

Common Troubleshooting Guide for FS Switches

Models: S3950-4T12S-R, S5800-48T4S, S5800-48T4S, S5800-48T4S-PE, S5800-48T4S-PE, S5800-48T4S-DC, S5800-48T4S-DC, S5800-48F4SR, S5800-48F4SR-DC, S5800-8TF12S, S5850-24S2Q-DC, S5850-24S2Q, S5850-48S6Q-R-PE, S5850-48S6Q-R-PE, S5850-24S2Q-PE, S5850-48S6Q-R, S5850-48S6Q-R, S5850-32S2Q, S5850-48S6Q, S5850-48S8C, S5850-48S8C-DC, S5850-24S2C, S5850-24S2C-DC, S5850-48S8C-PE, S5850-24S2C-PE, S5850-48S2Q4C, S5850-24T16B, S5850-48B8C, S5850-48B8C-PE, S5850-24B4C, S8050-20Q4C, S8550-32CS8550-32C-PE

Contents

Chapter 1 Management and Maintenance	1
1.1 Serial Port Login Failure.....	1
1.2 Telnet Login Failure.....	1
1.3 SSH Login Failure.....	2
1.4 Web Login Failure.....	3
1.5 Power Issue.....	3
1.6 CPU Issue.....	4
1.7 Memory Issue.....	4
1.8 Forgotten Password.....	5
1.9 File Copy Failure.....	5
1.10 Upgrade Failure.....	5
Chapter 2 Link Issue	1
2.1 The gigabit Ethernet port connection cannot be established.....	1
2.2 The gigabit fiber optic port connection cannot be established.....	1
2.3 The 10G fiber optic port connection cannot be established.....	2
2.4 The 25G fiber optic port connection cannot be established.....	2
2.5 The 40G fiber optic port connection cannot be established.....	3
2.6 The 100G fiber optic port connection cannot be established.....	3
2.7 The optical-electrical conversion for connection cannot be established.....	4
2.8 Additional Instructions for Split Ports.....	4
Chapter 3 Operating Issue	5
3.1 LACP Aggregation Failure.....	5
3.2 Unable to Ping.....	5
3.3 Operation Latency Issue.....	5
3.4 Operation Interruptions.....	6
Chapter 4 CPU Packet Capture	7
4.1 Port Mirroring.....	7
4.2 Flow Mirroring.....	7

Chapter 1 Management and Maintenance

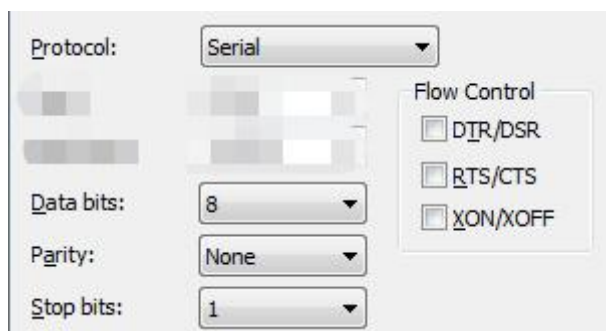
1.1 Serial Port Login Failure

Fault Symptom

Connecting to the switch through the serial port, there is no output from the serial interface, or the output is garbled.

Handling Method

1. Check whether the switch panel port connected with serial cable is proper, the one with 'CON' logo is serial port, and the one with 'ETH' logo is management port.
2. Check whether the serial port connection parameters are correct, the baud rate of S5800-8TF12S and S3950-4T12S model is 9600, and the baud rate of other models is 115200; the rest of the parameters are as follows:



The image shows a serial port configuration window. On the left, there are labels for 'Protocol:', 'Data bits:', 'Parity:', and 'Stop bits:'. To the right of these labels are dropdown menus. The 'Protocol' dropdown is set to 'Serial'. The 'Data bits' dropdown is set to '8'. The 'Parity' dropdown is set to 'None'. The 'Stop bits' dropdown is set to '1'. To the right of these settings is a 'Flow Control' section with three checkboxes: 'DTR/DSR', 'RTS/CTS', and 'XON/XOFF'. All three checkboxes are currently unchecked.

