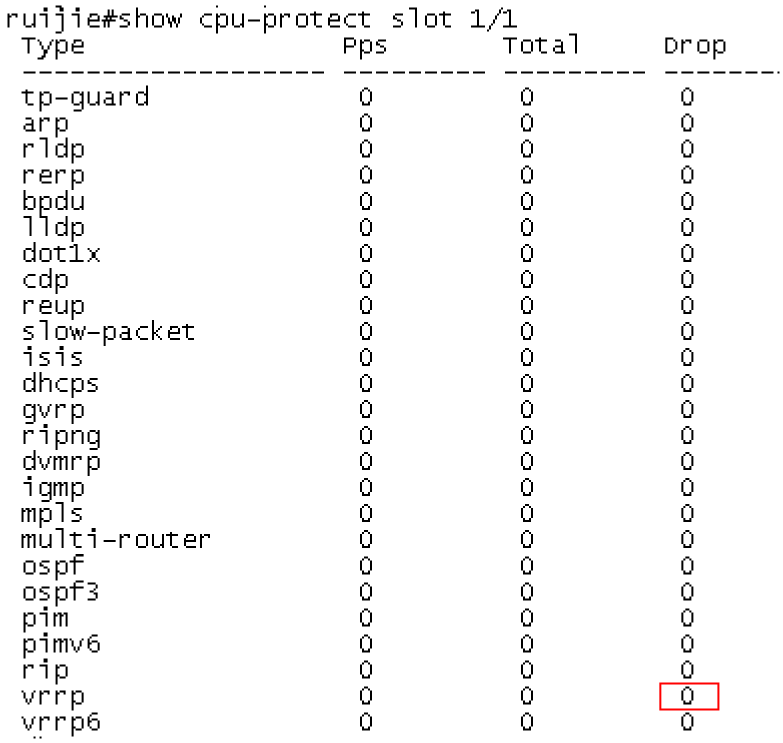
(1) Check whether the VRRP packets sent to the CPU of the management board are lost.



```
ruijie#show cpu-protect mboard
 Type                   Pps        Total      Drop
 -------------------- ---------- ---------- ------
 tp-guard                0          0          0
 arp                     0          1329630    0
 rldp                    0          0          0
 rerp                    0          0          0
 bpdu                    0          0          0
 lldp                    0          216429     0
 dot1x                   0          0          0
 cdp                     0          2411       0
 reup                    0          0          0
 slow-packet             0          108206     0
 isis                    0          0          0
 dhcps                   0          0          0
 gvrp                    0          0          0
 ripng                   0          0          0
 dvmrp                   0          0          0
 igmp                    0          0          0
 mpls                    0          0          0
 multi-router            0          0          0
 ospf                    0          350411     0
 ospf3                   0          0          0
 pim                     0          0          0
 pimv6                   0          0          0
 rip                     0          0          0
 vrrp                    0          0          0
```

--->> If this value is greater than 0 and increases, it indicates that VRRP packets sent to the CPU of the management board are lost, which may be the cause for network flapping.

(2) Check whether the VRRP packets sent to the CPU of the line card are lost.



```
ruijie#show cpu-protect slot 1/1
 Type                   Pps        Total      Drop
 -------------------- ---------- ---------- -------
 tp-guard                0          0          0
 arp                     0          0          0
 rldp                    0          0          0
 rerp                    0          0          0
 bpdu                    0          0          0
 lldp                    0          0          0
 dot1x                   0          0          0
 cdp                     0          0          0
 reup                    0          0          0
 slow-packet             0          0          0
 isis                    0          0          0
 dhcps                   0          0          0
 gvrp                    0          0          0
 ripng                   0          0          0
 dvmrp                   0          0          0
 igmp                    0          0          0
 mpls                    0          0          0
 multi-router            0          0          0
 ospf                    0          0          0
 ospf3                   0          0          0
 pim                     0          0          0
 pimv6                   0          0          0
 rip                     0          0          0
 vrrp                    0          0          0
 vrrp6                   0          0          0
```

--->> If this value is greater than 0 and increases, it indicates that VRRP packets sent to the CPU of the line card are lost, which may be the cause for network flapping.

If the VRRP packets sent to the CPU are lost, it is recommended to set the CPP threshold for VRRP packets to a larger value. In addition, you need to check whether the number of VRRP packets in the environment meet the expectation.

Step5:Fault Information Collection

Collect log information (pay attention to the time stamp and the time accuracy) for background analysis.

show logging

showcpu

showcpu-protect mb

show cpu-protect slot X *//X indicates the slot ID, such as use this command on Slot 4 of the stand-alone Switch8610: show cpu-pro slot 4;on Slot 4 of Chassis2 in the VSU: show cpu-pro slot 2/4.*

3. Troubleshooting link-aggregation

3.1 Troubleshooting link-aggregation fails or packet forwarding interrupt

3.1.1 Fault Symptom

Link aggregation fails or the traffic interrupt after the aggregation succeeds.

3.1.2 Possible Causes

1. The physical link is faulty.

2. LACP negotiation fails.

3. Traffic can’t be load balancing among the ports in the link-aggregation, in the case that ip or mac address didn’t change.

4. The duplex modes (only the port with full-duplex can be aggregated), Speed, media type and Layer2&3 port attribute must be consistent.

3.1.3 Troubleshooting Procedure

Step1: Check whether the configurations are correct.

1. If the local end is configured as a static aggregate port (AP), the peer end should also be configured as a static AP.

2. If the local end is configured with dynamic LACP aggregation, the peer end should also be configured with dynamic LACP aggregation.

```
Ruijie#show run int gi x/y      //Check the configurations of the aggregate member interfaces.
```

Step 2: Check whether the aggregate member interfaces have link faults.

1. Run **show interface status** command to check whether the aggregate member ports are in the Up state.

2. If not, check the physical links. Ensure that the member interfaces are in the Up state. If conditions permit, you can replace the member ports with other interfaces to exclude physical failure and find out the faulty member ports.

3. After the aggregate member ports are in the "Up" state, check whether the fault is rectified. If the yes, stop further troubleshooting.

4. If the fault remains after the member ports are replaced, collect information and submit cases to Ruijie Service Portal.

Step3: Shut down the member ports one by one and keep only one member ports in the Up state at a time to test whether the communication will recover.

Notes

This operation can be performed only after permitted by customer services because it may interrupt the service connection on the aggregate interfaces. Even though it is approved by customers, it is recommended to perform this operation at low-traffic periods.

Step4: Fault Information Collection

1. Collecting basic information:

--------Collect information in the privileged EXEC mode (ruijie#)----------

show aggregateport *aggregate x* load-balance

//Fill in the aggregate interface number based on the actual conditions. For example, if the aggregate interface number is 2, the command is **show aggregateport 2 load-balance**.

show aggregate port aggregation x summary

//Fill in the aggregate interface number based on the actual conditions. For example, if the aggregate interface number is 2, the command is **show aggregateport 2 summary**.

show running-config

show int gi x/y

r//Fill in the member interface number based on the actual conditions. For example, the command can be **show int g0/1**.

show int ag aggregation x

//Fill in the aggregate interface number based on the actual conditions. For example, if the aggregate interface number is 2, the command is **show int ag 2**.

Show lacp summary

show log

2. Collecting debugging information (If there is no output with Telnet used, use the Console port to access the switch for information collection.)

ruijie>enable

ruijie#terminal monitor

ruijie#config t

ruijie(config)#logging on

ruijie(config)#logging console

ruijie(config)#exit

3.2 Troubleshooting LACP negotiation fails between the switch of Ruijie and other Brand

3.2.1 Fault Symptom

LACP negotiation fails between the switch of Ruijie and other Brand.

3.2.2 Possible Causes

1. The switch hardware is faulty, which causes that the switch cannot normally negotiate interface parameters.

2. The duplex modes, Speed and media-type on the two-side switches are not consistent.

3. The switches of other enterprises do not use the standard LACP protocol. For example, the Cisco switches enable PAGP (a proprietary protocol) and therefore cannot form an aggregate link with Ruijie switches.

4. LACP parameters on switches at the two ends are incorrect such as wrong LACP mode. For example, if the switches are configured with the "passive mode-passive mode", you need to manually change it to "active mode-active mode" or "active mode-passive mode".

5. LACPDU packets fail to be received. For example, link faults cause packet loss and then negotiation failure.

6. LACPDU packet negotiation fails because the key fields of the packets do not match.

3.2.3 Troubleshooting Procedure

Step 1: Check the interface attributes of the switches at the two ends.

Step 2: Check the LACP configurations of the switches at the two ends.

Step 3: Check the transmission of LACP packets of the switches.

Step 4: Check the LACP negotiation between the switches.

Step 5: Collect fault information and submit cases to Ruijie Service Portal.

Step1: Check the interface attributes of the switches at the two ends.

1. Run the **show interface XX** command to check the interface attributes. Focus on the rates, traffic control policies and medium types of the interfaces, and configure the interfaces to work in the full-duplex mode.

For example:

```
Ruijie#show int gigabitEthernet 1/1

Index(dec):17 (hex):11

GigabitEthernet 1/1 is DOWN    , line protocol is DOWN

Hardware is Broadcom 5464 GigabitEthernet
```

```
Interface address is: no ip address
MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Switchport attributes:
    interface's description:""
admin medium-type is Copper, oper medium-type is Copper
    lastchange time:0 Day: 0 Hour: 1 Minute:22 Second
    Priority is 0
admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
flow control admin status is OFF, flow control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Port-type: access
    Vlan id: 1
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

2. Check the log information on the switches during negotiation or run the **show log** command to display logs.

1) If the rates at two ends are different, the following information is displayed during negotiation:

```
*Aug 26 21:58:50: %LACP-5-NOTCOMPATIBLE: Interface GigabitEthernet 1/3 is not compatible with
aggregators.(Port speed of GigabitEthernet 1/3 is 100M, GigabitEthernet 1/4 is 1000M).
```

The following information is displayed by using **show lacp summary command**:

```
Ruijie#show lacp summary

System Id:32768, 001a.a97d.8fc3

Flags:   S - Device is requesting Slow LACPDUs     F - Device is requesting Fast LACPDUs.

A - Device is in active mode.            P - Device is in passive mode.

Aggregate port 1:

Local information:

                                  LACP port        Oper     Port      Port

Port        Flags       State        Priority         Key      Number   State

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

Gi1/3       SP          sups         32768            0x1      0x3      0x44

Gi1/4       SA          bndl         32768            0x1      0x4      0x3d


Partner information:

                     LACP port                        Oper     Port      Port

Port        Flags       Priority       Dev ID         Key      Number    State

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

Gi1/3       SP          0              0000.0000.0000   0x0      0x0       0x0

Gi1/4       SA          32768       001a.a916.11b6    0x1      0x14      0x3d
```

Notes

If the interface status is **sups**, it means that when the interface link is in the Up state the interface is suspended (displayed in the **sups** state) through packet negotiation because the peer interface is not enabled with LACP or the interface attributes are different from those of the primary interface. Interfaces in the **sups** state are not involved in the data packet forwarding of the aggregate group.

2) If the duplex modes are different, the following information is displayed during negotiation:

```
*Aug 26 22:01:51: %LACP-5-NOTCOMPATIBLE: Interface GigabitEthernet 1/3 is not compatible with aggregators.(GigabitEthernet 1/3 is half duplex.)
```

The same information as above is displayed by using the following command:

```
Ruijie#show lacp summary
```

Step2: Check the LACP configurations of the switches at the two ends.

1. Check the LACP configurations of the two-side aggregate switches. Check whether they use the non-standard LACP protocol and whether their LACP negotiation mode is configured to "passive mode-passive mode".

1) If a Cisco switch is connected, ensure that the Cisco switch is enabled with LACP instead of PAGP (Cisco-proprietary).

2) LACP interfaces have two modes: active and passive. If both the two switch interfaces are configured to work in the passive mode, aggregation cannot be established. To enable aggregation, the two peer interfaces must work both in the active mode, or one is in the active mode and the other in the passive mode.

Step3: Check the transmission of LACP packets on the switches at the two ends.

Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time.

1. Check LACP packet interaction. Mirror the LACP aggregate port to another interface of the switch for packet capturing and then run the **debug lacp event** and **debug lacp packet** commands for checking.

2. LACPDU packets are sent every 30 seconds. Check the transmission of LACPDU packets on the switches to verify whether the packets are discarded. If the local switch does not send LACPDU packets, the local switch is faulty. If the peer switch does not receive LACPDU packets, the peer switch is faulty or the connected link is faulty.

```
*Aug 26 22:27:23: %7: [lacp packet]send a lacp pdu to ifx 19 success.

*Aug 26 22:27:24: %7: [lacp timer]port 19 hold_while expired

*Aug 26 22:27:25: %7: [lacp packet]port[19] rcvd LACP PDU packet

*Aug 26 22:27:25: %7: [lacp packet]received a pdu from 19.

*Aug 26 22:27:25: %7: Actor     sys pri:32768 sys id:001a.a97d.8fc3 port pri:32768 port no:3 port key:1

*Aug 26 22:27:25: %7: Passive   Aggregate In sync Collecting   Distributing
```

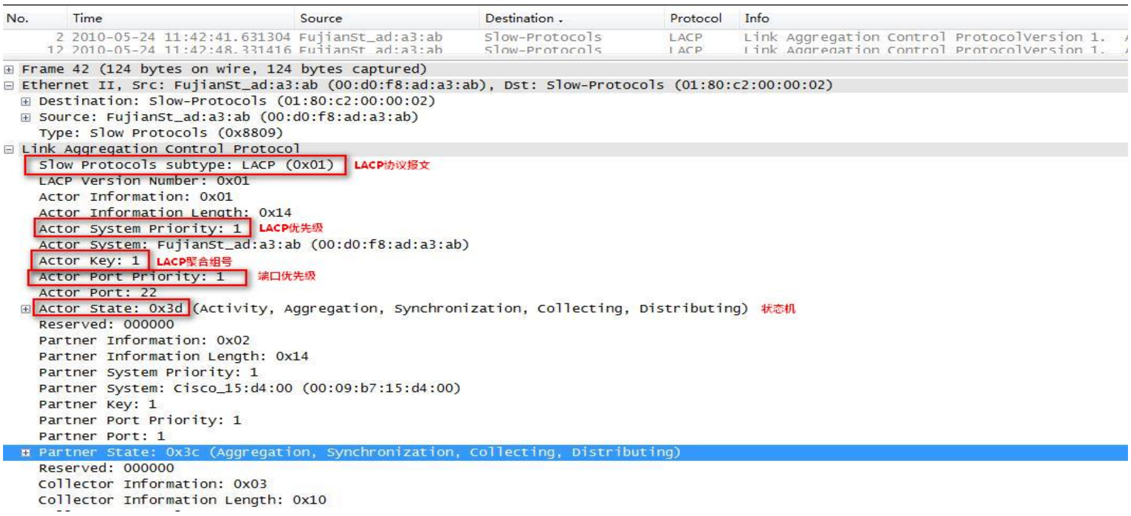
```
*Aug 26 22:27:25: %7: Partner sys pri:32768 sys id:001a.a916.11b6 port pri:32768 port no:19 port key:1
*Aug 26 22:27:25: %7: Active    Aggregate In sync Collecting   Distributing
*Aug 26 22:27:25: %7: port sys pri:32768 sys id:001a.a916.11b6 port pri:32768 port no:19 port key:1
*Aug 26 22:27:25: %7: Active    Aggregate In sync Collecting   Distributing
*Aug 26 22:27:25: %7: pdu sys pri:32768 sys id:001a.a916.11b6 port pri:32768 port no:19 port key:1
*Aug 26 22:27:25: %7: Active    Aggregate In sync Collecting   Distributing
*Aug 26 22:27:25: %7: [lacp timer]start current long while timer for port 19.
*Aug 26 22:27:53: %7: [lacp stm]port 19 tx machine ntt.
*Aug 26 22:27:53: %7: [lacp timer]port 19 start tx_scheduler.
*Aug 26 22:27:53: %7: [lacp stm]port 19 tx machine txd.
*Aug 26 22:27:53: %7: [lacp packet]port 19 tx pdu.
*Aug 26 22:27:53: %7: [lacp packet]get port 19 default vid 1
*Aug 26 22:27:53: %7: Actor    sys pri:32768 sys id:001a.a916.11b6 port pri:32768 port no:19 port
key:1
*Aug 26 22:27:53: %7: Active    Aggregate In sync Collecting   Distributing
*Aug 26 22:27:53: %7: Partner sys pri:32768 sys id:001a.a97d.8fc3 port pri:32768 port no:3 port key:1
*Aug 26 22:27:53: %7: Passive   Aggregate In sync Collecting   Distributing
*Aug 26 22:27:53: %7: [lacp packet]send a lacp pdu to ifx 19 success.
*Aug 26 22:27:54: %7: [lacp timer]port 19 hold_while expired
*Aug 26 22:27:57: %7: [lacp packet]port[19] rcvd LACP PDU packet
*Aug 26 22:27:57: %7: [lacp packet]received a pdu from 19.
*Aug 26 22:27:57: %7: Actor    sys pri:32768 sys id:001a.a97d.8fc3 port pri:32768 port no:3 port key:1
*Aug 26 22:27:57: %7: Passive   Aggregate In sync Collecting   Distributing
*Aug 26 22:27:57: %7: Partner sys pri:32768 sys id:001a.a916.11b6 port pri:32768 port no:19 port key:1
*Aug 26 22:27:57: %7: Active    Aggregate In sync Collecting   Distributing
*Aug 26 22:27:57: %7: port sys pri:32768 sys id:001a.a916.11b6 port pri:32768 port no:19 port key:1
*Aug 26 22:27:57: %7: Active    Aggregate In sync Collecting   Distributing
*Aug 26 22:27:57: %7: pdu sys pri:32768 sys id:001a.a916.11b6 port pri:32768 port no:19 port key:1
*Aug 26 22:27:57: %7: Active    Aggregate In sync Collecting   Distributing
*Aug 26 22:27:57: %7: [lacp timer]start current long while timer for port 19.
```

3. If the fault remains, go to Step 4 for further troubleshooting.

Step4: Check the LACP negotiation between the switches at the two ends.

1. Analyze the fields in the LACPDU packets captured and check whether the fault is caused by abnormal packets.

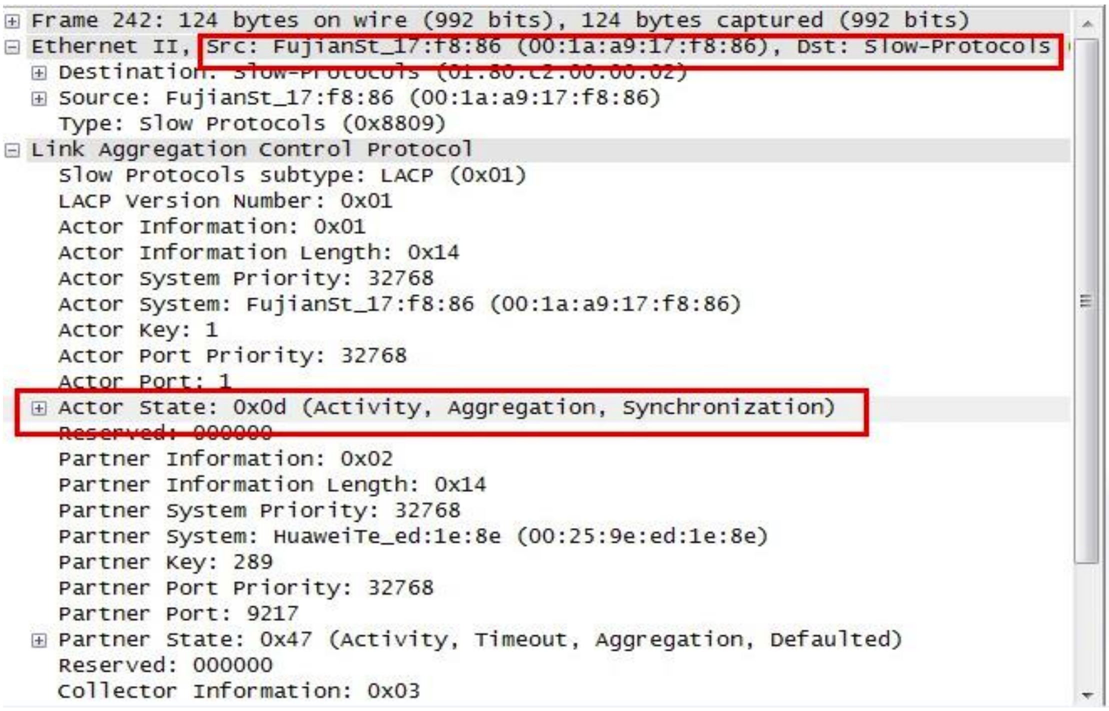
1) A normal LACPDU packet is as follows:



```
No.    Time                          Source               Destination .      Protocol  Info
     2 2010-05-24 11:42:41.631304 FujianSt_ad:a3:ab   Slow-Protocols     LACP      Link Aggregation Control Protocolversion 1.
    12 2010-05-24 11:42:48.331416 FujianSt_ad:a3:ab   Slow-Protocols     LACP      Link Aggregation Control Protocolversion 1.
⊞ Frame 42 (124 bytes on wire, 124 bytes captured)
⊟ Ethernet II, Src: FujianSt_ad:a3:ab (00:d0:f8:ad:a3:ab), Dst: Slow-Protocols (01:80:c2:00:00:02)
  ⊞ Destination: Slow-Protocols (01:80:c2:00:00:02)
  ⊞ Source: FujianSt_ad:a3:ab (00:d0:f8:ad:a3:ab)
    Type: Slow Protocols (0x8809)
⊟ Link Aggregation Control Protocol
    Slow Protocols subtype: LACP (0x01)   LACP协议报文
    LACP Version Number: 0x01
    Actor Information: 0x01
    Actor Information Length: 0x14
    Actor System Priority: 1   LACP优先级
    Actor System: FujianSt_ad:a3:ab (00:d0:f8:ad:a3:ab)
    Actor Key: 1   LACP聚合组号
    Actor Port Priority: 1   端口优先级
    Actor Port: 22
  ⊞ Actor State: 0x3d (Activity, Aggregation, Synchronization, Collecting, Distributing)   状态机
    Reserved: 000000
    Partner Information: 0x02
    Partner Information Length: 0x14
    Partner System Priority: 1
    Partner System: Cisco_15:d4:00 (00:09:b7:15:d4:00)
    Partner Key: 1
    Partner Port Priority: 1
    Partner Port: 1
  ⊞ Partner State: 0x3c (Aggregation, Synchronization, Collecting, Distributing)
    Reserved: 000000
    Collector Information: 0x03
    Collector Information Length: 0x10
```

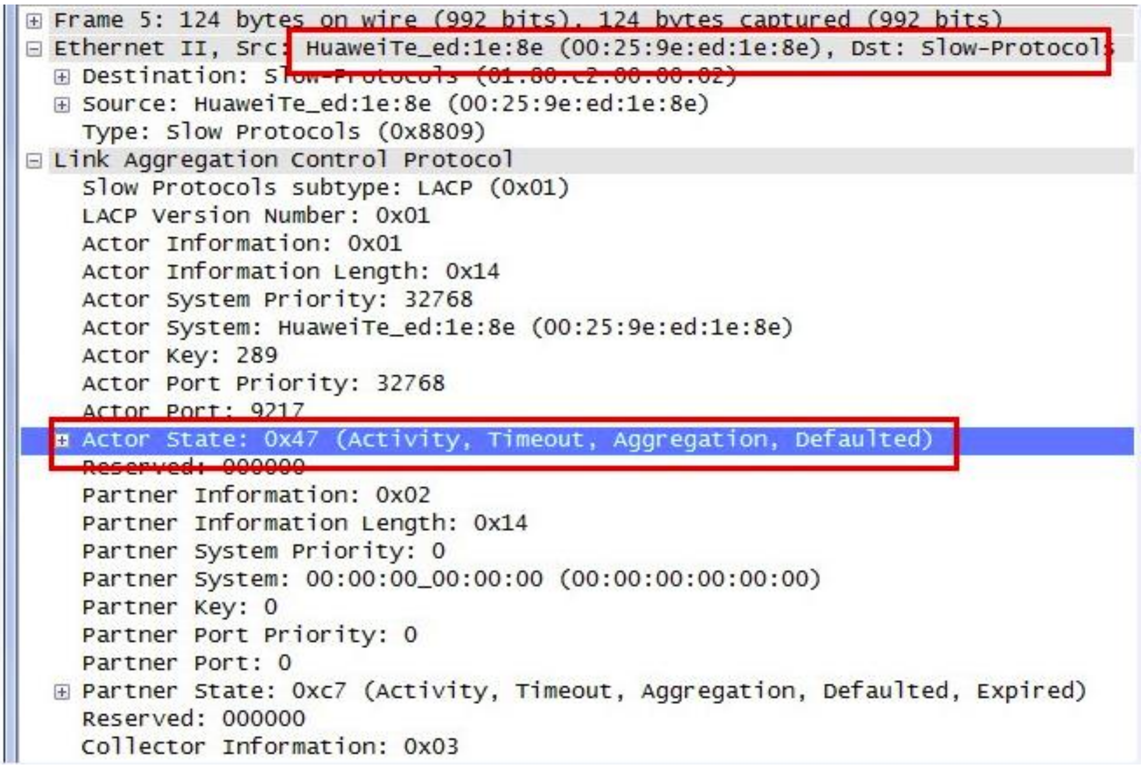
2) An LACPDU packet failing in negotiation is as follows:

Switch1:



```
⊞ Frame 242: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
⊟ Ethernet II, Src: FujianSt_17:f8:86 (00:1a:a9:17:f8:86), Dst: Slow-Protocols
  ⊞ Destination: Slow-Protocols (01:80:c2:00:00:02)
  ⊞ Source: FujianSt_17:f8:86 (00:1a:a9:17:f8:86)
    Type: Slow Protocols (0x8809)
⊟ Link Aggregation Control Protocol
    Slow Protocols subtype: LACP (0x01)
    LACP Version Number: 0x01
    Actor Information: 0x01
    Actor Information Length: 0x14
    Actor System Priority: 32768
    Actor System: FujianSt_17:f8:86 (00:1a:a9:17:f8:86)
    Actor Key: 1
    Actor Port Priority: 32768
    Actor Port: 1
  ⊞ Actor State: 0x0d (Activity, Aggregation, Synchronization)
    Reserved: 000000
    Partner Information: 0x02
    Partner Information Length: 0x14
    Partner System Priority: 32768
    Partner System: HuaweiTe_ed:1e:8e (00:25:9e:ed:1e:8e)
    Partner Key: 289
    Partner Port Priority: 32768
    Partner Port: 9217
  ⊞ Partner State: 0x47 (Activity, Timeout, Aggregation, Defaulted)
    Reserved: 000000
    Collector Information: 0x03
```

Switch 2:



```
⊞ Frame 5: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
⊟ Ethernet II, Src: HuaweiTe_ed:1e:8e (00:25:9e:ed:1e:8e), Dst: Slow-Protocols
  ⊞ Destination: Slow-Protocols (01:80:c2:00:00:02)
  ⊞ Source: HuaweiTe_ed:1e:8e (00:25:9e:ed:1e:8e)
    Type: Slow Protocols (0x8809)
⊟ Link Aggregation Control Protocol
    Slow Protocols subtype: LACP (0x01)
    LACP Version Number: 0x01
    Actor Information: 0x01
    Actor Information Length: 0x14
    Actor System Priority: 32768
    Actor System: HuaweiTe_ed:1e:8e (00:25:9e:ed:1e:8e)
    Actor Key: 289
    Actor Port Priority: 32768
    Actor Port: 9217
  ⊞ Actor State: 0x47 (Activity, Timeout, Aggregation, Defaulted)
    Reserved: 000000
    Partner Information: 0x02
    Partner Information Length: 0x14
    Partner System Priority: 0
    Partner System: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Partner Key: 0
    Partner Port Priority: 0
    Partner Port: 0
  ⊞ Partner State: 0xc7 (Activity, Timeout, Aggregation, Defaulted, Expired)
    Reserved: 000000
    Collector Information: 0x03
```

Step5: Collect fault information and submit cases to Ruijie Service Portal.

If the fault remains after the preceding operations are performed, collect the following fault information and submit cases to Ruijie Service Portal for help.

When a fault occurs, collect log information (pay attention to the time stamp and the time accuracy) for background analysis.

[Device debugging information, configuration, hardware models, software versions, device logs and operation logs]

show run

show version

show version slot

show logging

debug lacp event

debug lacp packet

debug lacp stm //Check the LACP state machine.

debug lacp timer //Check the LACP timer.

⚠ Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time.

4. Troubleshooting IP Routing protocol

4.1 Troubleshooting packet forwarding fails

4.1.1 Fault Symptom

The routing table contains route information but packet forwarding fails.

4.1.2 Possible Causes

1) Switch configurations problems, for example, security policies are configured.
2) The network environment problems, for example, packet loss occurs, ARP learning is abnormal and ICMP destination is unreachable.

4.1.3 Troubleshooting Procedure

Step1: Check whether the environment is normal.

Check the network topology, including the device interfaces and IP addresses.

Step2: Check whether route entries are normal.

1.Check a route along the forwarding path hop by hop, and check whether the local end has a route reachable to the peer end and whether the peer end has a return route.

Ruijie#show ip route | include X.X.X.X or show ip route X.X.X.X (X.X.X.X indicates the destination network segment)

If the route configurations are incorrect, modify the route configurations, and check whether the route forwarding is reachable.

2.Check whether a gateway address is configured on a PC NIC card. If not, configure the gateway address on the PC.

Step3: Check whether massive packets are lost.

Run **show interfaces counters** command to display the interface error counters like FCS, collisions and alignments. You can check whether the value of the **FCS Errors** increases orderly. If yes, it indicates packet loss occurs due to a hardware fault. If conditions permit, replace the interface and network cable to check whether the fault is rectified. Along the forwarding path, check whether the next device is faulty by using the same method.

Step4: Check the running status of interfaces.

Run **show interfaces [interface-id]** command to check the physical status, speed, duplex mode, auto-negotiation status of the interfaces to make sure that their physical status is up, and the speed, duplex mode and auto-negotiation status are consistent at the two ends.

For copper port, it works well with the 10M/100M negotiation speed; but it works abnormally with the 1000M negotiation speed. Check whether the network cable is normal. If not, replace the network cable.

Step5: Check whether security policies are configured.

Check whether the ACL, binding and other security functions are configured. If yes, disable the corresponding configurations and then test whether the links can be successfully pinged.

Step6: Check whether the ping failure is caused by a large delay in link transmission.

Using ping command to test the network reachability
Ruijie# **ping** ip-address [length bytes] [ntimes times] [**timeout** seconds]
If the ping succeeds after the delay is increased (specifying the **timeout** parameter for the ping command enables the setting of ping delay), it indicates that the forwarding path is normal and that the fault may be caused by link congestion.

Step7: Reduce the fault locating scope.

Ping the next hop one by one to check the link between which two devices is disconnected.

Perform ingress or egress packet capturing for a target device to check whether the packets that failed to be forwarded reach the target device. This step is critical because it can determine where the packets are lost and locate two faulty devices.

Step8: Check whether ARP entries are learned.

```
Ruijie#show arp | inc X.X.X.X
```

Check ARP entries on the faulty devices. If ARP entries of the peer end are not learned, it indicates that the fault occurs in ARP packets.

For a PC, run the following commands in the “command prompt” window:

```
>ipconfig /all
```

```
>arp -a
```

Check whether the PC has learned the ARP entries of the gateway.

If no ARP entries are learned, go to the next step to check whether packets are normally received and sent.

Step9: Check whether ARP packets or ICMP packets are unreachable.

Perform packet capturing on the faulty devices and PC to check the receiving and sending of ARP and ICMP packets.

Enable the debugging function for ARP and ICMP on the faulty devices to check whether the ARP and ICMP packets are normally sent to the CPUs.

```
Ruijie#debug arp +ACL
```

Disable the preceding debugging function.

```
Ruijie#undeug all
```

Note: This command outputs huge information; therefore an ACL must be configured for filtering. In addition, it is recommended to use a standard ACL, and define the source and destination IP segments to debug ARP request and reply packets respectively.

⚠ Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time.

Step10. Fault Information Collection

Collect log information (pay attention to the time switch and the time accuracy) for fault analysis.

[Device debugging information, configuration, hardware and software versions, device logs and operation logs]

Collecting basic information

```
show version

show version slots

show run

show log

show ip interface brief

show interface status

show interface counter sum

show interface counter   rate

show interfaces counters errors

show interfaces counters

show arp counter

show arp

show arp detail

show mac-address-table

show mac-address-table counter

show ip route

show ip route count

show cpu
```

4.2 Troubleshooting ospf flapping

4.2.1 Fault Symptom

OSPF route flapping occurs, routes are constantly added and deleted, LSAs are constantly refreshed, and the CPU usage is high.

4.2.2 Possible Causes

(1) Neighbor flapping causes route flapping.
(2) Interface IP addresses conflict, network LSAs frequently age and refresh, and route calculation are frequent.
(3) Network flapping, namely, flapping of interface or introduced external routes, causes OSPF route flapping.

4.2.3 Troubleshooting Procedure

Step1: Check whether the neighbor flaps.

1.Check whether the neighbor flaps through Syslog.

The following Syslog is displayed when the OSPF neighbor flaps:

%OSPF-5-ADJCHG: Process [dec], Nbr [chars1] from [chars2] to[chars3], [chars4]. For example:

%OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1-GigabitEthernet 0/1 from Full to Down, InactivityTimer.

2.If the neighbor flaps, the route flapping is caused by the neighbor flapping.

3.If the neighbor does not flap, the possible causes for route flapping are as follows:

1) Network flapping occurs.

2) There are IP addresses in conflict in the area.

Step2: Check whether network flapping occurs.

If network flapping occurs, you can find the following symptoms:

1. LSAs frequently refresh.

2. LSAs frequently age and refresh.

The procedure for checking whether network flapping occurs is as follows:

① Identify the LSA for the flapping route.

1) Identify the type of the flapping route: intra-area route, inter-area route or external route.

2) If the route is an intra-area route, focus on only Router-LSA and Network-LSA in subsequent operations.

If the route is an inter-area route, focus on Router-LSA, Network-LSA and Summary-LSA in subsequent operations.

If the route is an external route, focus on Router-LSA, Network-LSA, ASBR-Summary-LSA, External-LSA and NSSA-LSA in subsequent operations.

② Collect LSA summary information.

show ip ospf database //Collect summary information consecutively for three times at an interval of 1 minute.

③ Compare the LSA information collected at different times.

1) If the serial number of an LSA changes significantly (with a difference greater than 2), it indicates that the LSA frequently refreshes.

2) If the **Age** value of an LSA switches between 3600s and the normal state (between 0 and 1800), it indicates that the LSA constantly ages and refreshes.

④ Check whether network flapping occurs.

If it is found that Network-LSA frequently ages and refreshes in step ③, it indicates that there may be IP addresses in conflict in the network.

If it is found that an LSA frequently refreshes in step ③, it indicates that network flapping occurs. In this case, go to step ⑤.

If it is found that an LSA (not Network-LSA) frequently ages and refreshes in step ③, it indicates that network flapping occurs. In this case, go to step ⑤.

⑤ Collect detailed information about the changed LSAs.

debug ip ospf lsa **(If there are massive LSAs in the environment, screen refreshing may be caused. Perform the operation at low-traffic periods.)**

show ip ospf database [router | network | summary | asbr-summary | external | nssa-external] [adv-router A.B.C.D] [A.B.C.D]

Collect information for 10 times at an interval of 30 seconds.

You can specify the type and announcer based on the LSA that frequently changes found in step ③, specify a unique LSA for information collection and check the details only about the specified LSA.

⚠ Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time.

Step3: Check whether there are IP addresses in conflict in the area.

You can check whether there are IP addresses in conflict by using the following steps:

① Collect information on the faulty device.

show ip ospf database network

Display information about Network-LSA. If there are IP addresses in conflict in the area, Network-LSA constantly switches between aging and refreshing. According to the outputs of the **show** command, Network-LSA constantly switches between 3600s and the normal state (between 0 and 1800s).

② Display static configurations on other devices in the area.

Run the **show running-config** command on devices in the area to check whether their IP addresses are in conflict.

Note: If the IP address of an interface is in conflict against the interface IP address of another device in the area, OSPF route flapping may be caused even though the interface is in the down state.

Step4:Fault Information Collection

Collect log information (pay attention to the time switch and the time accuracy) for fault analysis.

[Device debugging information, configuration, hardware and software versions, device logs and operation logs]

----

show version

```
show version slots

show run

show log

show ip ospf

show ip ospf neighbor

show ip ospf interface

show ip ospf border-routers

show ip ospf spf

show ip ospf route count

show ip ospf route

show ip ospf database database-summary

show ip ospf database

show ip ospf database router

show ip ospf database network

show ip ospf database summary

show ip ospf database asbr-summary

show ip ospf database external

show ip ospf database nssa-external

Debug ip ospf lsa
```

Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time.

4.3 Troubleshooting the routing entry default

4.3.1 Fault Symptom

The OSPF database contains an LSA, but the routing table does not contain the corresponding route entry.

4.3.2 Possible Causes

1) The switch configurations have problems, for example, route filtering is configured and the network types do not match.

2) The network environment has problems, for example, better routes are available.
3) When the FA address is not 0, the route is not learned from OSPF. If the FA address is not 0, the route with the smallest metric to the FA address is preferred and the route to the FA address must be an intra-domain or inter-domain OSPF route; otherwise, the route entry will be ignored.

4.3.3 Troubleshooting Procedure

Step1: Check switch configurations.

1.Check whether the network types match.

If the network types at the two ends of a neighbor do not match, the routing table cannot be correctly loaded.

2.Check whether route filtering is configured.

If the **distribute-list in** table filters routes incorrectly, the routes cannot be added the routing table (distribute-list is used to filter routes).

3.Check whether the routing loop prevention function is enabled.

If the loop prevention function is enabled and a VPN route carries DN-Bit or the Route Tag value of an LSA is the same as that at the local end in an L3VPN environment, check whether the requirements for loop prevention are met.

Step2: Check the network environment.

1.Check whether better routes are available.
2.Check whether the routes in the routing table are better than the OSPF route, namely, the administrative distance is smaller than the OSPF route, which causes that the OSPF

route cannot be added into the routing table.

3.Check whether the route to the FA address is reachable.

When a router receives a Type 7-to-Type 5 LSA, the router finds that the routing table has no route to the FA address (not 0), which causes that the Type 5 LSA route cannot be added into the routing table.

Possible cause: Route filtering (distribute-list in) is configured, which filters the routes to the FA address.

Step3: Check the FA addresses.

For type-5 LSAs of OSPF, there are two types of FA addresses:

1) If OSPF imports an external route and the FA address of the generated type 5 LSA is 0.0.0.0, other routers will calculate the next-hop address of the external route by considering how to reach ASBR (namely, the router that generates the type 5 LSA) in order to reach the external network.

2) If OSPF imports an external route and the FA address of the generated type 5 LSA is not 0, other routers will calculate the next-hop address of the external route by considering how to reach this FA address in order to reach the external network.

If all of the following conditions are met:

1) the egress interface of the imported external route is enabled with OSPF;

2) the egress interface of the imported external route is not passive-interface;

3) the OSPF network type for the egress interface of the imported external route is broadcast;

the FA address (not 0) of the generated Type 5 LSA is the next-hop address of the imported external route.

Note: If the FA address is not 0, the route with the smallest metric to the FA address is preferred and the route to the FA address must be an intra-domain or inter-domain OSPF route; otherwise, the route entry will be ignored.

Above all, if a Type 5 LSA route is not added into the routing table, you have two solutions:

(1) Run the **show ip route | in x.x.x.x** (FA address) command to check whether the learned address is an intra-domain or inter-domain address. If not, the route will not be added into the routing table.

(2) Disable OSPF on the egress interface of the ASBR.

Step4: Fault Information Collection

Collect log information (pay attention to the time switch and the time accuracy) for fault analysis.

[Device debugging information, configuration, hardware and software versions, device logs and operation logs]

Collecting basic information

show version

show version slots

show run

show log

show ip interface brief

show interface status

show interface counter sum

show interface counter rate

show interfaces counters errors

show interfaces counters

show arp counter

show arp

show arp detail

show mac-address-table

show mac-address-table counter

show ip route

show ip route count

show memory

dir

show vlan

show cpu

show cpu-protect mb

show cpu-protect

show cpu-protect slot X //X indicates the slot ID, for example, slot 4 of the standalone device S8610: show cpu-pro slot 4; for example, slot 4 of chassis 2 in the VSU: show cpu-pro slot 2/4

show cpu-protect slot X //X indicates the slot ID, for example, slot 4 of the standalone device S8610: show cpu-pro slot 4; for example, slot 4 of chassis 2 in the VSU: show cpu-pro slot 2/4

show spanning-tree

show spanning-tree summary

Collecting OSPF information

show ip ospf

show ip ospf neighbor

show ip ospf interface

show ip ospf border-routers

show ip ospf spf

show ip ospf route count

show ip ospf route

show ip ospf database database-summary

show ip ospf database

show ip ospf database router

show ip ospf database network

show ip ospf database summary

show ip ospf database asbr-summary

show ip ospf database external

show ip ospf database nssa-external

show memory protocols

Collecting OSPF dynamic information

1. Ruijie#debug ip ospf route ase

Ruijie#clear ip ospf ase //(Note: This command is a hidden command.) undebug all: disables debugging.

2. Ruijie#show ip route //Check whether the route is available. If not, go to step 3; otherwise, stop collecting information.

3. Ruijie#debug ip ospf route spf

Configure the cost value on an interface enabled with OSPF ((config-if)# mode): ip ospf cost 99

Wait for 10 seconds.

Restore the configuration: no ip ospf cost (If the cost value is configured originally, it is reset to ip ospf cost xxx, where xxx indicates the originally configured value)

undebug all: disable debugging.

4. Ruijie#show ip route //Check whether the route is available. If not, go to step 5; otherwise, stop collecting information.

5. Ruijie#clear ip ospf process

6. Ruijie#show ip route //Check whether the route is available.

⚠ Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time.

4.4 Troubleshooting BGP Routes learning abnormally

4.4.1 Fault Symptom

Faults can be classified to the following types based on whether abnormal routes are BGP routes originated by the local device:
1) Exception occur in learning of local BGP routes.
2) Exception occur in learning of neighbor BGP routes.
Local BGP routes refer to routes imported to BGP by the **network** or the **redistribute** command. When a fault occurs, the BGP routing table does not contain these routes. Routes advertised to the local device by neighbors are also called dynamic routes. When a fault occurs, the BGP routing table or the routing table does not contain these routes.

4.4.2 Possible Causes

1.Possible causes for an exception occurring in learning of a local BGP route include that the routing table does not contain this route and that the route-map filters certain routes.
Faults occurring in neighbor route learning are classified into the following types based on whether BGP neighbors are established:
2.Neighbor sessions are not normally established. In this case, possible causes for the faults include incorrect configurations, network faults or other software faults.
3.Neighbor sessions are normally established. In this case, possible causes for the faults include that the neighbors do not advertise these routes, that certain attributes of the BGP routes advertised by the neighbors are abnormal (for example, the next hop is unreachable, router-IDs are in conflict, and AS path loops occur), and that the BGP routes are filtered or

suppressed by certain configurations.

4.4.3 Troubleshooting Procedure

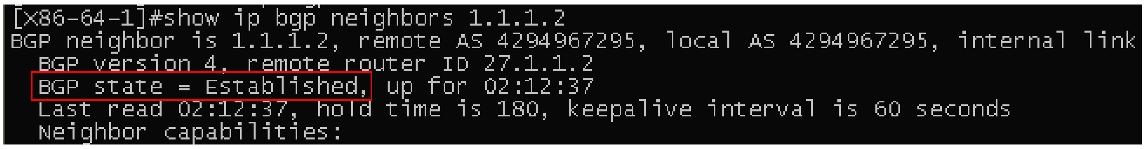
Step 1: Check the neighbor status.
Step 2: Check the route status.
Step 3: Collect information and contact ruijie post-sale for support.

Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time.

Step1: Check the neighbor status.

1) Run the **show ip bgp neighbor A.B.C.D** command to check the neighbor status. If "BGP state = Established" is displayed, it indicates that the neighbor is successfully established. See the following information:



```
[X86-64-1]#show ip bgp neighbors 1.1.1.2
BGP neighbor is 1.1.1.2, remote AS 4294967295, local AS 4294967295, internal link
  BGP version 4, remote router ID 27.1.1.2
  BGP state = Established, up for 02:12:37
  Last read 02:12:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
```

Related commands:

show bgp ipv4 unicast neighbor

//Displays the IPv4 unicast neighbor and has the same effect as **show ip bgp neighbor**.

show bgp ipv6 unicast neighbor

//Displays the IPv6 unicast neighbor.

show bgp vpnv4 unicast all neighbor

//Displays all VPN neighbors including PE neighbors of a public network and CE neighbors of a private VRF.

2) If the BGP neighbor fails to be established, continue locating the fault:

- Check whether the configurations on the local and neighbor devices are correct.

  The two ends must be configured with symmetric neighbor A.B.C.D remote-as as-number.

  In addition, the remote-as number must be correct.

- Check whether neighbor A.B.C.D update-source needs to be configured:

  Generally, update-source must be specified for IBGP neighbors.

  Extremely, when multiple pairs of BGP neighbors are established between two devices, update-source must be specified.

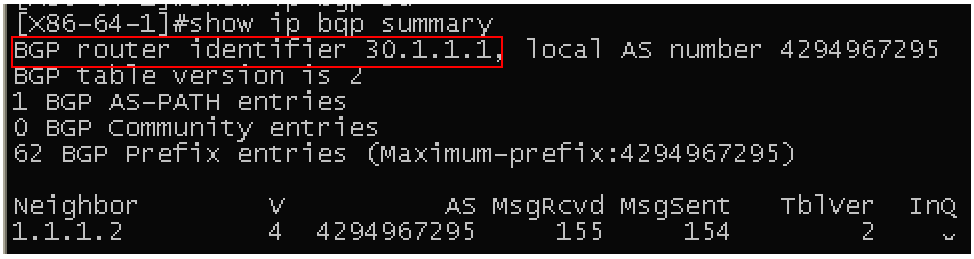
- Ping the IP address of the neighbor device to check whether the network connection is normal (If the neighbor device is configured with update-source, ping the IP address of the neighbor device with the source).

  If the neighbor device fails to be pinged, run the **show ip/ipv6 route** command on both devices to check whether the local device has a route that can reach the neighbor device.

- If the neighbor device can be successfully pinged but the neighbor cannot be established, check whether ebgp-multihop needs to be configured for the neighbor device.

  For non-directly-connected EBGP neighbors, ebgp-multihop must be configured.

- Check whether the router ID of the neighbor device is in conflict. Run the **show ip bgp summary** command to display the local router ID.



```
[X86-64-1]#show ip bgp summary
BGP router identifier 30.1.1.1, local AS number 4294967295
BGP table version is 2
1 BGP AS-PATH entries
0 BGP Community entries
62 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor          V          AS MsgRcvd MsgSent   Tblver  InQ
1.1.1.2           4  4294967295     155     154        2
```

- Check whether the neighbor configurations at both ends contain the IP address family.

3) If the neighbor is successfully established but no route can be learned, you need to further check whether the neighbor device supports the IP address family capability. Run the **show ip bgp neighbor** command for checking:

A BGP neighbor can support multiple IP address families. Only when negotiation about an IP address family capability succeeds, the routes corresponding to the IP address family can be learned. The negotiation results are as follows:

- advertised: The local device has an activated capability but the neighbor device has no activated capability; therefore, the negotiation fails.
- received: The local device has no activated capability but the neighbor device has an activated capability; therefore, the negotiation fails.
- advertised and received: Both the local and neighbor devices have activated capabilities; therefore, the negotiation succeeds.

Step2 : Check the route status.

If a BGP neighbor is normal but no route is learned, there are two possible causes: a) The BGP route fails to be learned; b) The BGP route is learned but fails to be calculated.

1) Check whether the BGP route is available in the routing table by running the **show ip bgp A.B.C.D** command.

Related commands:

show bgp ipv4 unicast A.B.C.D

Displays the IPv4 unicast route and has the same effect as **show ip bgp A.B.C.D**.

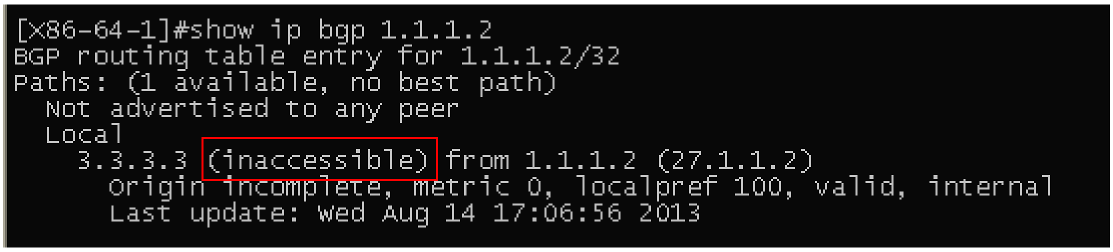
show bgp ipv6 unicast X:X::X::X/XX

Displays the IPv6 unicast route.

show bgp vpnv4 unicast all A.B.C.D

Displays the VPN route, as well as the VPNv4 route of a public network and the route of a private VRF.

2) If the BGP route exists but is unavailable in the routing table, it indicates that the route fails to be calculated. See the following information:



```
[x86-64-1]#show ip bgp 1.1.1.2
BGP routing table entry for 1.1.1.2/32
Paths: (1 available, no best path)
  Not advertised to any peer
  Local
    3.3.3.3 (inaccessible) from 1.1.1.2 (27.1.1.2)
      Origin incomplete, metric 0, localpref 100, valid, internal
      Last update: Wed Aug 14 17:06:56 2013
```

"inaccessible" indicates that the next-hop of the route is inaccessible. Such a BGP route cannot be calculated.

You need to check whether a valid IGP route to the next hop is available, for example, a route shown in the preceding figure. Run the **show ip route 3.3.3.3** command for checking.

3) If the BGP route does not exist, it indicates that no route is learned from the neighbor. You need to repeat the operation in step 2 on the peer device to check whether the route is available on the neighbor device.

If the route is also unavailable on the neighbor device, you need to further locate the fault upward.

4) Enable debugging to check whether the local device receives a route advertisement packet from the neighbor device.

debug ip bgp update in, debug ip bgp warn: enables debugging.

clear ip bgp peer-ip soft in: soft resets a BGP session to enable the neighbor to advertise the route again.

Related commands:

clear bgp ipv4 unicast A.B.C.D soft in

Soft restarts the ingress route of the IPv4 unicast neighbor and has the same effect as **clear ip bgp A.B.C.D soft in**.

clear bgp ipv6 unicast X:X::X::X soft in

Soft restarts the ingress route of the IPv6 unicast neighbor.

clear bgp vpnv4 unicast A.B.C.D soft in

Soft resets the ingress route of the VPNv4 neighbor.

If the local device receives this route, check the route filtering information: "Peer-IP-incoming/outgoing [RIB] Update: Prefix A.B.C.D/32 denied due to Reason". Where, **Reason** is a string, which can be:

a) **"attr comon check fail"**

Indicates that an invalid field is found in packet decoding and the route is filtered. For such an error, more information will be displayed to show the invalid field, for example:

i) "%s-%s [DECODE] Attr OrigID: OrigID(%r) same as Self, Ignoring UPDATE..." The route Originate-id is the local device, and a routing loop occurs.

ii) "%s-%s [DECODE] Attr Cluster: my cluster-id in the cluster-list" The route cluster-id includes the local device and a routing loop occurs.

iii) "%s-%s [DECODE] Update: Invalid Nexthop: %r" The next hop of the route is an invalid IP address or is an interface IP address of the local device.

b) **"MPLS VPN/BGP implicit inbound filter"**

Indicates that the RT attribute of the L3VPN or L2VPN fails to be matched. You need to check whether the import route-target configuration of the local VRF or VFI is correct.

c) **"as-path contains our own AS"**

Indicates that an AS-PATH loop occurs.

d) **"filter"**

Indicates that the route is filtered by the ingress policy. You need to check the ingress filtering policies of the neighbor, including filter-list, prefix-list, and distribute-list.

e) **“route-map”**

Indicates that the route is filtered by the route-map in configuration. You need to check the route map configuration.

f) **“non-connected next-hop”**

Indicates that the next hop of the IPv4 route received from the directly-connected EBGP neighbor is not a directly-connected interface. You need to check the network configurations.

g) **“max prefix overflow”**

Indicate that the route received from the neighbor exceeds the max limitation, which causes overflow. You need to check the neighbor configuration and the received route entry (show ip bgp summary) to check whether overflow occurs.

h) **“address-family overflow”**

Indicates that the total capacity of the routing table in the IP address family is abnormal. You need to check the maximum-prefix configuration in the BGP address family.

5) If the local device does not receive the route update message in the previous step, it indicates that the neighbor device does not advertise the route. You need to perform debugging on the neighbor device.

1. Run the **show** command to check the route status, such as **show ip bgp A.B.C.D**.

a) "(inaccessible)": indicates that the route calculation fails. You need to check whether the next hop calculation of the route fails.

b) "(suppressed due to dampening)": indicates that the local device is enabled with the dampening function and the route is suppressed by flapping. You need to check whether the network flaps all the time.

c) Check the community attributes of the route and check whether attributes that suppress route advertisement such as No_Export, Local_AS and NO_Advertise are included.

Related commands:

show bgp ipv4 unicast A.B.C.D

Displays the IPv4 unicast route and has the same effect as show ip bgp A.B.C.D.

show bgp ipv6 unicast X:X::X::X/XX

Displays the IPv6 unicast route.

show bgp vpnv4 unicast all A.B.C.D

Displays the VPN route, as well as the VPNv4 route of a public network and the route of a private VRF.

2. Check whether a route aggregation is configured and whether the route aggregation

carries the **summary-only** option. If yes, the route will be normally suppressed. To enable the neighbor device to learn the route, you need to cancel the **summary-only** parameter or configure unsuppress-map for this neighbor on the local device.
You can also run the **show ip bgp** command to display the route suppressed by the **summary-only** parameter, which is marked with "s" at the front. (This **show** command can be used in only a few routing states).

3. If the previous two steps can determine that the route is not suppressed, you need to debug other causes for suppression of the route advertisement.

```
debug ip bgp update out
```

```
debug ip bgp filter
```

```
debug ip bgp warn
```

Enable the preceding debugging functions.

4. clear ip bgp peer-ip soft out

Soft resets the BGP session and advertises the route to the neighbor again.

Related commands:

```
clear bgp ipv4 unicast A.B.C.D soft out
```

Soft restarts the egress route of the IPv4 unicast neighbor and has the same effect as **clear ip bgp A.B.C.D soft out**.

```
clear bgp ipv6 unicast X:X::X::X soft out
```

Soft restarts the egress route of the IPv6 unicast neighbor.

```
clear bgp vpnv4 unicast A.B.C.D soft out
```

Soft resets the egress route of the VPNv4 neighbor.

Determine the cause for route advertisement failure according to the debugging information as follows:

a) "%s-%s [RIB] Announce Check: %O Originator-ID is same as Remote Router-ID"

The Originate-ID of the route is the same as the neighbor device and the route loop is suppressed.

b) "%s-%s [RIB] Announce Check: %O site-of-origin is same as peer site"

The SOO attribute of the route is the same as the neighbor device and the route loop is suppressed.

c) "%s-%s [RIB] Announce Check: %O is denied by out filter"

The route is filtered by the egress policy. You need to check the neighbor configurations, including filter-list, prefix-list, and distribute-list.

d) "%s-%s [RIB] Announce Check: %O No announcement since AS %u is in AS Path"

A loop is detected along the AS-PATH.

e) "%s-%s [RIB] Announce Check: %O is denied by unsuppress-map"

A route in the suppress state is successfully matched by the unsuppress-map configuration of the neighbor.

f) "%s-%s [RIB] Announce Check: %O is denied by out routemap"

The route is filtered by the route-map out configuration. You need to check the route-map configuration.

Step4. Fault Information Collection

Collect log information (pay attention to the time switch and the time accuracy) for fault analysis.

[Device debugging information, configuration, hardware and software versions, device logs and operation logs]

Collecting basic information

```
show version

show version slots

show run

show log

show ip interface brief

show interface status

show interface counter sum

show interface counter  rate

show interfaces counters errors

show interfaces counters

show arp counter

show arp

show arp detail

show mac-address-table

show mac-address-table counter
show ip route
show ip route count
show memory
dir
show vlan
show cpu
show cpu-protect mb
show cpu-protect
```

show cpu-protect slot X (For switches S7600, S8600 and S12000, CPP statistics information should be collected twice for each line card.)

```
show spanning-tree
show spanning-tree summary
```

Collecting BGP information.

```
show ip bgp neighbor A.B.C.D
show bgp ipv4 unicast neighbor
show bgp ipv6 unicast neighbor
show bgp vpnv4 unicast all neighbor
show ip bgp summary
show ip/ipv6 route
show bgp ipv4 unicast A.B.C.D
show bgp ipv6 unicast X:X::X::X/XX
show bgp vpnv4 unicast all A.B.C.D
```

4.5 Troubleshooting BGP flapping

4.5.1 Fault Symptom

BGP route flapping occurs, routes are constantly added and deleted, LSAs are constantly refreshed, and the CPU usage is high.

Note: BGP route flapping is classified into flapping of routes originated by a local device and flapping of routes advertised by a neighbor. If BGP route flapping suppression is enabled, the route flapping advertisement from an EBGP neighbor will be suppressed and the route will not be sent to the routing table.

4.5.2 Possible Causes

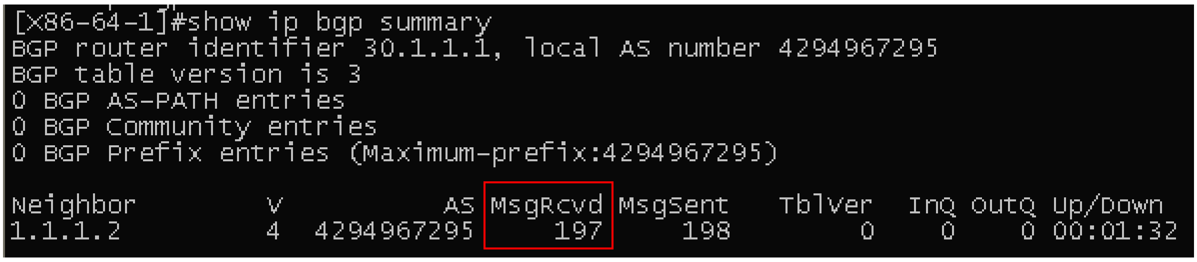
Flapping of a route originated by a local device is often caused by flapping of a local IGP route or directly-connected route. You can locate the fault by referring to the related manual; otherwise, the fault may be a software fault.

Causes for flapping of routes advertised by a neighbor are complex. Routes advertised by a neighbor can be learned by the BGP route table only after the routes are processed locally; therefore, the fault may be caused by flapping of local IGP routes, flapping of neighbor routes, or software faults.

4.5.3 Troubleshooting Procedure

Step1: Check whether the number of packets advertised by a neighbor is abnormal.

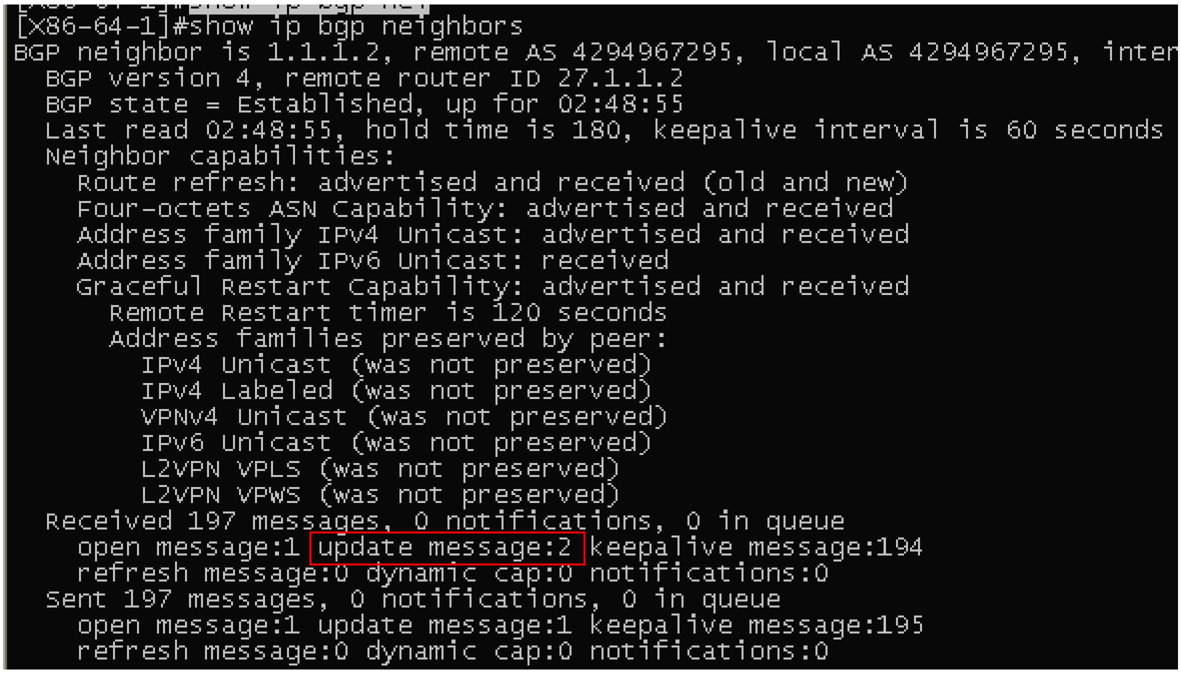
Run the **show ip bgp summary** command for multiple times to check whether the number of packets advertised by the neighbor increases normally.



```
[X86-64-1]#show ip bgp summary
BGP router identifier 30.1.1.1, local AS number 4294967295
BGP table version is 3
0 BGP AS-PATH entries
0 BGP Community entries
0 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor          V          AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
1.1.1.2           4  4294967295     197     198        0    0    0 00:01:32
```

The default BGP keepalive timeout duration is 60 seconds, that is, a packet is normally received every second. If the increase speed of packets received by the neighbor obviously exceeds this frequency, it indicates that flapping of routes advertised by the neighbor occurs.

You can also run the **show ip bgp neighbor** command to display the detailed packet statistics about the neighbor as follows:



```
[x86-64-1]#show ip bgp neighbors
BGP neighbor is 1.1.1.2, remote AS 4294967295, local AS 4294967295, inter
  BGP version 4, remote router ID 27.1.1.2
  BGP state = Established, up for 02:48:55
  Last read 02:48:55, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast (was not preserved)
        IPv4 Labeled (was not preserved)
        VPNv4 Unicast (was not preserved)
        IPv6 Unicast (was not preserved)
        L2VPN VPLS (was not preserved)
        L2VPN VPWS (was not preserved)
  Received 197 messages, 0 notifications, 0 in queue
    open message:1 update message:2 keepalive message:194
    refresh message:0 dynamic cap:0 notifications:0
  Sent 197 messages, 0 notifications, 0 in queue
    open message:1 update message:1 keepalive message:195
    refresh message:0 dynamic cap:0 notifications:0
```

If the received UPDATE packets continually increase, it indicates that the neighbor device constantly advertises route updates, which causes local route flapping.

Step2: Check whether flapping occurs in local route calculation.

If it is confirmed that the route flapping is not caused by neighbor advertisement in the previous step, it indicates that flapping occurs in local route calculation.

Run the **show ip bgp A.B.C.D** command to check the BGP flapping route. Run the **show** command for multiple times to check the status change before and after the flapping occurs. There are two situations:

1) The next hop of the BGP route constantly switches between the valid and invalid states, which is often caused by flapping on the next hop route (IGP route).

You can run the **show ip route A.B.C.D** command to display the status of the IGP route corresponding to the next hop of the BGP route. Run the **show** command for multiple times to check whether flapping occurs.

2) The BGP route has multiple next hops, and the best route switches between the multiple next hops.

a) This fault may also be caused by the valid status change of the next hop of the BGP route. You can run the **show ip route A.B.C.D** command to check the IGP route corresponding to the next hop for verification.

b) The BGP route is constantly updating, which affects the original calculation result.

Compare multiple output results of the **show ip bgp A.B.C.D** command to check whether the route changes. If the route changes, check whether the neighbor device advertises route updates. If the route change is not caused by route updates advertised by the neighbor device, there are two possible causes:

1) The local device is configured with route redistribution. Redistributed routes are constantly added and deleted. You can enable **debug ip bgp nsm** for verification.

2) There are software bugs, which causes that BGP constantly modifies route attributes when scanning routing tables. In this case, you need to run the **show ip bgp A.B.C.D** command to display the attributes that are constantly changed. Contact related support personnel.

Step3: Check whether the route flapping is caused by neighbor advertisement.

If the route flapping is caused by neighbor advertisement, you need to locate the fault on the neighbor device and check whether the neighbor device constantly advertises route update. There are also two situations:
1) The neighbor device receives route updates from higher-layer devices. You need to locate the fault upward layer by layer.
2) The local route calculation of the neighbor device changes. You need to locate the fault by repeating step 2.

Step4:Fault Information Collection

Collect log information (pay attention to the time switch and the time accuracy) for fault analysis.
[Device debugging information, configuration, hardware and software versions, device logs and operation logs]

Collecting basic information

show version

show version slots

show run

show log

show ip interface brief

show interface status

show interface counter sum

show interface counter rate

show interfaces counters errors

show interfaces counters

show arp counter

show arp

show arp detail

show mac-address-table

show mac-address-table counter

show ip route

show ip route count

show memory

dir

show vlan

show cpu

show cpu-protect mb

show cpu-protect

show cpu-protect slot X (For S76, S86 and S12000 switches, CPP statistics must to be collected for twice for each line card.)

show spanning-tree

show spanning-tree summary

Collecting BGP information

show ip bgp neighbor A.B.C.D

show bgp ipv4 unicast neighbor

show bgp ipv6 unicast neighbor

show bgp vpnv4 unicast all neighbor

show ip bgp summary

show ip/ipv6 route

show bgp ipv4 unicast A.B.C.D

show bgp ipv6 unicast X:X::X::X/XX

show bgp vpnv4 unicast all A.B.C.D

4.6 Troubleshooting DHCP

4.6.1 Fault Symptom

Client workstations fail to obtain IP address or obtain incomplete information (for example, obtain only IP address without DNS information).

Choose **Start** > **Control Panel** > **Network and Sharing Center**, and click the local connection for activating a network interface card.

You can also choose **Start** > **Run**, and input **cmd** in the dialog box, and then input **ipconfig /all** in the **cmd** command line window.

Identify the fault symptom.

4.6.2 Possible Causes

1) The PC or operating system is faulty.

2) The environment has problems (such as loops or attacks)

The physical link is disconnected.

3) The device configurations are incorrect or improper, mainly including:

The DHCP Snooping trust interface is incorrect configured.

The VLAN allocation on the switch is incorrect and the IP address of the layer-3 interface is not configured on the DHCP server.

The relay function is not enabled on the layer-3 interface.

No IP address pool is configured on the DHCP server or the IP address pool is configured with excluded addresses, which causes that no available IP addresses in the IP address pool.

The lease time configured for the DHCP server is too long, and no IP addresses can be released.

The network segment configuration for the IP address pool of the DHCP server is incorrect.

The switches are not enabled with DHCP.

4) The performance of the DHCP server is inadequate.

5) The software version has defects.

6) The DHCP architecture is incorrect:

When the DHCP relay and DHCP Snooping are deployed on the network of the customer, the enabling positions are improper, which causes that the client cannot obtain DHCP normally.

Cause: The DHCP relay will modify the source MAC address (modify to the MAC address of the dhcp relay) of a DHCP packet sent by the PC. If the DHCP relay is deployed before dhcp snooping device, the DHCP packet will be discarded by the snooping device.

Correct architecture deployment:

(1) Deploy the DHCP Snooping and DHCP relay function on the same device, eg, PC – Device(deploy DHCP Snooping and DHCP Relay simultaneously)–Device(deploy DHCP

Server).

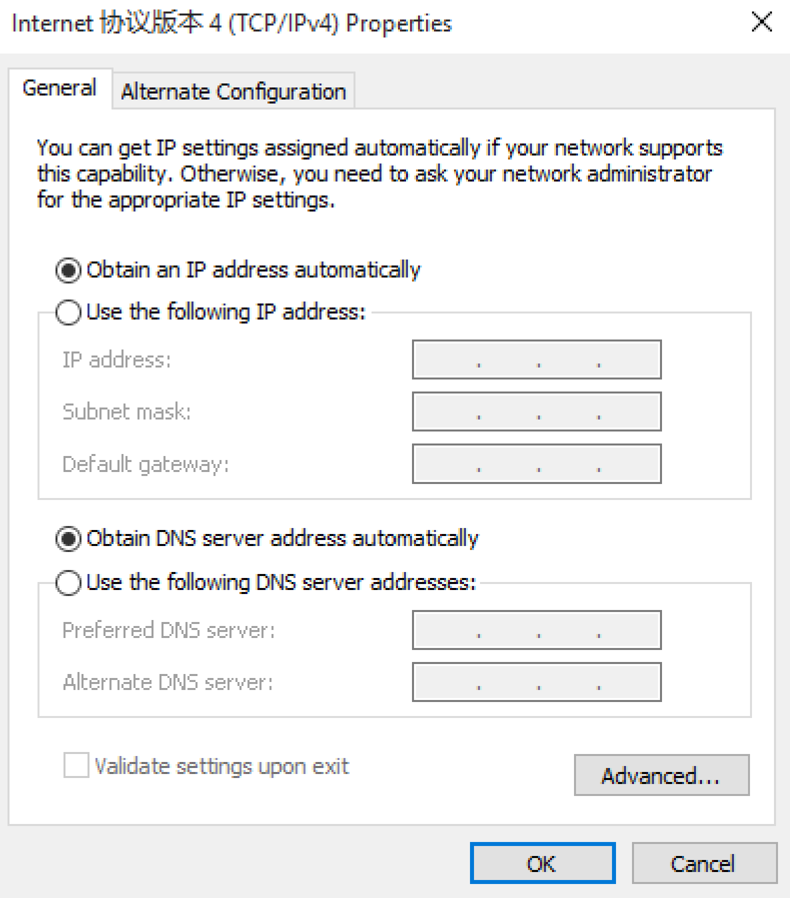
(2) Deploy DHCP Snooping on the downlink device of the DHCP relay, eg,PC -- Device(deploy DHCP Snooping) -- Device(deploy DHCP Relay) -- Device(deploy DHCP Server).

4.6.3 Troubleshooting Procedure

Step 1: Check the client and operating system.
Step 2: Check the network environment.
Step 3: Check whether the network device configurations are correct.
Step 4: Check whether the performance of the DHCP server is adequate.
Step 5: Check the software versions of network devices.
Step 6: Collect information and contact ruijie post-sale for help.

Step1: Check the client and operating system.

1. Identify the fault symptom and check whether the client is configured to dynamically obtain IP addresses. As shown in the following picture.



Internet 协议版本 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

2. Check whether a single client or many clients fail to obtain IP addresses automatically. If many clients fail to obtain IP addresses, go to the next step.

If this fault occurs only on a single client, you can install packet capturing software on the PC, or perform mirroring and packet capturing on the access switch to check whether the PC sends DHCP discover packets normally.

If not, you can attempt to disable and then enable the network interface card. For a diskless system, it is recommended to make a diskless server system.

If DHCP discover packets can be normally sent, retain the packets captured and go to the next step.

Step2: Check the network environment.

1. Check whether the physical link between the client and server is normal.

Configure the PC to use a static IP address and gateway. If you are sure that the switch is not configured with the IP source-guard function, ping the IP address of the server to check the connection. If the IP address can be successfully pinged, the delay is smaller than 100ms, and no packet loss or jitter occurs, it indicates that the connection is normal, namely, the physical link is not faulty. Go to the next step for fault locating. If the IP address fails to be pinged, the delay is large, or packet loss occurs, it indicates that the physical link is faulty or the server is unstable due to environment problems. In this case, you need to perform packet capturing from the client to the DHCP server node by node to identify the cause for the packet loss or large delay.

2. Check whether the link is disconnected. If yes, correctly connect the interfaces. Check whether the route of the devices is correct. If not, adjust the route.

If the fault persists, check whether the CPU usages of the switches along the route are high, especially when a device is used as the DHCP server. If the CPU usage of a switch is high, locate the cause by using <<>>.

If the fault still persists, go to the next step.

Step3: Check whether the configurations of network device are correct.

In a DHCP network, devices are classified into the DHCP relay, DHCP server and DHCP Snooping. DHCP Snooping ensures DHCP security and prevents static IP configuration, which can be used together with DAI to prevent ARP spoofing. A device may have one or more roles in the network(for example, a device can be configured as dhcp server and dhcp snooping simultaneously). Check whether the basic configurations are correct by using the following methods.

1. Log in to an access switch through the Console port, and then run the **show run** command to display the configurations.

2. Compare the following typical configurations to check whether the DHCP configurations of the device are correct.

Recommended configurations when a Ruijie switch is used as a DHCP server:

1) Enable DHCP.