3. Confirm the signal quality of the serial line and the compatibility of the serial line. Connect other FS switches to see if the serial port has normal printing; if there is only one FS switch, try to replace the other serial line to see if it is normal.
4. Some miscellaneous brand Bluetooth serial cables purchased online may exhibit unstable RS232 voltage levels due to their non-standard design. This can result in intermittent normal and abnormal states, or situations where a particular device experiences issues that are resolved by switching to another device. When encountering such issues, it is advisable to replace the serial cable used to connect to the switch.
5. Some serial cables utilize a DB9 to USB adapter, and these adapters can become a potential point of failure due to issues such as loosening or faulty contacts. It is recommended to address these problems by either replacing the adapter or using an integrated USB to serial cable.

Troubleshooting Experience

Serial port connection failures are most likely caused by incorrect serial port parameters or incompatible serial cables. Investigate these two aspects first. If both of these factors are ruled out, then check for potential serial port issues with the individual switch.

1.2 Telnet Login Failure

Fault Symptom

Can't connect to the switch through telnet

Handling Method

Identify troubleshooting directions based on the Telnet error messages: When unable to connect via Telnet, there are two types of error messages on the screen. The first type is no response at all, resulting in a timeout. The second type displays "connection refused".

- **Timeout:**

1. Check the connectivity from the Telnet client to the switch by conducting a ping test. If the ping test fails, use traceroute to identify the network nodes causing the communication breakdown.
2. If there is an intermediate network, check for firewall settings on that network. It's possible that the firewall is blocking Telnet TCP packets while allowing ICMP packets for ping.
3. If directly connected to the switch, pay attention to whether the PC has a wireless network card. For PCs with wireless network cards, the routes to private address ranges (such as 192, 172, 10, etc.) might go through the wireless network card. In Windows, you can use the 'route print' command in CMD to check if the routing is as expected.
4. If there is an alternative way to connect to the switch or if you have a backup of the switch configuration, check if access control policies, such as black or white lists, are configured on the switch, and verify if the current PC's IP is listed in any blacklists.
5. Check the configured port number for the Telnet service on the switch; the default is 23, but it can be modified through configuration.
6. If attempting Telnet in-band, inspect the Telnet packets for CPU rate limiting. Use 'show cpu traffic-limit | inc telnet' to view the CPU rate limit on Telnet packets, and 'show cpu traffic-statistics receive | inc telnet' to check the current CPU rate for Telnet packets. If these values are close, there may be an in-band Telnet attack causing connection issues.

- **Connection Refused:**

This type of scenario indicates that there is no issue with network connectivity from the PC to the switch; rather, the switch is rejecting the TCP connection for specific reasons. You can perform the following checks:

1. **Telnet Service Status:** Verify if the Telnet service is enabled on the switch. By default, Telnet is enabled. You can use the show run command in the configuration to check for the presence of service telnet disable configuration.
2. **Telnet Service Port Number:** Examine the configured Telnet service port number on the switch. If the Telnet port number used by the PC is not being listened to on the switch, it can result in a "connection refused" situation.

Troubleshooting Experience

Investigate Telnet in relation to the PC, the intermediary network (or direct network cable), and the switch from these aspects.

1.3 SSH Login Failure

Fault Symptom

Can't connect to the switch via ssh.

Handling Method

The troubleshooting methods are similar to Telnet, with additional troubleshooting tools introduced to account for the differences between SSH and Telnet:

1. SSH has two versions: v1 and v2. By default, switches often use v2. Check the SSH version used by the PC-side software, whether it is SSHv1 or SSHv2.
2. If using SSH key authentication, it's crucial to note that Putty uses a different key format compared to other software and keys generated on switches. It's recommended to use SecureCRT or Xshell.
3. If the switch has enabled AAA (configured with aaa new-model), both RADIUS and TACACS need to use the default template for SSH login to succeed; using a custom template may impact SSH login. This is a current software limitation.