```
Ruijie(config)#service dhcp
/*DHCP must be configured on the switch.*/
```

2) Configure the DHCP address pool.

```
Ruijie(config)#ip dhcp pool vlan2
/*Create a DHCP address pool named valn2.*/
Ruijie(dhcp-config)#lease 1 2 3
/*1, 2 and 3 indicate one day, tow hours and three minutes respectively. The default period for releasing the IP address of a Ruijie switch is 24 hours.*/
Ruijie(dhcp-config)#network 192.168.2.0 255.255.255.0
/*The IP addresses that can be assigned are in the range of 192.168.2.1~192.168.2.253.*/
Ruijie(dhcp-config)#dns-server 8.8.8.8    6.6.6.6
/*8.8.8.8 is the primary DNS and the 6.6.6.6 is the secondary DNS.*/
Ruijie(dhcp-config)#default-router 192.168.2.254
/*Configure the gateway IP address.*/
Ruijie(dhcp-config)#exit
Ruijie(config)#ip dhcp pool vlan3
Ruijie(dhcp-config)#network 192.168.3.0 255.255.255.0
Ruijie(dhcp-config)#dns-server 8.8.8.8
Ruijie(dhcp-config)#default-router 192.168.3.254
Ruijie(dhcp-config)#exit
```

3) Reserve certain IP addresses.

```
Ruijie(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
/*The IP addresses 192.168.2.1~~192.168.2.10 will not be assigned to clients.*/
```

4) Configure the DHCP IP addresses to be statically assigned.

```
Ruijie(config)#ip dhcp pool test
Ruijie(dhcp-config)# client-identifier 01bc.aec5.4bca.8d
/*Add the Ethernet flag 01 to the fixed MAC:bcae.c54b.ca8d, which will be 01bc.aec5.4bca.8d.*/
Ruijie(dhcp-config)# host 192.168.2.2 255.255.255.0
/*Configure IP address and mask.*/
Ruijie(dhcp-config)# dns-server 8.8.8.8 6.6.6.6
```

/*Configure primary DNS8.8.8.8 and secondary DNS 6.6.6.6.*/

```
Ruijie(dhcp-config)# default-router 192.168.2.254
```

/*Assigned gateway.*/

```
Ruijie(dhcp-config)#ip dhcp excluded-address 192.168.1.1 192.168.1.100
```

*/*The 100 IP addresses 1.1---1.100 are excluded and cannot be assigned.*/*

5) Recommended configurations when a Ruijie switch is used as a DHCP relay:

Enable DHCP.

```
Ruijie(config)#service dhcp
```

Configure the DHCP relay.

```
Ruijie(config)#ip helper-address 172.16.1.2
```

/*172.16.1.2 is the IP address of the DHCP server.*/

Notes

- A DHCP relay must be configured if the DHCP server and the user gateway are not in the same network segment. This configuration example does not include the configuration of a layer-3 interface. Generally, the relay is configured on a layer-3 gateway either based on a layer-3 interface or globally in the system. If the relay (ip helper-address) is configured both based on the layer-3 interface and globally in the system, the relay IP address configured based on the interface is used as the server IP address in priority; However, global configuration is sufficient.
- A switch will put the IP address of the layer-3 interface into DHCP packets as the relay IP address and convert the packets into unicast packets. Generally (except that the DHCP server is configured with IP address assignment based on the Option field), the DHCP server assigns an IP address in the same segment as the relay IP address to a PC. On a layer-2 switch (such as S21 switch), only one management IP address segment is activated by default; therefore, it is not recommended to enable the relay configuration except for IP address assignment in the DHCP Option field.

Recommended configurations when a Ruijie switch is used as a DHCP Snooping:

Enable DHCP Snooping on an access switch.

```
Ruijie(config)#ip dhcp snooping
```

/*Enable DHCP Snooping.*/

Configure the interface for connecting to the DHCP server as a trust interface.

```
Ruijie(config)#int FastEthernet0/24
Ruijie(config-FastEthernet 0/24)#ip dhcp snooping trust
```

/*All interfaces of a switch enabled with DHCP Snooping are untrust interfaces by default. The switch forwards only DHCP response packets (offer, ACK and NAK) received from a trust interface.Therefore, you must ensure that the interface for connecting to the DHCP server in the uplink is enabled with trust.*/

Configure the **dhcp snooping ver mac-address** command in global configuration mode.

```
Ruijie(config)#ip dhcp snooping verify mac-address
```

/*It is recommended to enable prevention against IP address exhaustion attacks. If the source MAC addresses are not matched with MAC addresses in the Client field, DHCP request packets will be discarded.*/

Notes

- For other optional configurations such as preventing users from manually setting IP addresses and preventing ARP spoofing, refer to the settings in the Typical Configuration Cases About Ruijie Middle- and Low-End Switches. When faults occur, ensure that users can obtain IP addresses by using the simplest configurations.

3.Check whether the DHCP configurations of the device are correct based on the preceding typical configurations and whether users can obtain IP addresses dynamically by using the simplest configurations.

Focus on the following configurations in checking:

- The trust interface of the DHCP Snooping is configured only on the uplink interface. If it is not configured, add the trust configuration of the uplink interface.
- Ensure that the VLANs corresponding to the user network segments are correctly assigned on the switch and that the network segments corresponding to layer-3 interfaces are within the IP address pool on the DHCP server and are not configured as excluded IP addresses (ip dhcp excluded-address. If they are configured as excluded IP addresses, there will be no IP addresses in this segment that can be assigned in the IP address pool.)
- If the DHCP server and the user gateway are not in the same network segment, ensure that the relay function is enabled based on a layer-3 interface or globally. Check whether there is a route between the relay and server. If yes, ensure that the route is normal.
- For scenarios that are frequently changed such as the hotel industry, it is recommend you set the lease period within 24 hours to avoid that IP addresses cannot be released due to long lease period of the DHCP server.
- The network segment configurations of the gateway and DNS corresponding to the IP address pool of the DHCP server must be correct.

If the fault still persists, go to the next step.

Step4: Check whether the performance of the DHCP server is adequate.

1. Check whether the capacity and performance of the DHCP server are exceeded.
2. Check whether there are available IP addresses in the address pool.

Run the **show ip dhcp server statistics** command to check whether there are available IP addresses in the address pool.

If there are no available IP addresses, run the **clear ip dhcp conflict** command to check whether there are IP addresses that have expired and whether the IP addresses and the interface IP addresses are in the same network segment.

If there are no IP addresses that have expired, run the **show ip dhcp conflict** command to check whether there are IP addresses in conflict, which causes that the IP addresses are unavailable. If many entries are found, you can run the **clear ip dhcp conflict** command for clearing and then check whether there are IP addresses in conflict by obtaining IP addresses.

After the preceding steps are completed, if there are no IP addresses that are available, have been expired and are in conflict in the address pool, it indicates that the IP addresses in the address pool are exhausted.

3. Increase available IP addresses in the address pool.

Step5: Collect fault information and submit the case to the service portal.

If the fault still persists, collect the following information (recorded operation results and logs) and submit the fault to the service portal (case.ruijienetworks.com) for further handling.

```
show runn

show log

show dhcp lease

show ip dhcp binding

show ip dhcp conflict

show ip dhcp server statistics
```

Collect the logs recorded during fault locating, and packets captured when the client obtains IP address via DHCP server.

5. Redundancy and reliability

5.1 Troubleshooting ERPS

5.1.1 Fault Symptom

Network failure occurs in an ERPS ring network (single ring or intersecting ring).

5.1.2 Possible Causes

1) Configurations are incorrect, for example, the device is not configured with the RPL owner node or device is configured with RPL owner nodes.
2) Operations are incorrect, for example, incorrect operations cause loops.
3) The ERPS ring cannot be stabilized to the idle state.

5.1.3 Troubleshooting Procedure

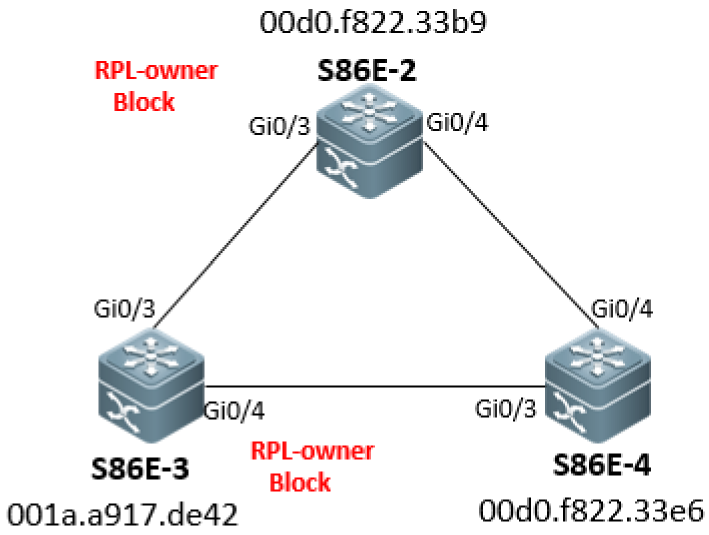
Step 1: Check the ERPS configurations of each device.
Step 2: Check operations on the ERPS ring network that may cause loops.
Step 3: Check whether the ERPS ring network can recover to the idle state.

Step1: Run the show run command to display the ERPS configurations of each device.

ERPS configuration tips:

1. Each ring has only one RPL owner node.

2. The **RPL-port** command is not required for non RPL-Owner nodes.



ERPS configurations of [S86E-2]

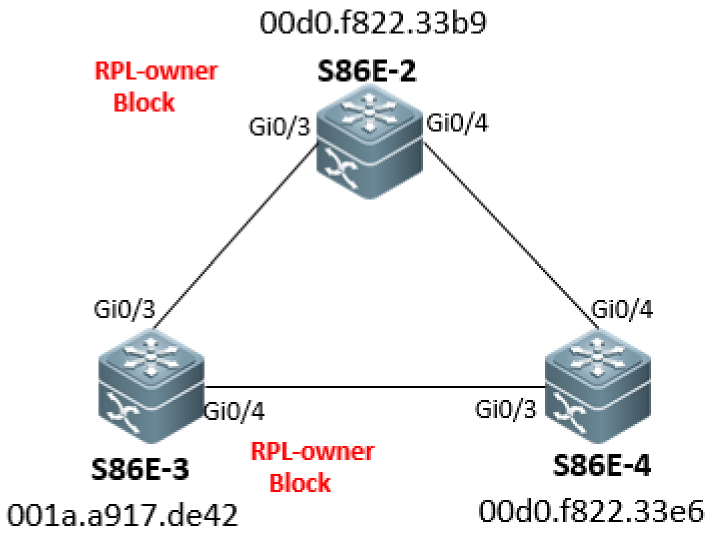
```
erps enable
erps raps-vlan 4001
  ring-port west GigabitEthernet 0/3 east GigabitEthernet 0/4
rpl-port west rpl-owner
  state enable

interface GigabitEthernet 0/3
  switchport mode trunk
  rldp port bidirection-detect shutdown-port
!
interface GigabitEthernet 0/4
  switchport mode trunk
  rldp port bidirection-detect shutdown-port
```

ERPS configurations of [S86E-3]

```
erps enable
erps raps-vlan 4001
  ring-port west GigabitEthernet 0/3 east GigabitEthernet 0/4
```

```
rpl-port east rpl-owner
  state enable

interface GigabitEthernet 0/3
  switchport mode trunk
  rldp port bidirection-detect shutdown-port
!
interface GigabitEthernet 0/4
  switchport mode trunk
  rldp port bidirection-detect shutdown-port
```

Run the **show run** command. If it is found that both devices are configured with the RPL owner node, the RPL owner node in the ERPS ring network will be Blocked, which will cause disconnection of the ring network. See the following topology.



2: Enable debug erps packet of the devices to check receiving and sending of ERPS packets.

If you cannot log into all devices to collect ERPS configurations due to network disconnection, you can run the **debug erps packet** command to check receiving and sending of ERPS packets on device S86E-2 (or S86E-4) on which RPL owner is deployed. You can check whether the MAC addresses in the R-APS (NR, RB) packets received in the same RAPS-VLAN are the same as the MAC address of the device. If not, it indicates that one ERPS ring network is configured with two RPL owner nodes.

Caution

Debugging operations cause risks (The worst case is to restart the switch for recovery). Perform debugging only after informing customers of the risks and get them accepted. It is recommended debugging at low-traffic periods (Be more cautious when dealing with core switches). If packet capturing is also required for troubleshooting, remember to collect information by debugging and packet capturing at the same time.

```
S86E-2# debug erps packet

22:23:34:35:   %7: [ERPS-PKT]:Send erps packet R-APS(NR, RB) at 198567506, raps-vlan 4001 status 0x80

22:23:34:35:   %ERPS-5-TOPOLOGY_CHANGE: Topology changed for R-APS VLAN 4001, The ring changed state from protection to idle

22:23:34:35:   %7: [ERPS-PKT]:Send erps packet R-APS(NR, RB) at 198567509, raps-vlan 4001 status 0x80

22:23:34:35:   %7: [ERPS-PKT]:Send erps packet R-APS(NR, RB) at 198567510, raps-vlan 4001 status 0x80

22:23:34:39:   %7: [ERPS-PKT]:Recv packet at 198567995, len = 60

22:23:34:39:   %7: [ERPS-PKT]:Recv erps packet R-APS(NR) at 198567995, raps-vlan 4001 ifx 4 status 0x0 node-id 001a.a917.de42

22:23:34:39:   %7: [ERPS-PKT]:Recv packet at 198567995, len = 60

22:23:34:39:   %7: [ERPS-PKT]:Recv erps packet R-APS(NR) at 198567995, raps-vlan 4001 ifx 3 status 0x0 node-id 001a.a917.de42     //Receive (NR,RB) packets from another RPL owner node. The MAC address implies that the packets are sent by device S86E-3, indicating that there is another ERPS RPL owner node in the network, namely, the network is configured with two RPL owner nodes.

S86E-2# no debug all

All possible debugging has been turned off
```

The ERPS status of each device is as follows:

Device S86E-2

```
S86E-2#sho erps

ERPS Information

Global Status                         : Enabled
```

```
Link monitored by              : Not Oam

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

R-APS VLAN                        : 4001

Ring Status                     : Enabled

West Port                        : Gi0/3           (Blocking)

East Port                       : Gi0/4           (Forwarding)

RPL Port                         : West Port

Protected VLANs                  : ALL

RPL Owner                          : Enabled

Holdoff Time                    : 0 milliseconds

Guard Time                        : 500 milliseconds

WTR Time                           : 2 minutes

Current Ring State             : idle
```

Device S86E-3

```
S86E-3#sho erps

ERPS Information

Global Status                   : Enabled

Link monitored by              : Not Oam

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

R-APS VLAN                        : 4001

Ring Status                     : Enabled

West Port                        : Gi0/3          (Forwarding)

East Port                       : Gi0/4          (Blocking)

RPL Port                         : East Port

Protected VLANs                  : ALL

RPL Owner                          : Enabled

Holdoff Time                    : 0 milliseconds

Guard Time                        : 500 milliseconds

WTR Time                           : 5 minutes
```

```
Current Ring State                : idle
```

Device S86E-4

```
S86E-4#sho erps

ERPS Information

Global Status                      : Enabled

Link monitored by                  : Not Oam

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

R-APS VLAN                            : 4001

Ring Status                         : Enabled

West Port                            : Gi0/3          (Forwarding)

East Port                           : Gi0/4          (Forwarding)

RPL Port                              : None

Protected VLANs                       : ALL

RPL Owner                               : Disabled

Holdoff Time                        : 0 milliseconds

Guard Time                            : 500 milliseconds

WTR Time                                : 2 minutes

Current Ring State                : idle
```

The preceding information shows that the Gi0/3 interface of device S86E-2 and the Gi0/4 interface of device S86E-3 are blocked, which causes that device S86E-2 cannot access device S86E-3.

3.Delete the RPL owner configuration from S86E-3, wait for 2 minutes (the WTR time period of S8600E devices is 2 minutes during which the ERPS convergence completes.), and then run the **show erps** command to display the ERPS status. After the ring status becomes stable (idle state), only the Gi0/3 interface of device S86E-2 is in the Block state.

The procedure for deleting RPL owner configurations is as follows:

1. Shut down an ERPS interface.
2. Disable ERPS of ring 4001.
3. Delete the RPL owner configuration.

4. Enable ERPS of ring 4001.

5. Enable the ERPS interface that is shut down previously.

Example: Modify the ERPS configurations of device S86E-3. The configurations are as follows:

```
SS86E-3(config)#int gi 0/4

SS86E-3(config-if)#shutdonwn

SS86E-3(config)#erps raps-vlan 4001

SS86E-3(config-erps 4001)#no state enable

SS86E-3(config-erps 4001)#no rpl-port

SS86E-3(config)#int gi 0/4

SS86E-3(config-if)#no shutdonwn
```

The ERPS status of device S86E-2 is as follows:

```
SS86E_2#show erps

ERPS Information

Global Status                    : Enabled

Link monitored by                : Not Oam

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

R-APS VLAN                          : 4001

Ring Status                       : Enabled

West Port                          : Gi0/3         (Block)

East Port                         : Gi0/4         (Forwarding)

RPL Port                           : None

Protected VLANs                    : ALL

RPL Owner                            : Disabled

Holdoff Time                      : 0 milliseconds

Guard Time                         : 500 milliseconds

WTR Time                             : 2 minutes

Current Ring State               : idle
```

The ERPS status of device S86E-4 is as follows:

```
SS86E_4#show erps

ERPS Information

Global Status                   : Enabled

Link monitored by               : Not Oam

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

R-APS VLAN                          : 4001

Ring Status                     : Enabled

West Port                        : Gi0/3            (Forwarding)

East Port                       : Gi0/4            (Forwarding)

RPL Port                          : West

Protected VLANs                   : ALL

RPL Owner                           : Disabled

Holdoff Time                    : 0 milliseconds

Guard Time                        : 500 milliseconds

WTR Time                            : 2 minutes

Current Ring State             : idle
```

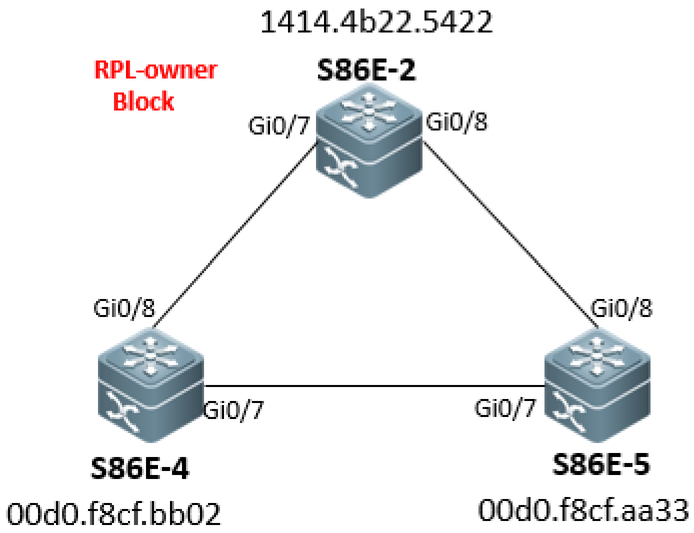
The ERPS status of device S86E-4 is as follows:

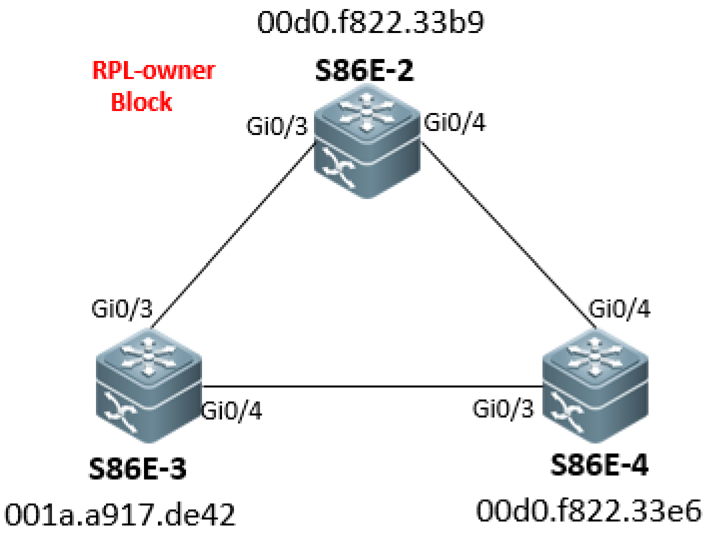
```
SS86E_4#show erps

ERPS Information

Global Status                   : Enabled

Link monitored by               : Not Oam

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

R-APS VLAN                          : 4001

Ring Status                     : Enabled

West Port                        : Gi0/3            (Forwarding)

East Port                       : Gi0/4            (Forwarding)

RPL Port                          : None

Protected VLANs                   : ALL
```

```
RPL Owner                          : Disabled

Holdoff Time                     : 0 milliseconds

Guard Time                         : 500 milliseconds

WTR Time                             : 2 minutes

Current Ring State              : idle
```

Step2: Check whether the ERPS interface is modified during the operations. If the ERPS interface is directly modified without being shut down, convergence will fail and then a loop will occur.

The topology is as follows:





The problem operation procedures are as follows:

Scenario 1: The topology is shown in the preceding figure.

1. S86E-2 is an RPL owner node in the ERPS ring. The ERPS interfaces on S86E-2 should be Gi0/3 (up) and Gi0/4 (up). However, the ERPS interfaces are configured as Gi0/3 (up) and Gi0/6 (down) incorrectly.

```
S86E-2(config)#erps raps-vlan 4010

S86E-2(config-erps 4010)#no state enable

S86E-2(config-erps 4010)#ring-port west gi0/3 east gi0/6

S86E-2(config-erps 4010)#ring-port west rpl-owner

S86E-2(config-erps 4010)#state enable
```

2. Since the Gi0/6 interface of S86E-2 is in the down state, the Gi0/3 interface sends an SF packet. Then, S86E-2 enters the protection state and needs to receive an NR packet to trigger the WRT timer and recover to the idle state.

3. On device S86E-2, modify the ERPS interface from Gi0/6 to Gi0/4. However, this configuration does not shut down the ERPS interface Gi0/3 (or Gi0/4).

```
S86E-2(config)#erps raps-vlan 4010

S86E-2(config-erps 4010)#no state enable     //Stop sending SF packets.

S86E-2(config-erps 4010)#ring-port west gi0/3 east gi0/4      //Configure the ERPS interface.

S86E-2(config-erps 4010)#ring-port west rpl-owner    //Enable ERPS without triggering NR packets, which causes that the WTR timer cannot be enabled, the ERPS control packets in the entire network are lost, ERPS convergence fails and then a loop occurs. ERPS is in the protection state and the ERPS interface is in the (Link Normal) forwarding state.
```

```
S86E-2(config-erps 4010)#state enable
```

4. The ERPS ring state modified through the preceding operations is as follows:

```
S86E-2#sho erps
ERPS Information
Global Status                  : Enabled
Link monitored by              : Not Oam
------------------------------------------
R-APS VLAN                       : 4010
Ring Status                    : Enabled
West Port                       : Gi0/3           (Forwarding)
East Port                      : Gi0/4           (Forwarding)
RPL Port                        : West Port
Protected VLANs                 : ALL
RPL Owner                        : Enabled
Holdoff Time                   : 0 milliseconds
Guard Time                      : 500 milliseconds
WTR Time                         : 2 minutes
Current Ring State             : protection
S86E-2# debug erp pa      //debug erps packet is enabled, but no packet is received, the WTR timer of ERPS is lost, and the ERPS control plane of loses effect.
```

[Scenario 2] The topology is shown in the preceding figure. The ERPS interfaces on S86E-4 should be Gi0/3 (up) and Gi0/4 (up). However, the ERPS interfaces are configured as Gi0/3(up) and Gi0/6 (down) incorrectly.

```
S86E-4(config)#erps raps-vlan 4010
S86E-4(config-erps 4010)#no state enable
S86E-4(config-erps 4010)#ring-port west gi0/3 east gi0/6
S86E-4(config-erps 4010)#state enable
S86E-4(config-erps 4010)#00:00:20:23:   %ERPS-5-PORT_STATE_CHANGE: Port GigabitEthernet 0/6 on R-APS VLAN 4010 has been set to forwarding state.
00:00:20:23:   %ERPS-5-PORT_STATE_CHANGE: Port GigabitEthernet 0/3 on R-APS VLAN 4010 has
```

been set to forwarding state.

```
S86E-4#show erps

ERPS Information

Global Status                  : Enabled

Link monitored by              : Not Oam

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

R-APS VLAN                        : 4010

Ring Status                    : Enabled

West Port                      : Gi0/3           (Link Normal)

East Port                      : Gi0/6           (Link Failure)    //A down interface is associated. In the
ERPS ring network, only the Gi0/6 interface is in the down state and the Gi0/3 interface sends SF
packets.

RPL Port                       : None

Protected VLANs                : ALL

RPL Owner                        : Disabled

Holdoff Time                   : 0 milliseconds

Guard Time                       : 500 milliseconds

WTR Time                          : 2 minutes

Current Ring State             : protection
```

2) The interface Gi0/6 is replaced by the interface Gi0/4 when the ERPS interface (Gi0/3 or Gi0/4) is not shut down. This causes that the WTR timer is lost, ERPS control packets are lost, ERPS convergence fails, and a loop occurs. The ERPS is in the protection state and the ERPS interface is in the (Link Normal) forwarding state.

```
S86E-2#config

S86E-2(config)#erps raps-vlan 4010

S86E-2(config-erps 4010)#no state enable

S86E-2(config-erps 4010)#ring-port west gi0/3 east gi0/4     //Make the modification directly without
shutting down the ERPS interface gi0/3 or gi0/4.

S86E-2(config-erps 4010)#state enable

S86E-2#sho erps

ERPS Information

Global Status                  : Enabled
```

```
Link monitored by                   : Not Oam
-------------------------------------------
R-APS VLAN                              : 4010
Ring Status                         : Enabled
West Port                            : Gi0/3          (Link Normal)
East Port                           : Gi0/4          (Link Normal)
RPL Port                              : None
Protected VLANs                      : ALL
RPL Owner                               : Disabled
Holdoff Time                        : 0 milliseconds
Guard Time                            : 500 milliseconds
WTR Time                                : 2 minutes
Current Ring State                 : protection
```

If you are sure that the loop occurring on the ERPS ring network is caused by preceding operations, rectify the fault by using the following configurations:

```
int gi 0/3       //On the faulty device, shut down the ERPS interface.
shutdown
erps raps-vlan 4010
no state enable
ring-port west gi0/7 east gi0/8    //Change the ERPS interface.
ring-port west rpl-owner
state enable
int gi 0/3    //After completing the preceding configurations, enable the interface.
no shutdown
```

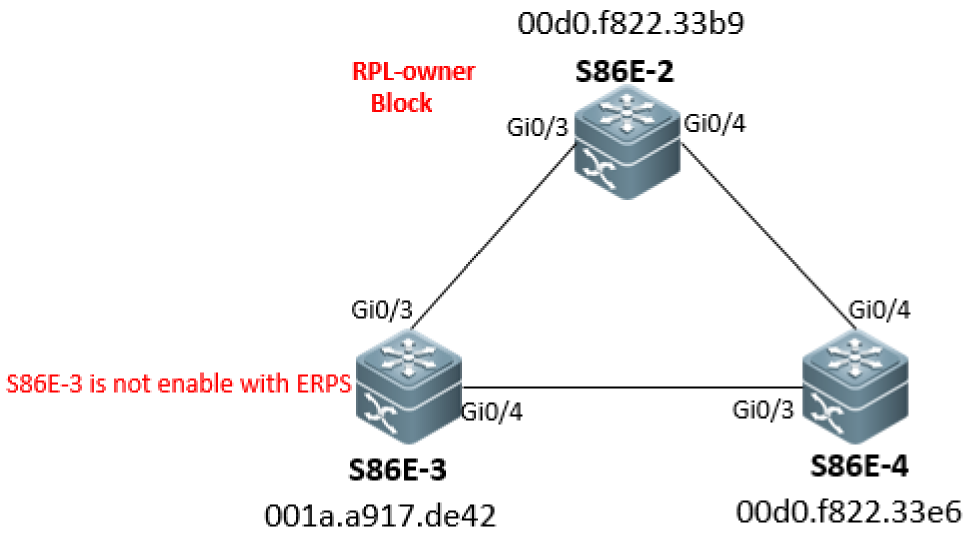
Step 3: Check ERPS status that cannot be converged to the idle state in the network.

1. Run **show** commands to check the device status in the ERPS ring network and check whether the ERPS status cannot be converged to idle.

```
S86E-2#sho erps

ERPS Information

Global Status                : Enabled

Link monitored by            : Not Oam

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

R-APS VLAN                      : 4010

Ring Status                   : Enabled

West Port                     : Gi0/3          (Blocking)

East Port                    : Gi0/4          (Forwarding)

RPL Port                      : West Port

Protected VLANs                : ALL

RPL Owner                        : Enabled

Holdoff Time                 : 0 milliseconds

Guard Time                     : 500 milliseconds

WTR Time                         : 2 minutes

Current Ring State          : protection      //The device keeps the protection state all the time.
```

2. Check whether all devices in the ERPS ring network are enabled with ERPS.

As shown in the following topology, S86E-3 is not enabled with ERPS.



1. After ERPS is correctly configured for S86E-2 and S86E-4, check the ERPS status through debug erps packets on S86E-2. Since S86E-3 is not enabled with ERPS, RLDP of S86E-2 and S86E-4 detects a loop, which will disable the Gi0/3 interface of each device.

Device S86E-2

```
S86E-2#sho rldp

rldp state          : enable

rldp hello interval: 3

rldp max hello      : 6

rldp local bridge   : 00d0.f822.33b9

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

GigabitEthernet 0/3

port state          : error

neighbor bridge : 001a.a917.de42

neighbor port       : GigabitEthernet 0/3

bidirection detect information :

        action: shutdown-port

state : error


GigabitEthernet 0/4

port state          : normal

neighbor bridge : 00d0.f822.33e6

neighbor port       : GigabitEthernet 0/4

bidirection detect information :

        action: shutdown-port

        state : normal


S86E-2#debug erps packet

21:22:42:32:   %7: [ERPS-PKT]:Send erps packet R-APS(SF) at 189615201, raps-vlan 4001 status 0x0

21:22:42:36:   %7: [ERPS-PKT]:Recv packet at 189615682, len = 60

21:22:42:36:   %7: [ERPS-PKT]:Recv erps packet R-APS(SF) at 189615682, raps-vlan 4001 ifx 4 status
0x0 node-id 00d0.f822.33e6
```

```
21:22:42:37:   %7: [ERPS-PKT]:Send erps packet R-APS(SF) at 189615701, raps-vlan 4001 status 0x0

21:22:42:41:   %7: [ERPS-PKT]:Recv packet at 189616182, len = 60
```

//Since the Gi0/3 interface is in the error state detected by RLDP, the device sends SF packets to notify the peer device. (When the node link is down, the node sends this packet to notify other nodes.)

```
S86E-2#no debug all

S86E-2#sho erps

ERPS Information

Global Status                    : Enabled

Link monitored by                : Not Oam

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

R-APS VLAN                          : 4001

Ring Status                      : Enabled

West Port                        : Gi0/3         (Link Failure)              //Since this interface is
detected as error by RLDP, link failure is displayed.

East Port                        : Gi0/4         (Forwarding)

RPL Port                          : West Port

Protected VLANs                   : ALL

RPL Owner                          : Enabled

Holdoff Time                     : 0 milliseconds

Guard Time                        : 500 milliseconds

WTR Time                           : 2 minutes

Current Ring State              : protection
```

Device S86E-4

```
S86E-4#sho rldp

rldp state              : enable

rldp hello interval: 3

rldp max hello        : 2

rldp local bridge   : 00d0.f822.33e6

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

GigabitEthernet 0/4
```

```
port state          : normal

neighbor bridge : 00d0.f822.33b9

neighbor port      : GigabitEthernet 0/4

bidirection detect information :

        action: shutdown-port

        state : normal

loop detect information               :

        action: shutdown-port

        state : normal


GigabitEthernet 0/3

port state          : error

neighbor bridge : 001a.a917.de42

neighbor port      : GigabitEthernet 0/4

bidirection detect information :

        action: shutdown-port

        state : error

loop detect information               :

        action: shutdown-port

        state : normal


S86E-4#debug erps packet

07:01:23:57:   %7: [ERPS-PKT]:Send erps packet R-APS(SF) at 60983722, raps-vlan 4001 status 0x0

07:01:24:01:   %7: [ERPS-PKT]:Recv packet at 60984141, len = 60

07:01:24:01:   %7: [ERPS-PKT]:Recv erps packet R-APS(SF) at 60984141, raps-vlan 4001 ifx 4 status
0x0 node-id 00d0.f822.33b9

07:01:24:02:   %7: [ERPS-PKT]:Send erps packet R-APS(SF) at 60984222, raps-vlan 4001 status 0x0


S86E-4#sho erps

ERPS Information
```

```
Global Status                  : Enabled

Link monitored by              : Not Oam

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

R-APS VLAN                        : 4001

Ring Status                     : Enabled

West Port                        : Gi0/3          (Link Failure)

East Port                       : Gi0/4          (Forwarding)

RPL Port                         : None

Protected VLANs                  : ALL

RPL Owner                          : Disabled

Holdoff Time                    : 0 milliseconds

Guard Time                        : 500 milliseconds

WTR Time                           : 2 minutes

Current Ring State             : protection
```

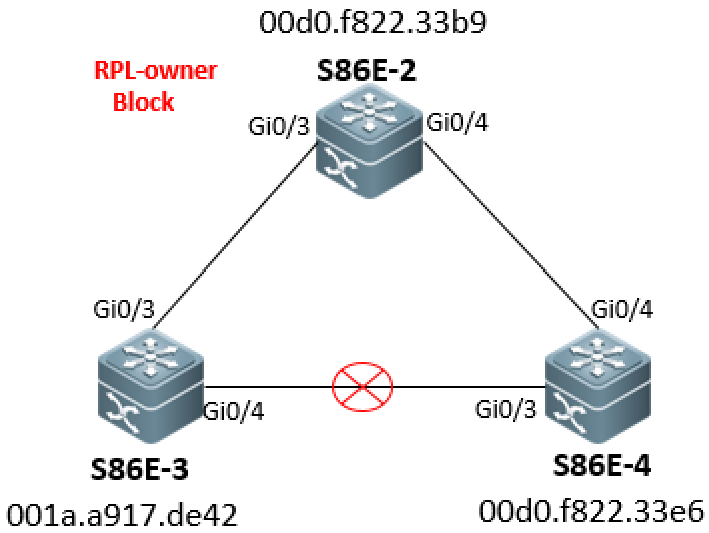
Note: In the ERPS ring network, S86E-3 not enabled with ERPS can transparently transmit ERPS packets. However, RLDP takes effect first in this process; therefore, the Gi0/3 interfaces of S86E-2 and S86E-4 are always in the RLDP error state, and the corresponding interfaces in the ERPS ring network are always in the link failure state. When the entire ERPS ring network is faulty and then the faulty is rectified, the ERPS cannot recover to the idle state but the interconnection of the entire network is normal without any loop.

Solution: Configure the **erps** command for devices not enabled with the ERPS function.

Step3: Check whether any link connection in the network is down. When a physical link in the ERPS ring network is down, the link failure state is kept all the time.

When a faulty link is recovered, the ERPS state can be recovered to idle. If the faulty link is always in the down state, ERPS state cannot be recovered to idle, which is a normal behavior of ERPS.

The topology is as follows:



```
S86E-3#sho erps

ERPS Information

Global Status                  : Enabled

Link monitored by              : Not Oam

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

R-APS VLAN                        : 4001

Ring Status                    : Enabled

West Port                      : Gi0/3          (Forwarding)

East Port                      : Gi0/4          (Link Failure)

RPL Port                       : None

Protected VLANs                : ALL

RPL Owner                        : Disabled

Holdoff Time                   : 0 milliseconds

Guard Time                     : 500 milliseconds

WTR Time                         : 5 minutes

Current Ring State             : protection
```

```
S86E-2#22:23:22:29:   %ERPS-5-PORT_STATE_CHANGE: Port GigabitEthernet 0/3 on R-APS VLAN 4001 has been set to forwarding state.

22:23:22:29:   %ERPS-5-TOPOLOGY_CHANGE: Topology changed for R-APS VLAN 4001, The ring
```

```
changed state from idle to protection

S86E-2#debug erps pack

S86E-2#22:23:23:39:   %7: [ERPS-PKT]:Recv packet at 198501930, len = 60

22:23:23:39:   %7: [ERPS-PKT]:Recv erps packet R-APS(SF) at 198501930, raps-vlan 4001 ifx 3 status
0x0 node-id 001a.a917.de42

22:23:23:39:   %7: [ERPS-PKT]:Recv packet at 198501943, len = 60

22:23:23:39:   %7: [ERPS-PKT]:Recv erps packet R-APS(SF) at 198501943, raps-vlan 4001 ifx 4 status
0x0 node-id 00d0.f822.33e6

//SF packets are continuously received from S86E-3 and S86E-4. The ERPS is in the protection state.

S86E-2#no debug all

All possible debugging has been turned off

S86E-2#sho erps

ERPS Information

Global Status                       : Enabled

Link monitored by                   : Not Oam

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

R-APS VLAN                              : 4001

Ring Status                          : Enabled

West Port                             : Gi0/3          (Forwarding)

East Port                            : Gi0/4          (Forwarding)

RPL Port                               : West Port

Protected VLANs                       : ALL

RPL Owner                               : Enabled

Holdoff Time                         : 0 milliseconds

Guard Time                             : 500 milliseconds

WTR Time                                : 2 minutes

Current Ring State                  : protection
```

Solution: Recover the faulty link. If it is confirmed that an interface is shut down (which can be recovered by the **no shutdown** command), check whether the interface is shut down due to cable problems (which can be solved by cable replacement).

Step4: Fault Information Collection

If the fault persists after the preceding operations are performed, collect the following fault information and dial the number 4008-111-000 for help.

```
show version

show run

show log

show cpu

show interface description

show interface status

show interface counter

show mac-address-table

show erps

show erps global

debug erps packet
```

Collect the logs during troubleshooting.

5.2 Collecting information when VSU fails

Step1: Check the status of the Virtual Switch Unit (VSU) system.

Check the status of the VSU system to determine whether the network is disconnected due to VSU failure.
(1) Check whether VSU configurations are correct.

```
ruijie#show switch virtual config
```

(2) Check whether Virtual Switching Links (VSLs) are normal.

```
ruijie#show sw vir link

ruijie#show sw vir link port //Check whether VSLs are normal. If yes, the VSU system is not split.

ruijie#show int count error

ruijie#show int trans //If VSLs are created using optical transceivers, check the optical transceivers.

ruijie#show int trans dia //If VSLs are created using optical transceivers, check optical attenuation of the
```

fiber.

(3) If all VSLs go down, log in to two switches at link ends to check whether one of them enters the recovery mode. The one entering recovering mode is the standby.

```
ruijie#show sw virtual dual-active summary

BFD dual-active detection enabled: Yes

Aggregateport dual-active detection enabled: NO

In dual-active recovery mode: Yes //At least one switch should be in the recovery mode. If neither one enters the recovery mode, VSLs are abnormal and the dual-active detection is disabled when two active switches exist.
```

(4) If one switch enters the recovery mode (all its interfaces are shut down this time), check whether the disconnected PCs connect to the standby switch. If yes, re-connect the PCs to the active switch to avoid the influence of the recovering mode.

(5) If all VSLs go down, check whether the fault is caused by software problems or link disconnection.

a. Enter the management board and the corresponding VSL line card to check whether crash information exists. Run the following commands to collect fault information:

```
Ruijie#debug support

Ruijie(support)#tech-support package
```

b. Check whether the keepalive timeout information of the line card is logged.

c. Check whether the abnormal reset of management board (not crash) is logged.

Step2: Check whether the VSU system properly sends packets to the control panel.

(1) Run the show arp command to check whether the switches in disconnected network segments can learn MAC addresses.

(2)Check by CPP whether related packets are sent to the CPU. (You have to check packets under protocols enabled in the network especially for connectivity protocols, for example, ARP, VRRP, and BPDU.)

Run each of the following commands for five times:

```
Ruijie#show cpu-pro

Ruijie#show cpu-pro mb
```

Ruijie#show cpu-protect slot X *//X* indicates the slot ID. For example, run **show cpu-pro slot 4** to display information of Slot 4 on the standalone server S86E; run **show cpu-pro slot 2/4** to display information of Slot 4 on Cabinet 2 of the VSU system.

If the number of packets sent to the CPU of the line card or management board is always 0, the packet reception by CPU is abnormal.

Step3: Check the interface traffic of the VSU system.

Ruijie#show int count rate //Check whether the interface rate exceeds the interface bandwidth.

Ruijie#show int count summary //Check whether the interface input/output broadcast packets increase rapidly. If yes, a loop must have occurred in the network.

Step4: Check whether VSU system resources are normal.

Ruijie#show cpu //Check whether CPU resources of the VSU system are normal.

Ruijie#show memory //Check the memory utilization of the VSU system.

Ruijie#debug support

Ruijie(support)#tech-support package

Step5: Collect and summarize log information.

Collect log information (enable the time stamp and ensure time accuracy) and provide it to Ruijie technical support for analysis.

Collect basic information:

ruijie>enable

ruijie#

---------In Privileged EXEC Mode (ruijie#)----------------

show ver

show ver slot

show run

show cpu

```
show memory

show logging

show cpu-protect

show cpu-protect mb
```

show cpu-protect slot X //*X* indicates the slot ID. For example, run **show cpu-pro slot 4** to display information of Slot 4 on the standalone server S86E; run **show cpu-pro slot 2/4** to display information of Slot 4 on Cabinet 2 of the VSU system.

```
show interfaces counters rate

show interfaces counters

show int count summary

show int count error

show mac-address-table

show arp

show mac-address-table count

        show arp count
```

Collect VSU information:

```
ruijie>enable

ruijie#
```

---------In Privileged EXEC Mode (ruijie#)----------------

```
show switch virtual link

show switch virtual link port

show switch virtual config

show switch virtual role
```

5.3 Console Faults in the VSU scenario

Check logs about Console faults such as Console crash, switch abnormalities, memory insufficiency, and high CPU utilization. These faults may influence data forwarding, which depends on the actual situation.

If the switches work properly, collect the information as follows:

Note:1) If the switches work as a VSU group, collect information on each standby switch: (If there are more than three VSU members, collect information on any three members.)

2) Enter @@@@C on the standby switch to enable Console printing.

3) If a command is repeated, it means collecting information for multiple times.

```
show ver
show version slot
show run
showcpu
showcpu pro mb
showcpu-pro
show memory //Run this command every 5 seconds for three times.
show memory protocols //Run this command every 5 seconds for three times.
show interface status
show arp counter
show mac-address-table count
show arp
show mac-address-table
show spanning
show spanning summary//Run this command every 5 seconds for three times.
show int count rate//Run this command every 5 seconds for three times.
show tcp connect
show log
showcpu pro mb
showcpu-pro
Ruijie#debug su
Ruijie(support)#tech-support package
```

If the show commands cannot be run or the switches cannot be managed through the Console port, collect information as follows:

Caution

1) Risks: Collection poses high risks. Due to high priority and frequent interruption, collection may affect customers' services, and even interrupt the customer's network (in this case, you need to restart the switches to recover services).

2) If the switches work as a VSU group, collect information on each standby switch(see the "Note" above):(If there are more than three VSU members, collect information on any three members.)

3) Enter @@@@C in the standby switches to enable Console printing.

Notes

- 1) Collect information as follows if a customer wants to restart a switch for service recovery immediately but the switch cannot be managed through Console, Telnet or SSH.
- If the customer agrees to collect information after being informed of the risks, you can restart the switch.
- 2) Information collection must be complete within the allowed downtime of the customer's services. If not, you should restart the switch as well.
- 3) Before restarting the switch, confirm with the customer on the restart time to make the customer well-prepared.

1) High-risk collection:

Run the following commands in sequence. If the customer wants to recover services, restart the switch whether the collection is complete or not.

Enter 4**Esc**+**f** (4**Esc** indicates pressing the **Esc** button for four times) to collect all information at the time when the fault occurs. Collect other information as follows:

4Esc + b : reboot

4Esc + d : debug_show_all_locks

4Esc + c : open and close console

4Esc + h : help

4Esc + i : dump cli debug info

4Esc + j : dump irq info

4Esc + k + pid + # : kill pid proc

4Esc + l : dump start process

4Esc + m : dump mem info

4Esc + n	: start hrtimer
4Esc + o	: stop hrtimer
4Esc + p	: close logging message(same as: no logging on)
4Esc + q	: dump context switches and runtime
4Esc + r	: dump other cpudump_stack
4Esc + s	: show 5@ info
4Esc + t	: show task states
4Esc + x	: start dot task
4Esc + y	: stop dot task

2) Remove any network cable on the switch and check whether any log is displayed. (Perform this operation only when allowed by the customer.)

//This operation usually applies when the switch cannot be managed through the console port and console printing fails.

3) Remove the cables one by one from the switch. After a while, check whether you can enter the privileged EXEC mode. (Perform this operation only when allowed by the customer.)

//Check whether your failure to enter the privileged EXEC mode is due to environment problems, and identify the faulty port.

⚠ Caution

Notify the customer to mark the cables before removing them to prevent cables from being connected to wrong ports

4) If the switch can be managed through the console port after the network cables are removed, collect information using the show commands.

5) If the switch cannot be managed through the console port after the network cables are removed, restart the switch and collect information using the show commands.

6) After the switch is restarted, it is recommended that the customer collect information using the show commands every day, report such information to us, and check whether

the network is prone to memory leak.

6. IP Multicast

6.1 Troubleshooting Multicast service abnormal

6.1.1 Fault Symptom

Multicast is enabled in the network but users cannot demand the multicast service.

6.1.2 Possible Causes

1) The multicast receiver is not connected to the server and therefore no unicast route is established.
2) Multicast configuration is abnormal on the intermediate switches.
3) Packet TX/RX is abnormal between the multicast receiver and server.

6.1.3 Troubleshooting Procedures

Step 1: Check whether the connection between the multicast receiver and server is normal.
Step 2: Check whether configurations among switches are correct.
Step 3: Check whether the multicast source and receiver can properly send and receive multicast packets.
Step 4: Check whether multicast entries on the multicast source and receiver are normal.
Step 5: Check whether IGMP snooping entries are created on the access switches.
Step 6:Collectfault information and submit cases to Ruijie Service Portal.

Step1: Check whether the connection between the multicast receiver and server is normal.

1.Verify the following items carefully:
- Interfaces between the server and the switches
- IP address and MAC address of the server
- Interfaces between the switches and their IP addresses
- Interfaces between the PC and the switches

- IP address and MAC address of the PC
- IP address of the gateway

2.Check whether the multicast server properly communicates with the multicast receiver on demand. (Before demanding, check routing problems to ensure that multicast routing protocol is communicable.)

Step2: Check whether configurations among switches are correct.

1.Check basic configurations in PIM-DM mode:

1) Whether the multicast routing protocol is globally enabled

2) Whether all the interfaces to send or receive multicast packets are enabled with PIM-DM and IGMP (IGMP is enabled by default when multicast routing is enabled.)

2.Check advanced configurations in PIM-DM mode:

1) Whether neighbor filtering is incorrectly configured

2) Whether ACLs for optimized filtering are incorrectly configured which causes legitimate multicast and IGMP packets to be discarded

3.Check basic configurations in PIM-SM mode:

1) Whether the multicast routing protocol is globally enabled

2) Whether all the interfaces to send or receive multicast packets are enabled with PIM-SM and IGMP (IGMP is enabled by default when multicast routing is enabled.)

3) Whether static or dynamic RPs (C-RP and C-BSR) are configured

4.Check advanced configurations in PIM-SM mode:

1) Whether neighbor filtering is incorrectly configured

2) Whether the RP registry packet filtering is correctly configured

3) Whether the BSR range limit is correctly configured

4) Whether the legitimate C-RP range and multicast group are correctly configured

5) Whether ACLs for optimized filtering are incorrectly configured which causes legitimate multicast and IGMP packets to be discarded

5.Check advanced configurations of IGMP:

1) Whether IGMP access group is configured for multicast control and whether ACLs are correctly added

2) Whether the immediate-leave feature is incorrectly configured on a multi-user interface

3) Whether the IP IGMP limit is too small on an interface. The default value is 1,024.

6.Check the IGMP snooping configuration on the access switches:

For example, run the **show ip igmp snooping** command:

```
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: SVGL
SVGL vlan: 1
SVGL profile number: 11
```

```
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

1) Check whether IVGL or SVGL is configured. (SVGL must be used with the IGMP profile.)