Troubleshooting Experience

Refer to telnet.

In addition, whether using Telnet or SSH, if there is a console connection or any other method to access the switch's CLI, you can attempt to Telnet or SSH to the address 127.0.0.1. If the connection fails, it indicates an issue related to the switch itself rather than external factors. Proceed to troubleshoot based on the configuration, and if the configuration is correct, seek assistance from technical support.

1.4 Web Login Failure

Fault Symptom

Can't connect to the switch via web.

Handling Method

1. Using ping to check the connectivity between the PC and the switch.
2. Checking for any firewall settings in between that might block web access.
3. Inspecting the switch configuration to see if web services are enabled. Enabling web services requires two configurations:

```
http server load flash:xxxxxxxxx
service http/https enable
```
4. Verifying the method used by the PC to access the web (using HTTP or HTTPS) and ensuring it aligns with the services enabled on the switch. For instance, if the switch enables HTTPS but the PC uses HTTP, it can result in login issues.
5. Checking if the switch has modified the default port numbers. The default port number for HTTP is 80, and for HTTPS is 443. Both can be manually configured.
6. If accessing the web via an in-band method, inspecting the CPU rate on HTTP packets to see if it has reached the limit. Using `show cpu traffic-limit | inc tcp` (displaying the first number) to view the CPU rate limit on HTTP packets and `show cpu traffic-statistics receive | inc tcp` (displaying the first number) to check the current CPU rate on HTTP packets. If these values are close, it indicates that the CPU is experiencing protocol packet impact, potentially causing connectivity issues with the web.

Troubleshooting Experience

Web-related issues and the troubleshooting approach for Telnet/SSH share certain similarities. Essentially, both involve services enabled on the switch. Based on the location of the fault, they can be categorized into issues with the intermediary network or problems with the endpoints on both sides. Intermediary network issues correspond to connectivity problems, while endpoint issues on both sides relate to access control and protocol packet impact.

1.5 Power Issue

Fault Symptom

When using the `show environment` command and observing the "Power status" section, if one of the power modules displays "FAIL" in the "Power" column or "YES" in the "Alert" column, it indicates a power-related issue.

Handling Method

1. After powering on the device, observe the indicator lights on the back of the power module. If there is no light, it indicates an interruption in the connection between the power module and the switch slot. This could be due to the power module not being securely inserted, a malfunction in the power module, or a fault in the switch slot. If the light is orange, it signifies a warning, potentially indicating a power module malfunction or a fault in the switch slot. If the light is red, it means that the power is properly connected to the switch, but there is no external power supply. This could be due to a faulty power cable, necessitating a replacement.

2. Test the problematic power module in another power module slot (which can be in another normally functioning device) and check if the show results still exhibit anomalies. This helps confirm whether the issue follows the power module.
3. Insert another functional power module into the current power module slot and check if the show results still show abnormalities. This helps confirm whether the issue follows the slot.
4. Through the cross-testing in steps 2 and 3, determine whether the problem lies with the power module or the device's power slot.

Troubleshooting Experience

The power supply for the equipment involves three factors: power cable, power module, and power slot. Perform cross-testing across these three aspects to identify the root cause of the issue.

1.6 CPU Issue

Fault Symptom

Continued CPU utilization at 100%, or even high percentages such as 80% or 90%, for an extended period without decreasing may indicate a performance issue.

Handling Method

1. Confirm the current CPU utilization through the command `show process cpu history`.
2. Use the command `show process cpu sorted` to identify which process or processes are utilizing the CPU the most.
3. Check if the in-band network is experiencing CPU impact. Use `show cpu traffic-statistics receive` to monitor the real-time CPU rates on packets. Check if one or more reasons are approaching the limits set by `show cpu traffic-limit`.
4. Examine the received packet rate on the out-of-band management interface using the results displayed in `show management interface`. Monitor the interface's packet reception statistics by consecutively executing `show` every 1 second and estimating the received packet rate. If there are thousands of packets per second, it may lead to high CPU utilization. Out-of-band management interfaces typically don't have significant traffic. In cases of unexpectedly high traffic, further investigate the cause, such as a loop in the out-of-band network.
5. Check device logs for any abnormal prints, such as MAC address drift, CPU reaching traffic limits, SSH attacks, and more.
6. Examine device services, such as SNMP, RPC-API, Web, etc., to determine if they are executing frequently. When these services are active, the switch's CPU utilization may temporarily increase to a higher value.