2) In the IGMP profile, only data packets in the multicast address range can be forwarded across VLANs. By default, all multicast groups are not in the SVGL range and all the multicast packets are discarded.

3) Check whether the routing interfaces are statically configured or automatically learning and whether source interface/IP address check is enabled. (When troubleshooting the fault, you can disable source interface check to prevent related advanced security functions from influencing troubleshooting.)

4) Check whether IGMP snooping filter is enabled on user interfaces. If yes, disable it before troubleshooting.

Step3: Check whether the multicast source and receiver can properly send and receive multicast packets.

Capture packets on the application layer to check whether the multicast source and receiver properly work. In some cases, the multicast source server may be incorrectly deployed and parameter settings are incorrect on the multicast receiver. You can exclude or replace the faulty devices.

Packet capture on the multicast source helps understand parameters of multicast packets, for example, fragmentation, multicast packet size, source and destination IP addresses, port, and TTL. Generally, these parameters are useful for troubleshooting.

Step4: Check whether correct multicast routing entries are created on intermediate switches (from the multicast source to the multicast receiver). (Prerequisite: ensure the unicast routing is normal.)

PIM-DM

1. Check the multicast routing table in PIM-DM mode:

```
ruijie#show ip mroute

IP Multicast Routing Table

Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed

Timers: Uptime/Stat Expiry

Interface State: Interface (TTL)

Multicast source        Multicast destination

(210.34.130.27, 224.3.1.2), uptime 00:18:04 (creation time), stat expires 00:01:21 (expiration time)
```

```
Owner PIMDM, Flags: TF

Incoming interface: TenGigabitEthernet 3/1    //Enter the RPF interface.

Outgoing interface list:     Outgoing interface

TenGigabitEthernet 3/2 (1)
```

2. Check detailed entries:

show ip pim dense-mode mroute (protocol table)

```
Ruijie# show ip pim dense-mode mroute

PIM-DM Multicast Routing Table

(1.1.1.111, 229.1.1.1)

MRT lifetime expires in 205 seconds

RPF Neighbor: 50.50.50.1, Nexthop: 50.50.50.1, VLAN 4    RPF check

Upstream IF: VLAN 4

Upstream State: Pruned, PLT:200

Assert State: NoInfo

Downstream IF List:

FastEthernet 0/45:

Downstream State: NoInfo

Assert State: Loser, AT:170
```

Notes

- The preceding example lists information of the entry (1.1.1.111, 229.1.1.1), among which the MRT lifetime is 205 seconds. The RPF neighbor is 50.50.50.1, which is the next hop. The outgoing interface of the next hop is VLAN 4. The upstream interface VLAN 4 is in Pruned state, indicating that the entry has no downstream forwarding egress. The downstream interface FastEthernet0/45 is in NoInfo state and its Assert state is Loser. FastEthernet 0/45 is not a forwarding egress.

Pay attention to three points: 1. whether entries are created; 2. whether ingresses meet the expectation; 3. whether forwarding interfaces are available.

3. If entries are not created, check the following items:

1) Whether PIM neighbors are normal

show ip pim dense-mode neighbor

show ip pim dense-mode interface

show ip mvif

2) Whether PIM packets are properly sent and received (packet capture or debugging)

Caution

Since debugging is risky (you may even need to restart the device to recover services), collect such information after the customer is notified of the risks and agrees on debugging. Debugging is recommended in low peak hours. (Perform careful assessment before debugging a core switch.) If packet capture is required for troubleshooting, perform debugging and packet capture at the same time.

show ip pim dense-mode track

debug ip pim sparse-mode fsm

debug ip pim sparse-mode nsm

debug ip pim sparse-mode all

PIM-SM

1. Check the multicast routing table in PIM-SM mode:

PIM has two trees: shortest path tree (SPT) from the multicast source to the rendezvous point (RP) and rendezvous point tree (RPT) from the multicast destination to the RP.

The multicast routing table of the RPT differs from that of the SPT. Since RPT can be shared by many sources, its protocol routing entries are in (*,G) mode (including RP information). The routing entries of the SPT are in (S,G) mode. The RP has both (*,G) [RPF next hop is 0.0.0.0] and (S,G) entries.

show ip mroute

On Ruijie switches, the **show ip mroute** command displays information about the forwarding table instead of the protocol table. Whether in PIM-DM or PIM-SM mode or not, the entries are in (S,G) format. On Cisco switches of the same type, the entries in the **show ip mroute** command are in (*,G) format.

Ruijie PIM-SMv4/v6 does not support forwarding based on (*,G) entries. In implementation, ***** indicating all sources changes to **s** indicating a specific source. The switch uses the NSM module to forward protocol tables based on (S,G) entries, which is reflected in the **debug nsm** command. Multicast forwarding is based on the forwarding table, which is reflected in the **debug msf** command. The **show ip mroute** and **show ip igmp-sn gda** commands respectively provide Layer-3 and Layer-2 tables to user interfaces. The **show msf msc** command provides multicast forwarding tables to debugging interfaces.

The **show ip pim sparse-mode mroute** command displays routing entries in PIM-SM mode.

2. Check detailed entries:

show ip pim sparse-mode mroute

show ip mroute //Layer-3 table

show ip igmp-sn gda //Layer-2 table

show msf msc

3. If protocol entries are not created, check the following items:

1) Whether PIM neighbors are normal

show ip pim sparse-mode neighbor [detail]

show ip pim sparse-mode interface

show ip mvif

2) Whether RP mapping exists

show ip pim sparse-mode rp mapping

3) BSR information

show ip pim sparse-mode bsr-router

4) Whether the PIM packet RX/RX and processing mechanism are normal (by packet capture or debugging)

show ip pim sparse-mode track

debug ip pim sparse-mode packets

debug ip pim sparse-mode event

debug ip pim sparse-mode state

debug ip pim sparse-mode nsm

debug ip pim sparse-mode mfc

debug ip pim sparse-mode all

Step5: Check whether IGMP snooping entries are created on the access switches.

IGMP snooping can effectively restrict multicast data from spreading on Layer-2 network. If IGMP snooping is disabled, multicast packets are regarded as broadcast packets and forwarded in the VLAN. If IGMP snooping is enabled, user interfaces with demanding requirements can receive related data. If multicast becomes abnormal after SNP is enabled, check SNP entry creation.
Check entries.

```
Ruijie#show ip igmp snooping gda-table

Multicast Switching Cache Table

  D: DYNAMIC

  S: STATIC

  M: MROUTE

(*, 224.1.1.1, 100):

  VLAN(100) 2 OPORTS:

    GigabitEthernet 0/13(M)

    GigabitEthernet 0/22(D)
```

If entries are not created, check the following items:

1) Run the **show ip igmp group** and **debug ip igmp events** commands or capture packets on the gateway to check the TX/RX status of IGMP packets.

2) Capture packets on the PC to check the TX/RX status of IGMP packets.

3) Run the **debug igmp-snp event**, **debug igmp-snp packets**, and **debug igmp-snp msf** (optional) commands on the access switches.

Step6: Collect fault information on all Layer-3 switches between the multicast source and the multicast receiver.

1 Collect basic information:

```
show run
show ver
show ver slo
show int co su     //Run this command every 15 seconds for three times if the fault occurs.
show int co rate
show int co         //Run this command every 15 seconds for three times if the fault occurs.
show cpu
show cpu mb
show ip mroute
show ip route
show ip route cou
show ip igmp groups
show ip igmp groups    detail
show log
```

In PIM-DM mode, run the following commands to collect information:

```
show ip pim dense-mode mroute
show ip pim dense-mode neighbor
show ip pim dense-mode interface
show ip mvif
show ip pim dense-mode track
```

In PIM-SM mode, run the following commands to collect information:

```
show ip pim sparse-mode mroute
show ip pim sparse-mode neighbor [detail]
show ip pim sparse-mode interface
show ip mvif
show ip pim sparse-mode rp mapping
show ip pim sparse-mode bsr-router
show ip pim sparse-mode track
```

2. Collect information on the access switches.

```
show run
show ver
show ver slo
show int co su      //Run this command every 15 seconds for three times if the fault occurs.
show int co rate
show int co         //Run this command every 15 seconds for three times if the fault occurs.
show cpu
show ip igmp snooping
show ip igmp snooping gda-table
show ip igmp snooping interfaces
show ip igmp snooping mrouter
show ip igmp snooping querier
show ip igmp snooping statistics
show ip igmp profile
show msf nsf
show msf msc
```

3. Perform SPAN packet capture on switches between the multicast source and the multicast receiver.

Capture packets first on the access switches and then on upstream switches to identify the switches that the packets can reach and that do not forward multicast data flow.

6.2 Multicast service pause or pixilation occur

6.2.1 Fault Symptom

When multicast is enabled in the network, the PC can demand the multicast service. However, pause or pixilation may occur.

6.2.2 Possible Causes

1) Packet loss occurs on interfaces or links.
2) Congestion occurs on switches.

6.2.3 Troubleshooting Steps

Step1: Check the topology connections.

Check the following items:
- Interfaces between the server and the switches
- IP address and MAC address of the server
- Interfaces between the switches and their IP addresses
- Interfaces between the PC and the switches
- IP address and MAC address of the PC
- IP address of the gateway

Step2: Check whether packet loss occurs on interfaces.

show interfaces counters //Display the counter of error packets on each interface to check whether error packets such as FCSErrors increase continuously. If packet loss occurs on the hardware, replace the interface and network cable to check whether the fault is rectified. Use this method to check whether the next-hop switch is faulty.

Step3: Check whether congestion occurs on interfaces.

show interfaces counters rate //Check whether the rates at the ingoing and outgoing directions of each interface exceed the interface bandwidth. If yes, check whether the interface traffic is normal and whether any attack occurs.

Step4: Check whether GE interfaces send packets to FE interfaces.

Since GE interfaces are connected with the switches while FE interfaces are connected with PCs, PCs may not able to process multicast packets and therefore pixilation occurs. If it happens, enable flow control on the interfaces and check whether the fault is rectified. Note: Flow control takes effect only when it is enabled on the devices at both ends.

Step 5: Check the flow control status on interfaces.
In multicast scenarios, enable flow control on interfaces to prevent untimely packet processing in the case of great traffic.

Step5:Fault Information Collection

Collect fault information by running the following commands, record all operation logs and packet capture information, and report them to Ruijie technical support.

```
show version
show version slots
show run
show log
show ip interface brief
show interface status
show interface counter sum
show interface counter sum
show interface counter sum
show interface counter   rate
show interface counter   rate
show interface counter   rate
show interfaces counters errors
show interfaces counters errors
show interfaces counters errors
show interfaces counters
show interfaces counters
show interfaces counters
show arp counter
show arp
show cpu
show cpu-protect mb
show cpu-protect mb
show cpu-protect mb
show cpu-protect
show cpu-protect slot X    //X indicates the slot ID. For example, run show cpu-pro slot 4 to display information of Slot 4 on the standalone server S86E; run show cpu-pro slot 2/4 to display information of Slot 4 on Cabinet 2 of the VSU system.
show cpu-protect slot X    //X indicates the slot ID. For example, run show cpu-pro slot 4 to display information of Slot 4 on the standalone server S86E; run show cpu-pro slot 2/4 to display information of Slot 4 on Cabinet 2 of the VSU system.
show spanning-tree
show spanning-tree summary
```

2. Collect information about multicast entries.

In PIM-DM mode, run the following commands to collect information:

```
show ip pim dense-mode mroute
show ip pim dense-mode neighbor
show ip pim dense-mode interface
show ip mvif
show ip pim dense-mode track
```

In PIM-SM mode, run the following commands to collect information:

```
show ip pim sparse-mode mroute
show ip pim sparse-mode neighbor detail
show ip pim sparse-mode interface
show ip mvif
show ip pim sparse-mode rp mapping
show ip pim sparse-mode bsr-router
show ip pim sparse-mode track
```

On the access switches, run the following commands to collect information:

```
show ip igmp snooping
show ip igmp snooping gda-table
show ip igmp snooping interfaces
show ip igmp snooping mrouter
show ip igmp snooping querier
show ip igmp snooping statistics
show ip igmp profile
show msf nsf
show msf msc
```

7. Device Management

7.1 No output occurs on the console

7.1.1 Fault Symptom

On the console terminal, no log is displayed or only part of logs are displayed when you type characters.
The switch may properly work or abnormally forward packets (for example, the network under the switch is interrupted).

Note: No log is displayed on standby S86Es in the VSU system by default. You can type @@@@C to enable logging to the console terminal.

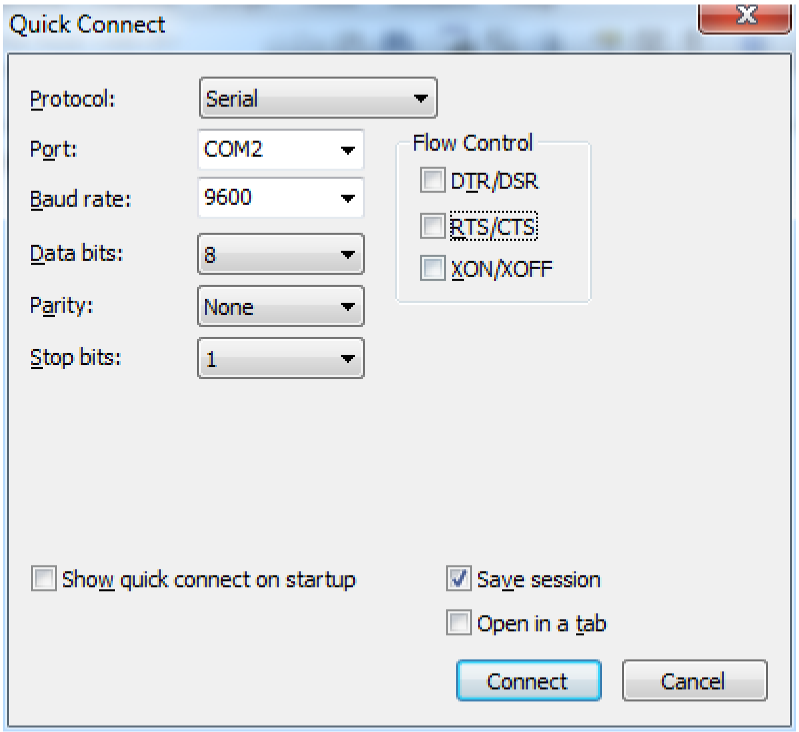
7.1.2 Possible Causes

1) Console setting errors (baud rate, flow control, and COM port) on the host
2) Console cable damage
3) PC system faults
4) Switch software faults, causing process crash
5) Switch hardware faults (for example, faults of stacking modules or cables causing switch crash, and faults of console-based circuit)

7.1.3 Troubleshooting Procedure

Step1: Check whether flow control is disabled on the terminal management software (SecureCRT or Hyper Terminal).

If the setting is incorrect, correct and saved it, exit and the restart the software. Flow control is enabled by default on the SecureCRT. Disable flow control when setting parameters.



Quick Connect

Protocol: Serial

Port: COM2

Baud rate: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow Control

□ DTR/DSR

□ RTS/CTS

□ XON/XOFF

□ Show quick connect on startup

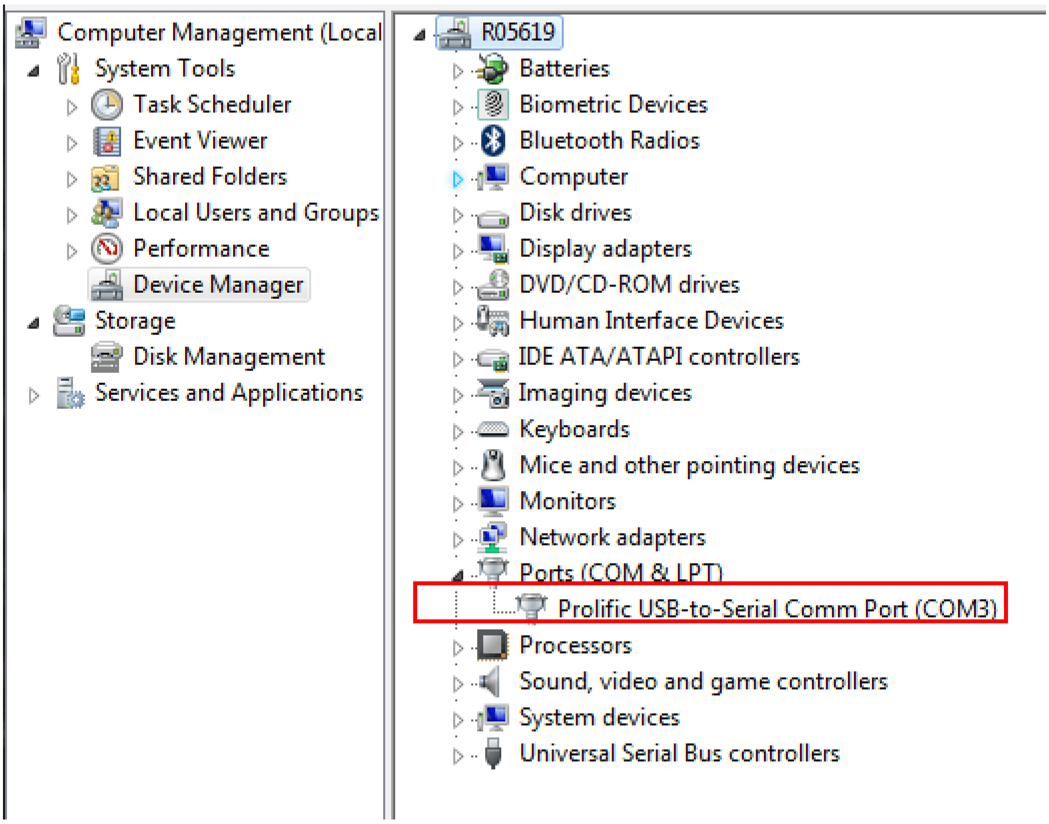
☑ Save session

□ Open in a tab

Flow control is disabled on the Hyper Terminal by default. If it is enabled, reset its default setting.

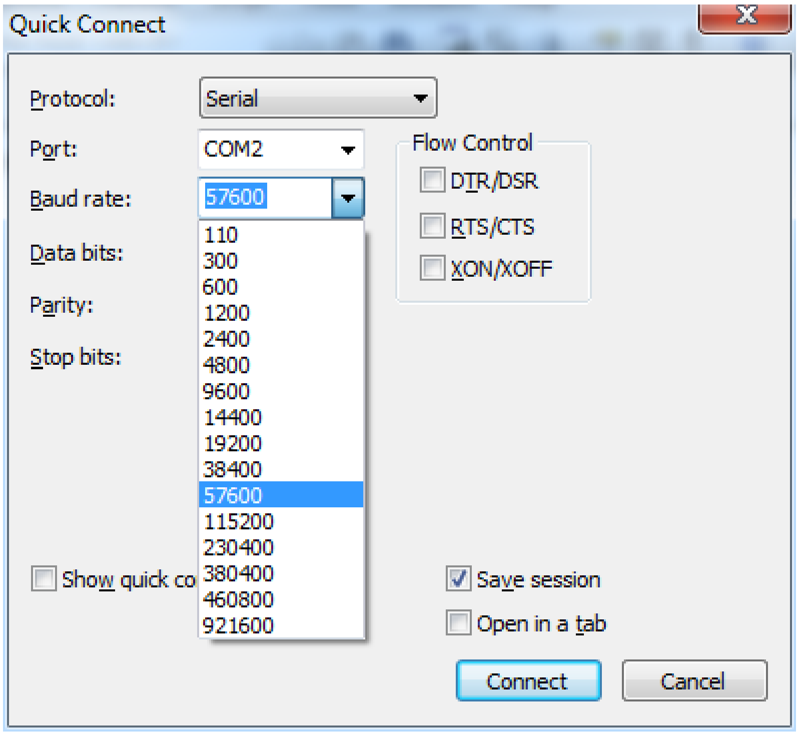
Step2: Check whether the COM port is correct.

Right-click **My Computer** and then choose **Device Manager > Ports (COM & LPT)**.



The COM port needs to be the same as the serial port specified on the Hyper Terminal or SecureCRT.

Step3: Change the baud rate to 57600 or 115200 to check whether the fault is rectified. The default baud rate is 9600 on the console port.



Quick Connect

Protocol: Serial

Port: COM2

Baud rate: 57600

Data bits:

Parity:

Stop bits:

Flow Control

□ DTR/DSR

□ RTS/CTS

□ XON/XOFF

□ Show quick co

☑ Save session

□ Open in a tab

If the fault persists, go to Step 4.

Step4: Press Ctrl+Shift+6 and then enter x to check whether the console port is recovered.

Step5: Check whether the device can be accessed through Telnet and check with the customer about whether services are operational.

If services are operational and the device supports Telnet, run the following commands under Telnet (no risk) to identify the cause for no output on the console terminal:

```
Ruijie#debug su
```

```
Ruijie(support)#tech-support package
```

After information collection, run the **clear line console 0** command to recover services. If the services are not recovered, collect information and contact Ruijie technical support.

If services are operational but the device cannot be accessed through Telnet, run the following commands to identify the cause for no output on the console terminal:

Caution

Collection poses high risks (@@@@@ may even cause network interruption). Before performing the following operations, clarify the risks with the customer and collect information when no service or service risk is available.

Connect the faulty device to the console port.

Run the following commands in sequence. If the customer wants to recover services, restart the switch whether the collection is complete or not. (4Esc indicates pressing the Esc button for four times.)

4Esc + b	: reboot
4Esc + d	: debug_show_all_locks
4Esc + c	: open and close console
4Esc + f	: dump tech-support info
4Esc + h	: help
4Esc + i	: dump cli debug info
4Esc + j	: dump irq info
4Esc + k + pid + #	: kill pid proc
4Esc + l	: dump start process
4Esc + m	: dump mem info
4Esc + n	: start hrtimer
4Esc + o	: stop hrtimer
4Esc + p	: close logging message(same as: no logging on)
4Esc + q	: dump context switches and runtime
4Esc + r	: dump other cpu dump_stack
4Esc + s	: show 5@ info
4Esc + t	: show task states
4Esc + x	: start dot task
4Esc + y	: stop dot task

If the devices are in a VSU system, run the following commands on each standby device:

```
@@@@C

Ruijie#debug su

Ruijie(support)#tech-support package
```

After information collection, submit cases to the service portal for further troubleshooting.

7.2 SPAN failure

7.2.1 Fault Symptom

SPAN is enabled on the switch but the SPAN destination port cannot receive any data.

7.2.2 Possible Causes

1) SPAN configuration error
2) PC faults, such as failure to capture tagged packets

7.2.3 Troubleshooting Procedure

Step1: Check switch configurations and topology connections.

1. Check whether switch configurations are correct. For details, see the switch configuration guide.
2. Check the connections of the network topology, including the SPAN source and destination ports.

Step2: Check whether the SPAN source and destination ports are in Up state.

```
show interfaces status
```

If not, 1) check whether the cables are connected properly; 2) replace network cables.

Step3: Check whether the SPAN source port sends and receives packets.

```
show interfaces counters summary

show interfaces gx/y counters
```

You can check the Tx/Rx traffic counters on the port. If the Tx/Rx traffic counters on the

SPAN source port are unchanged, the SPAN is operational but no traffic is generated on this port.

Step4: Check whether the Packet Capture PC or tester can support tagged packets.

Some PC network adapters or testers cannot capture tagged packets. If SPAN packets are tagged, they may be lost. If so, change the network adapter or tester (is there any solution to this? For example, modifying the registry), or capture untagged packets (for details about how to enable capturing tagged packets, see the XXX section) to check whether the server does not support SPAN tagged packets.

Step5:Fault Information Collection

Based on the fault symptoms, record all operation logs and packet capture information, and report them to Ruijie technical support.

1. Collect basic information:

```
ruijie>enable
```

```
ruijie#
```

---------In Privileged EXEC Mode (ruijie#)----------------

```
    show ver
    show ver slo
    show run
    show log
    show int counter summary
    show int counter summary
    show int counter summary
    show int counter rate
    show int counter rate
    show int counter rate
    show int counter
    show monitor
    show mac-address-table
    show arp
```

8. Appendix

To troubleshoot your S8600E, follow these general tools guidelines：

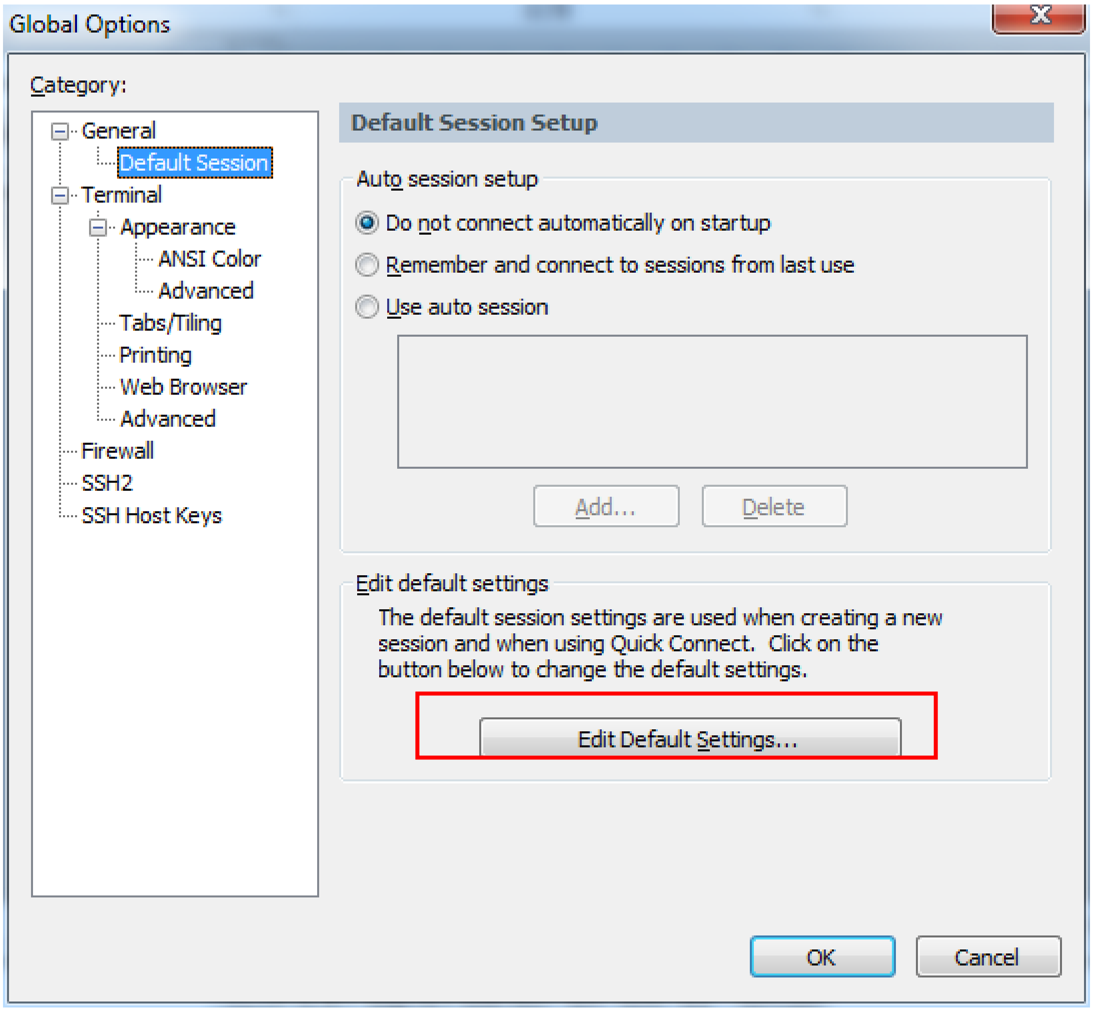
8.1 Secure CRT

8.1.1 Configure SecureCRT automatic logging

SecureCRT automatic logging is very practical. It can automatically and completely record all operations on devices to prevent loss of important failure information due to human error.

Configure SecureCRT automatic logging as follows:

Step1. Choose **Option** > **Global Options** > **Edit Default Settings**.



Global Options

Default Session Setup

Auto session setup

● Do not connect automatically on startup

○ Remember and connect to sessions from last use

○ Use auto session

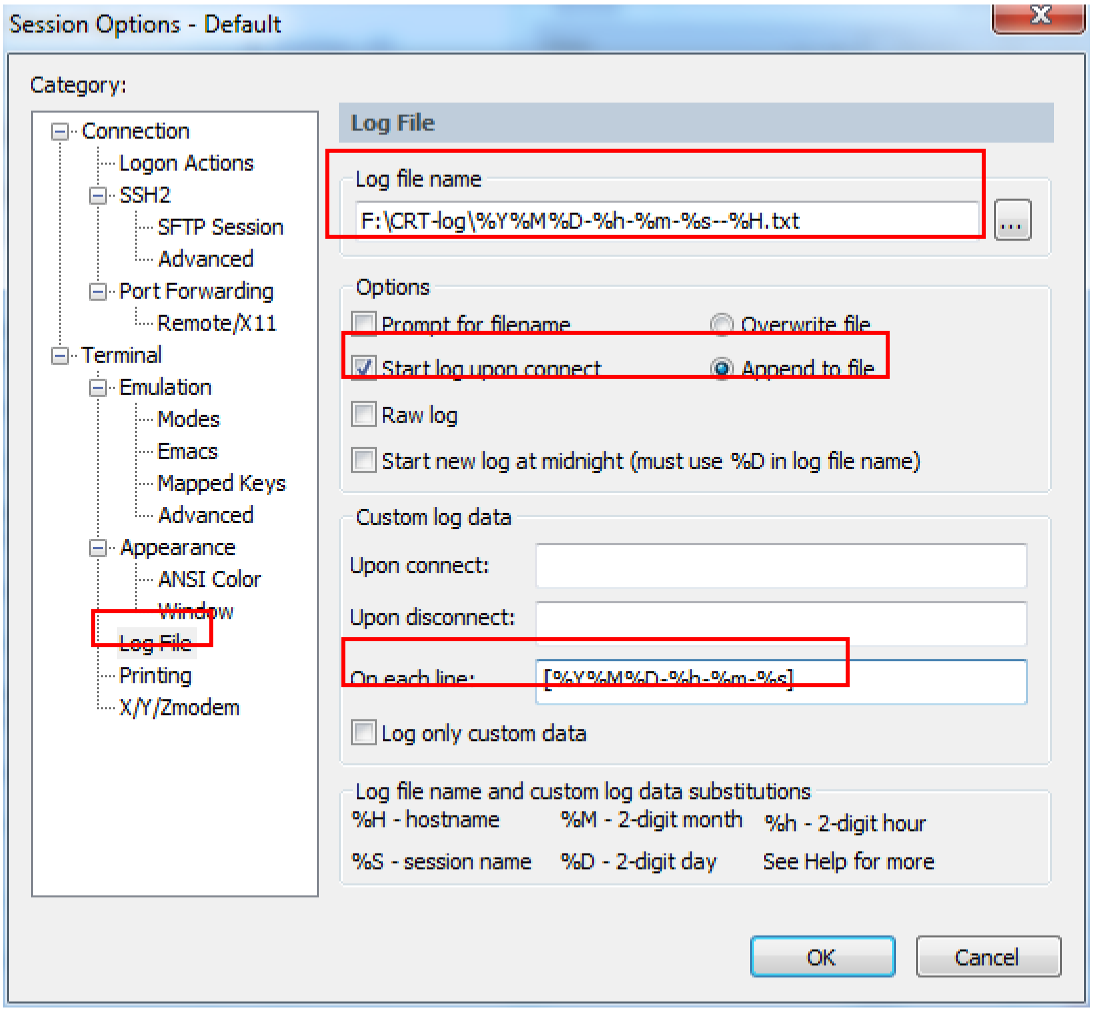
Edit default settings

The default session settings are used when creating a new session and when using Quick Connect. Click on the button below to change the default settings.

2. Create a folder in any location of the disk to store all subsequent logs, for example, F:\CRT-log. After the folder is created, perform the following configuration in the SecureCRT:

F:\CRT-log\%Y%M%D-%h-%m-%s--%H.txt

[%Y%M%D-%h-%m-%s]



Log File

Log file name

F:\CRT-log\%Y%M%D-%h-%m-%s--%H.txt

Options

☐ Prompt for filename ○ Overwrite file

☑ Start log upon connect ● Append to file

☐ Raw log

☐ Start new log at midnight (must use %D in log file name)

Custom log data

Upon connect:

Upon disconnect:

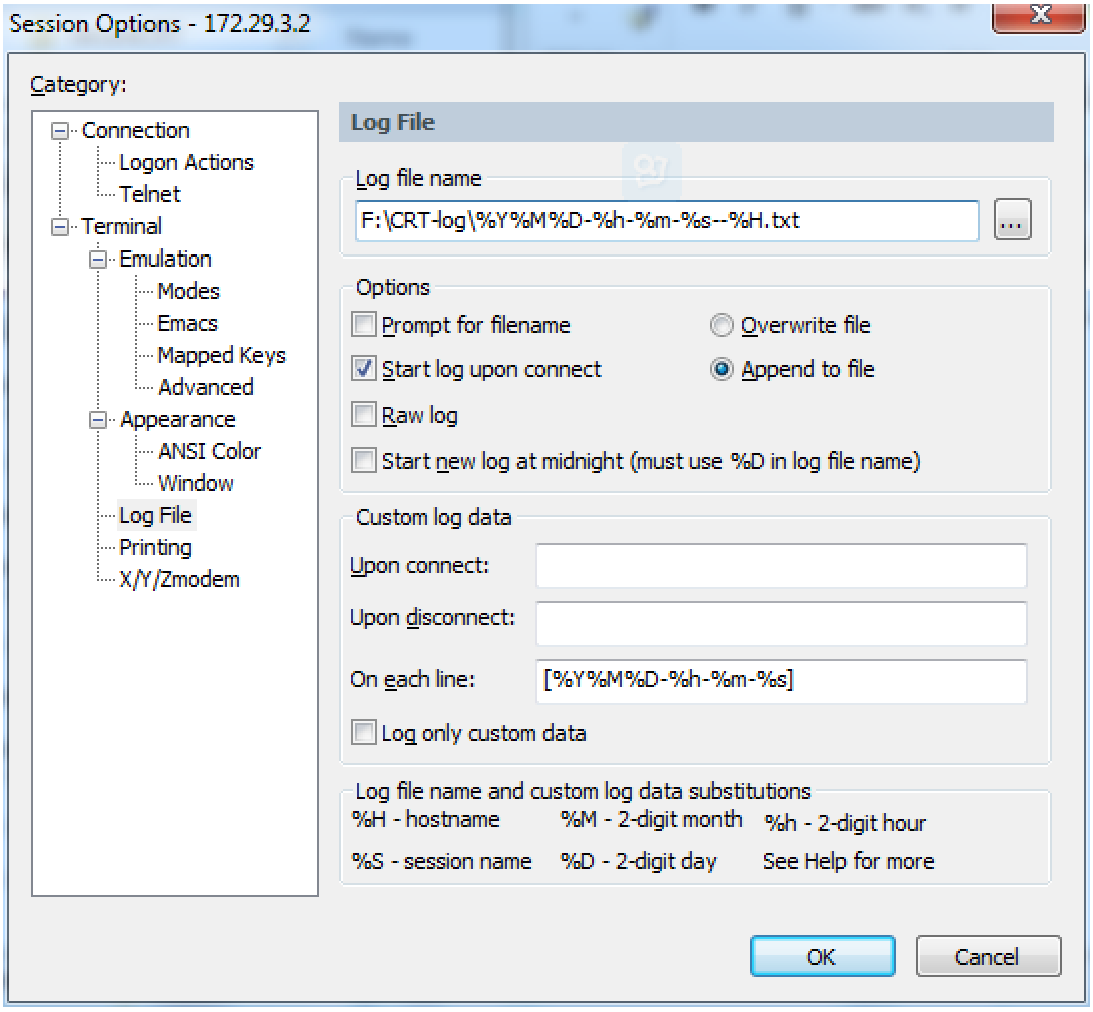
On each line: [%Y%M%D-%h-%m-%s]

☐ Log only custom data

Log file name and custom log data substitutions

%H - hostname	%M - 2-digit month	%h - 2-digit hour
%S - session name	%D - 2-digit day	See Help for more

Step3. Configure the same items in **Option** > **Session Options** > **Log File** as in step 2.



Session Options - 172.29.3.2

Category:

Log File

Log file name: F:\CRT-log\%Y%M%D-%h-%m-%s--%H.txt

Options

□ Prompt for filename ○ Overwrite file

☑ Start log upon connect ● Append to file

□ Raw log

□ Start new log at midnight (must use %D in log file name)

Custom log data

Upon connect:

Upon disconnect:

On each line: [%Y%M%D-%h-%m-%s]

□ Log only custom data

Log file name and custom log data substitutions

%H - hostname %M - 2-digit month %h - 2-digit hour

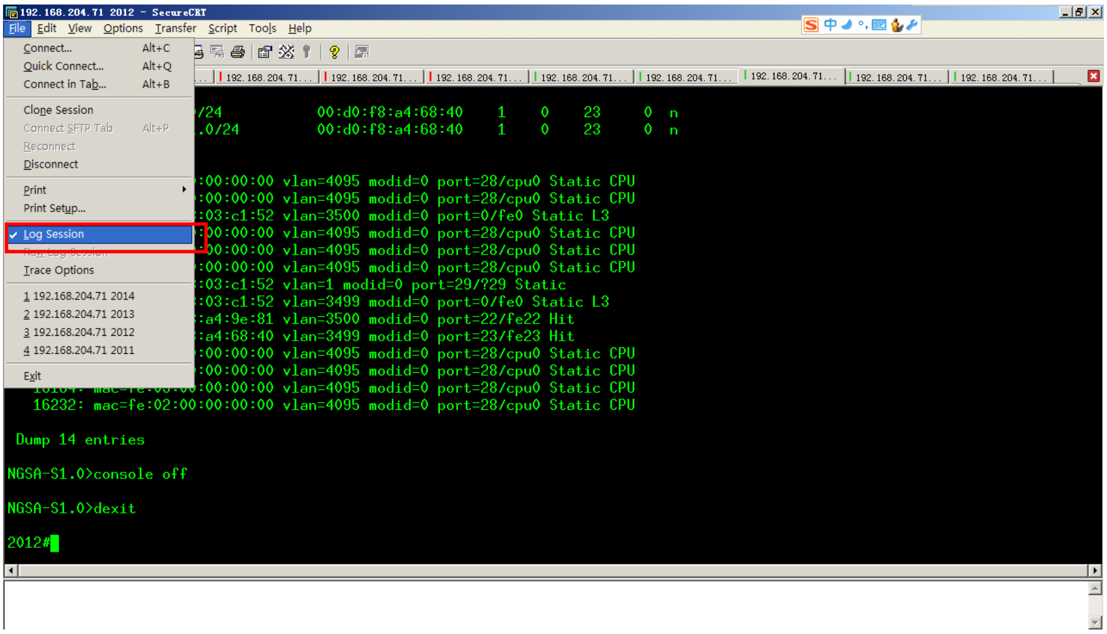
%S - session name %D - 2-digit day See Help for more

After the preceding configuration is complete, restart the SecureCRT, and the SecureCRT automatic logging takes effect. Logs generated by the SecureCRT are automatically stored in folder **F:\CRT-log**.

After the preceding configuration is complete, use the SecureCRT to record device operation logs so as to check whether the automatic logging function works properly as expected.

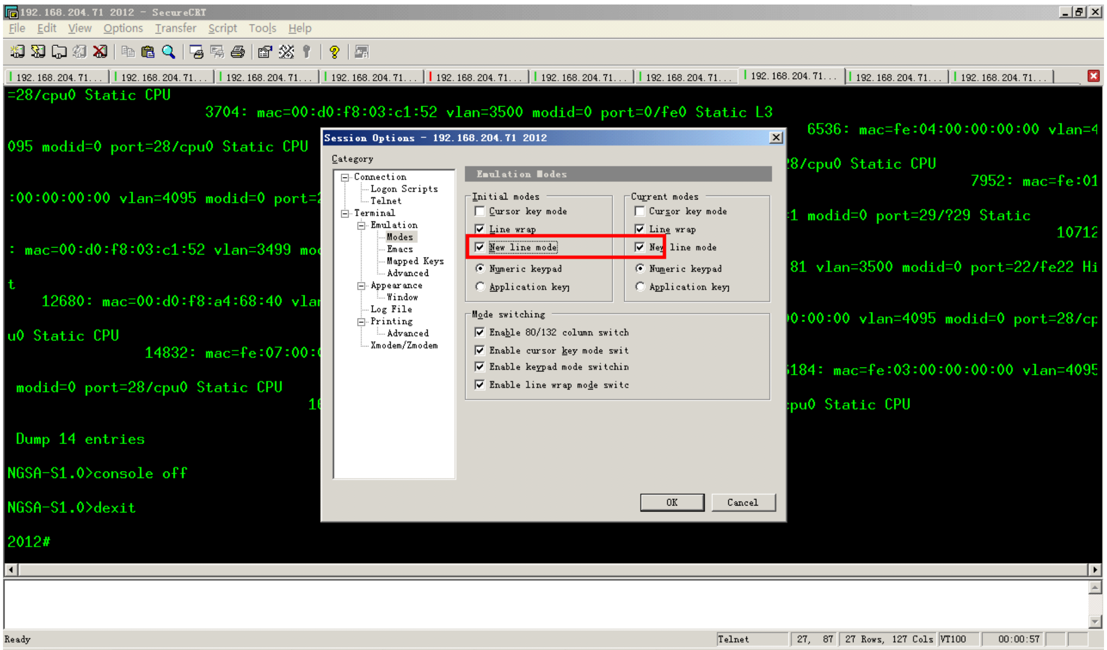
8.1.2 Running VBS script in SecureCRT

Step1. If SecureCRT logging is disabled, enter the SecureCRT to record the logs or enable automatic logging.



```
/24          00:d0:f8:a4:68:40    1    0    23     0  n
.0/24        00:d0:f8:a4:68:40    1    0    23     0  n

:00:00:00 vlan=4095 modid=0 port=28/cpu0 Static CPU
:00:00:00 vlan=4095 modid=0 port=28/cpu0 Static CPU
:03:c1:52 vlan=3500 modid=0 port=0/fe0 Static L3
00:00:00 vlan=4095 modid=0 port=28/cpu0 Static CPU
00:00:00 vlan=4095 modid=0 port=28/cpu0 Static CPU
:00:00:00 vlan=4095 modid=0 port=28/cpu0 Static CPU
:03:c1:52 vlan=1 modid=0 port=29/?29 Static
:03:c1:52 vlan=3499 modid=0 port=0/fe0 Static L3
:a4:9e:81 vlan=3500 modid=0 port=22/fe22 Hit
:a4:68:40 vlan=3499 modid=0 port=23/fe23 Hit
:00:00:00 vlan=4095 modid=0 port=28/cpu0 Static CPU
:00:00:00 vlan=4095 modid=0 port=28/cpu0 Static CPU
:00:00:00 vlan=4095 modid=0 port=28/cpu0 Static CPU
  16232: mac=fe:02:00:00:00:00 vlan=4095 modid=0 port=28/cpu0 Static CPU

 Dump 14 entries

NGSA-S1.0>console off

NGSA-S1.0>dexit

2012#
```

Step2. Choose **Option** > **Session Options**, and then select **New line mode** and **New line mode**.