Troubleshooting Experience

High CPU utilization is typically caused by external factors and is often accompanied by a large number of packets impacting the CPU. By reviewing device logs and capturing packets, it is possible to identify the external factors contributing to the issue.

1.7 Memory Issue

Fault Symptom

The command `show memory summary total` indicates that the memory utilization has been consistently above 60%, or the device is logging messages indicating insufficient memory.

Handling Method

1. After executing `logging sync`, check the logs in the `flash:/syslog` file to see if there are any current abnormalities.

2. Review the historical records of SNMP monitoring for memory to determine if memory usage is gradually increasing or if there's a sudden spike at a specific time. If there's a sudden increase, examine the logs at that time and compile a list of operations performed on the switch around that time (not limited to actions directly on the switch).
3. Consider seeking technical support for further assistance.

Troubleshooting Experience

Memory utilization consistently remaining high generally indicates an abnormality. Before seeking technical support, gather necessary information.

1.8 Forgotten Password**Fault Symptom**

Forget the login password of the device

Handling Method

Connecting to the device through a serial port, if:

1. If a password is set on the serial port, preventing successful login, maintain the current serial port connection, power off the device, and restart it. During the device reboot, enter Bootrom mode to reset the password. Detailed steps can be found in the "Bootrom Mode Operation Guide."
2. If no password is set on the serial port and login is successful, reset the configurations related to the system password.
3. If interrupting power and restarting the device in step 1 poses a risk of losing unsaved configurations, consider seeking technical support.

Troubleshooting Experience

None

1.9 File Copy Failure**Fault Symptom**

Copying the new version file to the switch from an external source via FTP or TFTP, an error occurs when executing the copy command on the switch.

Handling Method

1. Check if the FTP/TFTP service on the external server is enabled.
2. Examine the external server (especially the PC) for firewall-related configurations.
3. When using a PC as an FTP/TFTP server, pay attention to the PC's wireless network card and ensure that the route to the switch's IP does not go through the wireless network card.
4. Verify that the file to be copied is located in the root directory of FTP/TFTP to prevent path errors.

Troubleshooting Experience

Based on the error message from the 'copy' command, determine which specific aspect among the points 1 to 4 mentioned above is causing the issue.

1.10 Upgrade Failure**Fault Symptom**

When executing the 'boot system' command for a version upgrade, encounter the error 'has corrupted data'

Handling Method

The specified upgrade file is currently corrupted. It is necessary to delete it and recopy the file.

Troubleshooting Experience

Even if you haven't encountered this error, it's advisable to check the integrity of the version file you are about to use for the upgrade. You can confirm this by checking the MD5 hash of the file

Chapter 2 Link Issue

2.1 The gigabit Ethernet port connection cannot be established.

Fault Symptom

The gigabit Ethernet port connection on FS switches cannot be established.

Handling Method

1. The gigabit Ethernet port supports three speeds: 10/100/1000 Mbps, with default auto-negotiation.
2. Use the command "show interface status" to check the current status of the port. "admin down" indicates that the port is configured with shutdown, "Errdisable" means the port is forcefully down due to some reason, and "down" indicates a down status for non-specific reasons. If it's in Errdisable state, use "show Errdisable recovery" to check the reason for being in Errdisable.
3. For the physical medium, use the same network cable to loop the two ports on the switch (test multiple sets) and check if the ports can come up. This helps to identify any issues with the network cable. Regarding loopback, there are two possibilities: If the loopback itself cannot come up, the cable may be faulty and needs replacement. If the loopback comes up but at 100 Mbps, it indicates that the cable can only support a link at 100 Mbps (related to the cable's own properties), and attempting to restore the connection to another device at 1000 Mbps might result in a failure to come up. In this case, test whether it comes up at 100 Mbps.
4. On the port side, try different ports to identify any issues with a specific port.