Initial modes
- □ Cursor key mode
- ☑ Line wrap
- ☑ New line mode
- ● Numeric keypad
- ○ Application key

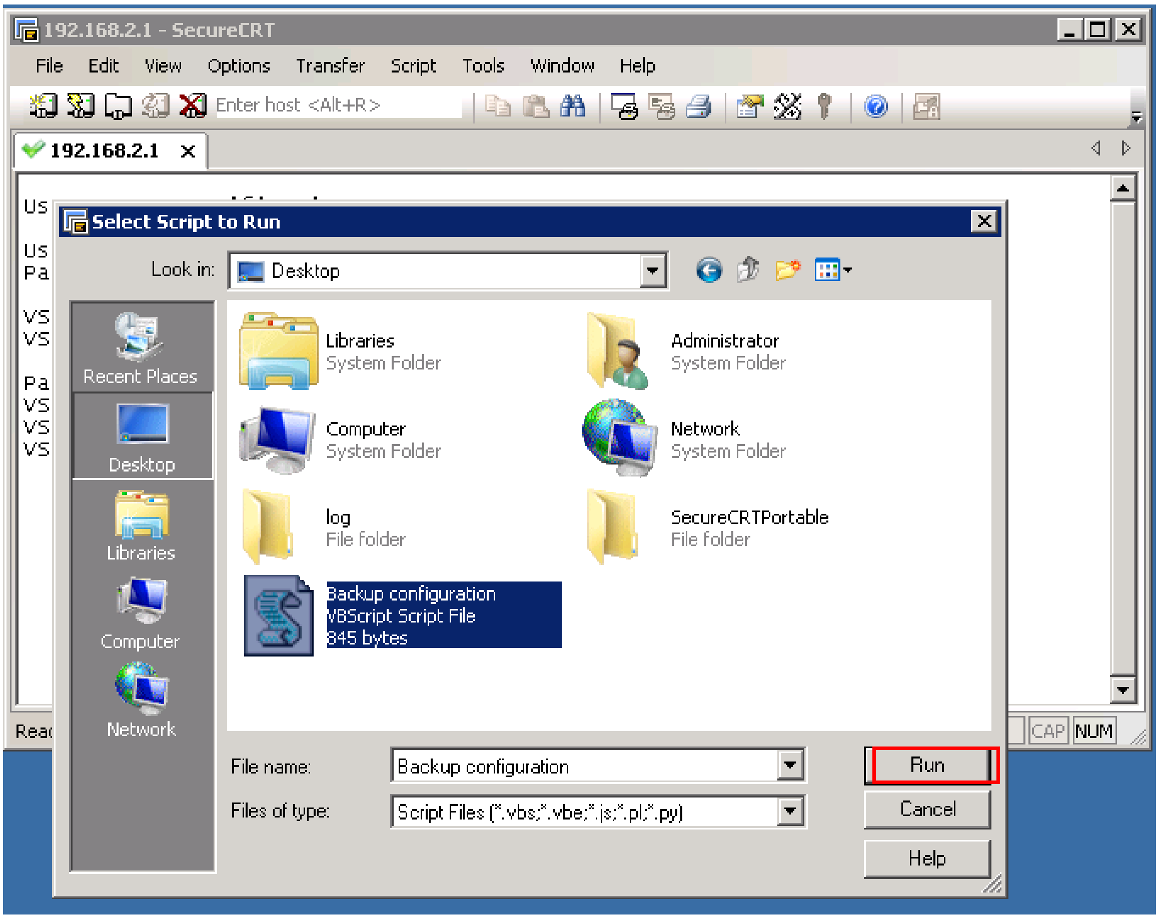
Current modes
- □ Cursor key mode
- ☑ Line wrap
- ☑ New line mode
- ● Numeric keypad
- ○ Application key

Mode switching
- ☑ Enable 80/132 column switch
- ☑ Enable cursor key mode swit
- ☑ Enable keypad mode switchin
- ☑ Enable line wrap mode switc

```
=28/cpu0 Static CPU
                        3704: mac=00:d0:f8:03:c1:52 vlan=3500 modid=0 port=0/fe0 Static L3
                                                                 6536: mac=fe:04:00:00:00:00 vlan=4
095 modid=0 port=28/cpu0 Static CPU
                                                                8/cpu0 Static CPU
                                                                            7952: mac=fe:01
:00:00:00:00 vlan=4095 modid=0 port=2
                                                                1 modid=0 port=29/?29 Static
                                                                                       10712
: mac=00:d0:f8:03:c1:52 vlan=3499 mo
                                                                81 vlan=3500 modid=0 port=22/fe22 Hi
t
    12680: mac=00:d0:f8:a4:68:40 vla
                                                                0:00:00 vlan=4095 modid=0 port=28/cp
u0 Static CPU
                14832: mac=fe:07:00:
                                                                184: mac=fe:03:00:00:00:00 vlan=4095
 modid=0 port=28/cpu0 Static CPU
                                   1
                                                                pu0 Static CPU

 Dump 14 entries

NGSA-S1.0>console off

NGSA-S1.0>dexit

2012#
```

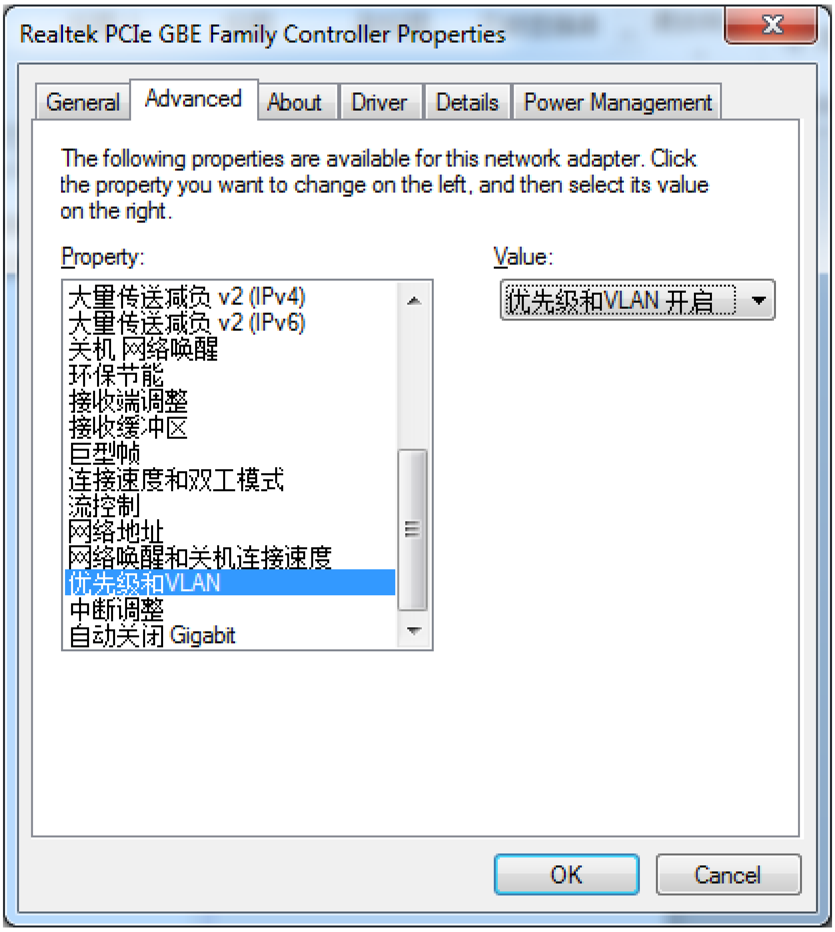
Ready   Telnet   27, 87   27 Rows, 127 Cols   VT100   00:00:57

Step3. Connect the serial cable to the console port and enter the configuration mode. Then select a script and click **Run** to run the script.


192.168.2.1 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
192.168.2.1
Select Script to Run
Look in: Desktop
Recent Places
Desktop
Libraries
Computer
Network
Libraries System Folder
Administrator System Folder
Computer System Folder
Network System Folder
log File folder
SecureCRTPortable File folder
Backup configuration VBScript Script File 845 bytes
File name: Backup configuration
Files of type: Script Files (*.vbs;*.vbe;*.js;*.pl;*.py)
Run
Cancel
Help
CAP NUM

8.2 Enable the PC to Capture VLAN-tagged Packets

Step1. Right click network adapter (**Local Connection**) and choose **Properties**. In the displayed dialog box, click **Advanced**, select **Priority and VLAN** from the **Property** drop-down list, and check whether the **Priority and VLAN** option is enabled in the **Value** drop-down list. If not, enable it and click **OK**. (If this option is unavailable, you may need to upgrade the network adapter driver to a higher version.)



Realtek PCIe GBE Family Controller Properties

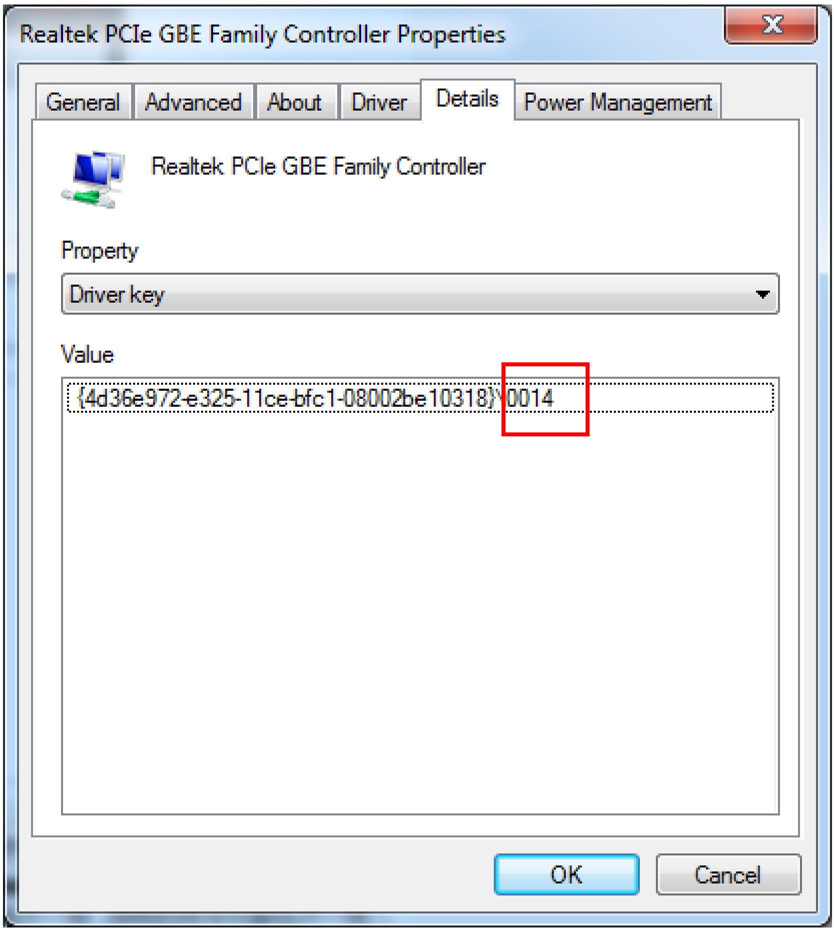
The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- 大量传送减负 v2 (IPv4)
- 大量传送减负 v2 (IPv6)
- 关机 网络唤醒
- 环保节能
- 接收端调整
- 接收缓冲区
- 巨型帧
- 连接速度和双工模式
- 流控制
- 网络地址
- 网络唤醒和关机连接速度
- 优先级和VLAN
- 中断调整
- 自动关闭 Gigabit

Value: 优先级和VLAN 开启

Step2. Right click **Local Connection** and choose **Properties**.. In the displayed dialog box, click **Details**, and select **Driver key** from the **Property** drop-down list, as shown in the following figure.



Realtek PCIe GBE Family Controller Properties

Realtek PCIe GBE Family Controller

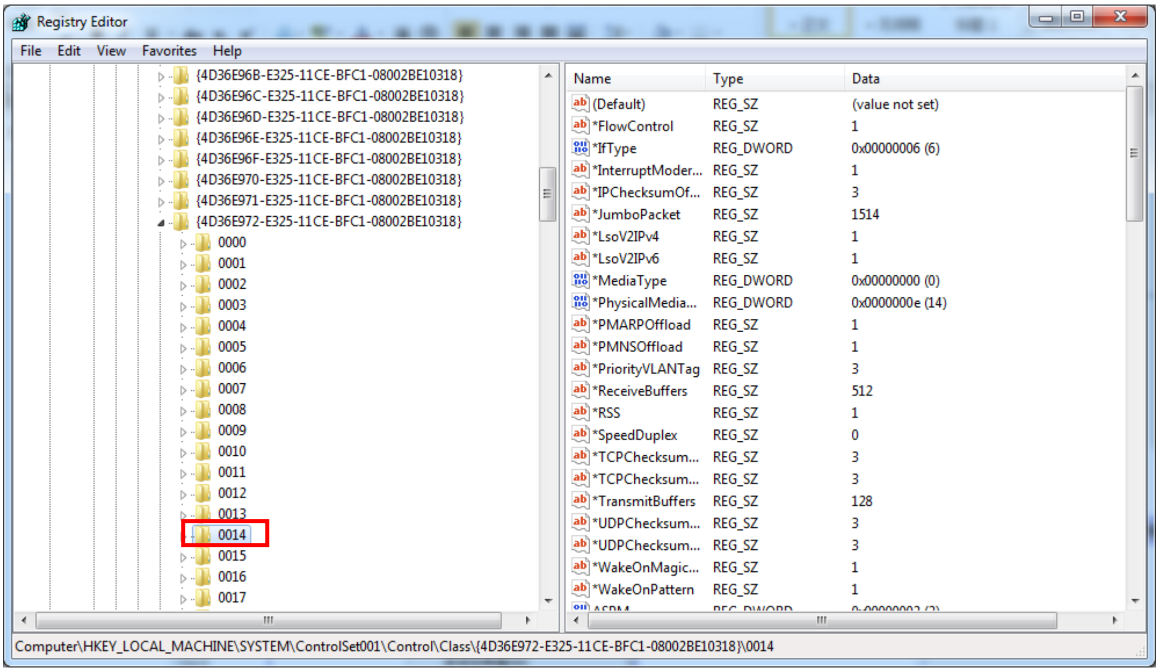
Property: Driver key

Value: {4d36e972-e325-11ce-bfc1-08002be10318}\0014

Remember the last four digits in the **Value** area, for example, 0014. This value may vary with network adapters. Even the same type of network adapters may have different values.

Step3. Start Registry Editor by clicking on **Start** > **Run**, enter **regedit i**n the **Run** text box, and then press **Enter** or click **OK**: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}

This directory has multiple files named 00*xx*. Find the folder named after the four digits in step 2, where your network adapter is located. For example, 0014.


Registry Editor
File Edit View Favorites Help
{4D36E96B-E325-11CE-BFC1-08002BE10318}
{4D36E96C-E325-11CE-BFC1-08002BE10318}
{4D36E96D-E325-11CE-BFC1-08002BE10318}
{4D36E96E-E325-11CE-BFC1-08002BE10318}
{4D36E96F-E325-11CE-BFC1-08002BE10318}
{4D36E970-E325-11CE-BFC1-08002BE10318}
{4D36E971-E325-11CE-BFC1-08002BE10318}
{4D36E972-E325-11CE-BFC1-08002BE10318}
0000
0001
0002
0003
0004
0005
0006
0007
0008
0009
0010
0011
0012
0013
0014
0015
0016
0017

Name	Type	Data
(Default)	REG_SZ	(value not set)
*FlowControl	REG_SZ	1
*IfType	REG_DWORD	0x00000006 (6)
*InterruptModer...	REG_SZ	1
*IPChecksumOf...	REG_SZ	3
*JumboPacket	REG_SZ	1514
*LsoV2IPv4	REG_SZ	1
*LsoV2IPv6	REG_SZ	1
*MediaType	REG_DWORD	0x00000000 (0)
*PhysicalMedia...	REG_DWORD	0x0000000e (14)
*PMARPOffload	REG_SZ	1
*PMNSOffload	REG_SZ	1
*PriorityVLANTag	REG_SZ	3
*ReceiveBuffers	REG_SZ	512
*RSS	REG_SZ	1
*SpeedDuplex	REG_SZ	0
*TCPChecksum...	REG_SZ	3
*TCPChecksum...	REG_SZ	3
*TransmitBuffers	REG_SZ	128
*UDPChecksum...	REG_SZ	3
*UDPChecksum...	REG_SZ	3
*WakeOnMagic...	REG_SZ	1
*WakeOnPattern	REG_SZ	1

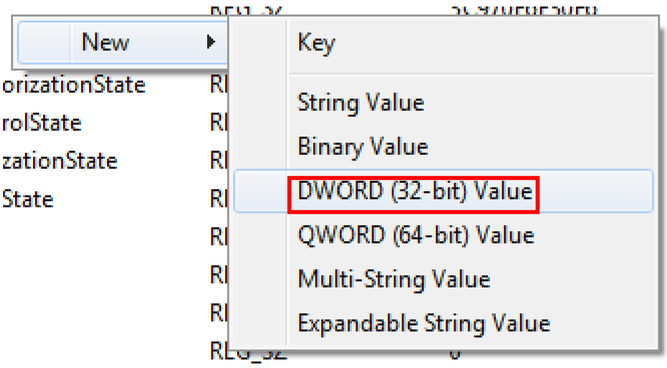
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0014

Step4. Click 00*xx* to see whether the **MonitorMode** and **MonitorModeEnabled** files exist. If not, take the following step to create them:

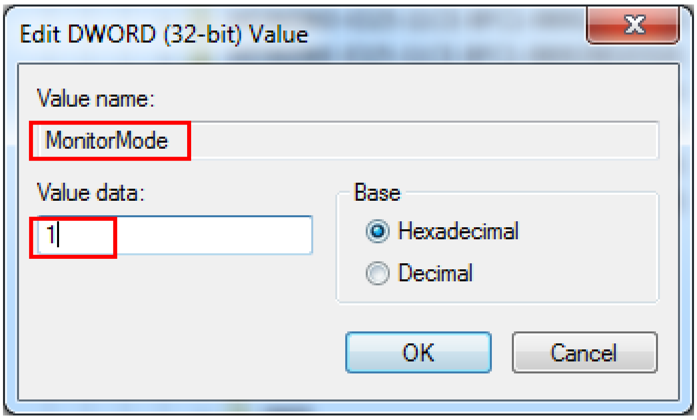
Right-click the blank area and choose **New**.

Choose **DWORD (32-bit) Value**.

(Note: 64-bit operation system should choose **DWORD (64-bit) Value**)



Name the created file **MonitorMode** and change the value data to **1**.



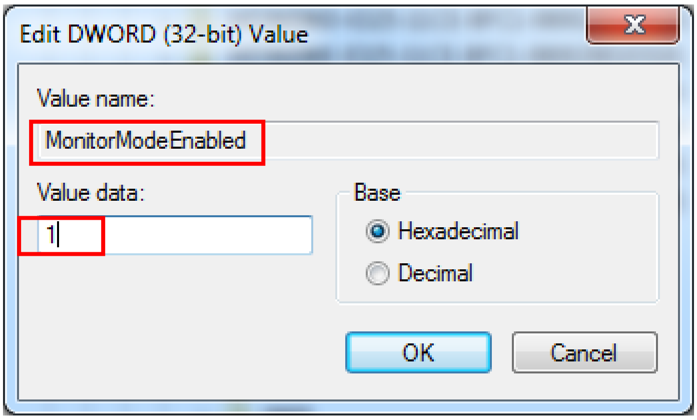
Edit DWORD (32-bit) Value

Value name: MonitorMode

Value data: 1

Base: ● Hexadecimal ○ Decimal

Create another file in the same way, name it **MonitorModeEnabled**, and change the value data also to **1**.



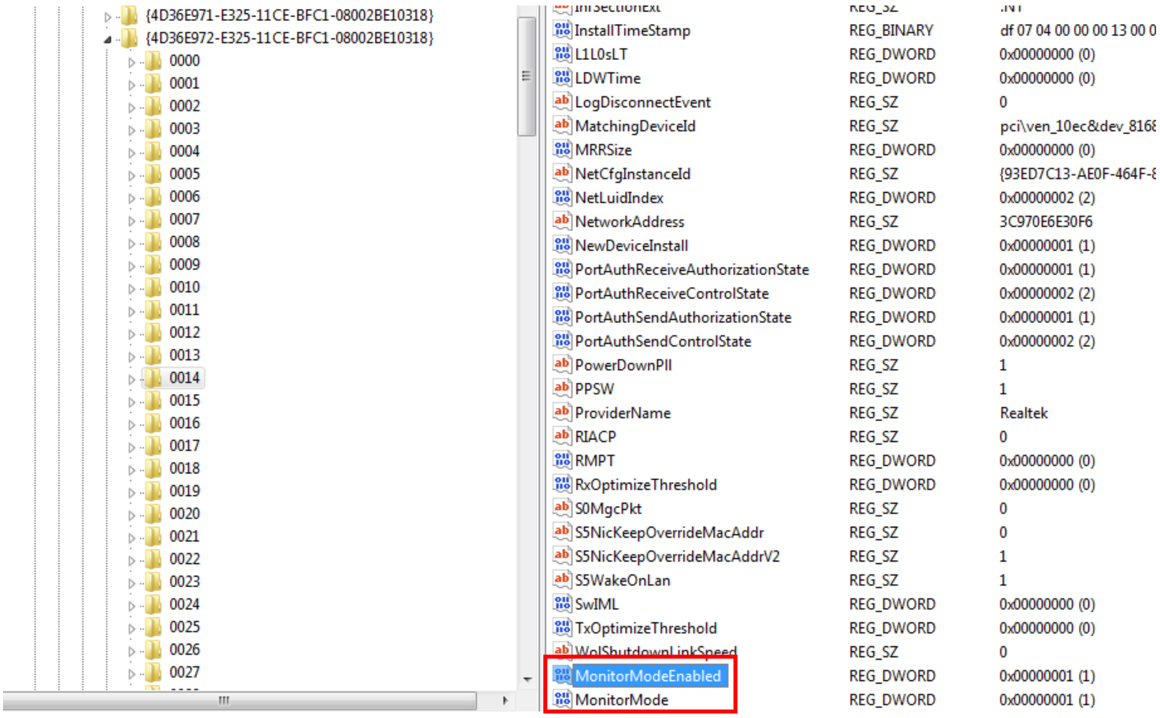
Edit DWORD (32-bit) Value

Value name: MonitorModeEnabled

Value data: 1

Base: ● Hexadecimal ○ Decimal

Then the configuration is shown as the following figure.



```
▷ {4D36E971-E325-11CE-BFC1-08002BE10318}
◢ {4D36E972-E325-11CE-BFC1-08002BE10318}
    ▷ 0000
    ▷ 0001
    ▷ 0002
    ▷ 0003
    ▷ 0004
    ▷ 0005
    ▷ 0006
    ▷ 0007
    ▷ 0008
    ▷ 0009
    ▷ 0010
    ▷ 0011
    ▷ 0012
    ▷ 0013
    ▷ 0014
    ▷ 0015
    ▷ 0016
    ▷ 0017
    ▷ 0018
    ▷ 0019
    ▷ 0020
    ▷ 0021
    ▷ 0022
    ▷ 0023
    ▷ 0024
    ▷ 0025
    ▷ 0026
    ▷ 0027
```

InfSectionExt	REG_SZ	.NT
InstallTimeStamp	REG_BINARY	df 07 04 00 00 00 13 00 0
L1L0sLT	REG_DWORD	0x00000000 (0)
LDWTime	REG_DWORD	0x00000000 (0)
LogDisconnectEvent	REG_SZ	0
MatchingDeviceId	REG_SZ	pci\ven_10ec&dev_816
MRRSize	REG_DWORD	0x00000000 (0)
NetCfgInstanceId	REG_SZ	{93ED7C13-AE0F-464F-
NetLuidIndex	REG_DWORD	0x00000002 (2)
NetworkAddress	REG_SZ	3C970E6E30F6
NewDeviceInstall	REG_DWORD	0x00000001 (1)
PortAuthReceiveAuthorizationState	REG_DWORD	0x00000001 (1)
PortAuthReceiveControlState	REG_DWORD	0x00000002 (2)
PortAuthSendAuthorizationState	REG_DWORD	0x00000001 (1)
PortAuthSendControlState	REG_DWORD	0x00000002 (2)
PowerDownPll	REG_SZ	1
PPSW	REG_SZ	1
ProviderName	REG_SZ	Realtek
RIACP	REG_SZ	0
RMPT	REG_DWORD	0x00000000 (0)
RxOptimizeThreshold	REG_DWORD	0x00000000 (0)
S0MgcPkt	REG_SZ	0
S5NicKeepOverrideMacAddr	REG_SZ	0
S5NicKeepOverrideMacAddrV2	REG_SZ	1
S5WakeOnLan	REG_SZ	1
SwIML	REG_DWORD	0x00000000 (0)
TxOptimizeThreshold	REG_DWORD	0x00000000 (0)
WolShutdownLinkSpeed	REG_SZ	0
MonitorModeEnabled	REG_DWORD	0x00000001 (1)
MonitorMode	REG_DWORD	0x00000001 (1)

Step 5. Restart the PC and capture packets to check whether the configuration takes effect.