Troubleshooting Experience

1. All link-related issues follow a common troubleshooting approach, focusing on two aspects: the physical layer, which includes the physical medium, and the protocol layer, which encompasses behaviors defined by different speed protocols, such as auto-negotiation, speed, duplex, FEC (Forward Error Correction), etc.
2. For switches, the port's auto-negotiation is controlled by the configuration of the "speed" and "duplex" settings. If either is set to "auto," auto-negotiation is enabled. Auto-negotiation is only disabled when "speed" is set to a specific value (non-auto) and "duplex" is also set to a specific value (non-auto), meeting both conditions simultaneously.

2.2 The gigabit fiber optic port connection cannot be established.

Fault Symptom

The gigabit fiber optic port connection on FS switches cannot be established.

Handling Method

1. The gigabit fiber optic port supports three speeds: 10/100/1000 Mbps, with default auto-negotiation.
2. Use the command "show interface status" to check the current status of the port. "admin down" indicates that the port is configured with shutdown, "Errdisable" means the port is forcefully down due to some reason, and "down" indicates a down status for non-specific reasons. If it's in Errdisable state, use "show Errdisable recovery" to check the reason for being in Errdisable.
3. Run show transceiver eth-0-x detail to examine the current port's transmit and receive optical information, checking for any anomalies, such as a receive light level of -40, indicating no received light, meaning it cannot receive signals from the opposite end.
4. Try configuring the switch port with speed 10/100/1000 to see if the link cannot be established in all three cases.
5. Try configuring the switch port with speed 1000 and duplex full to check if the link cannot be established.
6. Attempt to replace the optical module and fiber optic cable to investigate compatibility issues and cable problems.
7. Try changing the port to see if the link cannot be established.

Troubleshooting Experience

For Gigabit Ethernet optical ports, there is a peculiar scenario: when both ends are set to a Gigabit speed, but one end has auto-negotiation enabled while the other end has it disabled. According to the protocol behavior, the end with auto-negotiation disabled will establish a link (up), while the end with auto-negotiation enabled will not establish a link (down). If you encounter a situation where one end is up and the other end is down, investigate whether this is the cause.

2.3 The 10G fiber optic port connection cannot be established.

Fault Symptom

The 10G fiber optic port connection on FS switches cannot be established.

Handling Method

1. The 10G fiber optic port supports three speeds: 1000M and 10Gbps, with default auto-negotiation.
2. Use the command "show interface status" to check the current status of the port. "admin down" indicates that the port is configured with shutdown, "Errdisable" means the port is forcefully down due to some reason, and "down" indicates a down status for non-specific reasons. If it's in Errdisable state, use "show Errdisable recovery" to check the reason for being in Errdisable.
3. Run show transceiver eth-0-x detail to examine the current port's transmit and receive optical information, checking for any anomalies, such as a receive light level of -40, indicating no received light, meaning it cannot receive signals from the opposite end.
4. Try configuring the switch port with speed 1000/ 10G to see if the link cannot be established in all three cases. When configuring speed as 1000, try both duplex auto and duplex full settings.
5. If a 10G optical module is used and the opposite end port is a 1000M port, check if the 10G optical module supports downgrading to gigabit speed.
6. Attempt to replace the optical module and fiber optic cable to investigate compatibility issues and cable problems.
7. Try changing the port to see if the link cannot be established.

Troubleshooting Experience

Refer to former passage.

2.4 The 25G fiber optic port connection cannot be established.

Fault Symptom

The 25G fiber optic port connection on FS switches cannot be established.

Handling Method

1. The 25G optical ports are set to enable auto-negotiation by default, and 25G ports have FEC parameters, with FEC auto-negotiation mode being enabled by default.
2. For some models, the 25G port works in 10G mode by default. To switch the port to 25G mode, use the "group-speed 25g" command on the interface.
3. Use the command "show interface status" to check the current status of the port. "admin down" indicates that the port is configured with shutdown, "Errdisable" means the port is forcefully down due to some reason, and "down" indicates a down status for non-specific reasons. If it's in Errdisable state, use "show Errdisable recovery" to check the reason for being in Errdisable.
4. Run show transceiver eth-0-x detail to examine the current port's transmit and receive optical information, checking for any anomalies, such as a receive light level of -40, indicating no received light, meaning it cannot receive signals from the opposite end..
5. Try configuring the switch port with speed 1000/ 10G/ 25G to see if the link cannot be established in all three cases.

When configuring the speed as 1000M, try using both duplex auto and duplex full modes (some models may not support the 1000M speed, and you can ignore the "Unsupported" error if encountered during configuration).

6. If using a 10G optical module and the opposite port is a 1000M port or another port with a speed lower than the module's speed, check if the optical module supports lowering the speed to match the port speed.
7. Additionally, attempt to configure various FEC parameters on the switch side to see if it helps bring the port up.
8. Attempt to replace the optical module and fiber optic cable to investigate compatibility issues and cable problems.
9. Try changing the port to see if the link cannot be established.

Troubleshooting Experience

Refer to former passage.

2.5 The 40G fiber optic port connection cannot be established.

Fault Symptom

The 40G fiber optic port connection on FS switches cannot be established.

Handling Method

1. The 40G optical port has self-negotiation disabled by default, and it does not support modification of this setting.
2. Use the command "show interface status" to check the current status of the port. "admin down" indicates that the port is configured with shutdown, "Errdisable" means the port is forcefully down due to some reason, and "down" indicates a down status for non-specific reasons. If it's in Errdisable state, use "show Errdisable recovery" to check the reason for being in Errdisable.
3. Run show transceiver eth-0-x detail to examine the current port's transmit and receive optical information, checking for any anomalies, such as a receive light level of -40, indicating no received light, meaning it cannot receive signals from the opposite end..
4. If a DAC cable is being used, check if the opposite end has self-negotiation enabled. If it does, the opposite end should disable self-negotiation.
5. Attempt to replace the optical module and fiber optic cable to investigate compatibility issues and cable problems.
6. Try changing the port to see if the link cannot be established.

Troubleshooting Experience

Refer to former passage.

2.6 The 100G fiber optic port connection cannot be established.

Fault Symptom

The 100G fiber optic port connection on FS switches cannot be established.

Handling Method

1. The 100G optical ports are set to enable auto-negotiation by default, and 100G ports have FEC parameters, with FEC auto-negotiation mode being enabled by default.
2. Use the command "show interface status" to check the current status of the port. "admin down" indicates that the port is configured with shutdown, "Errdisable" means the port is forcefully down due to some reason, and "down" indicates a down status for non-specific reasons. If it's in Errdisable state, use "show Errdisable recovery" to check the reason for being in Errdisable.
3. Run show transceiver eth-0-x detail to examine the current port's transmit and receive optical information, checking for any anomalies, such as a receive light level of -40, indicating no received light, meaning it cannot receive signals from the opposite end..

4. Try configuring the switch port with speed 100g/40g and duplex auto/full to check if the link cannot be established.
5. If a 100G optical module is used and the opposite end port is a 40G port, check if the 100G optical module supports downgrading to gigabit speed.
6. Additionally, attempt to configure various FEC parameters on the switch side to see if it helps bring the port up.
7. Attempt to replace the optical module and fiber optic cable to investigate compatibility issues and cable problems.
8. Try changing the port to see if the link cannot be established.

Troubleshooting Experience

Refer to former passage.

2.7 The optical-electrical conversion for connection cannot be established.**Fault Symptom**

When connecting the optical port of switch with an optical-electrical converter using an Ethernet cable on the other end, the interface fails to come up.

Handling Method

The overall approach is similar to the previous cases, with a few additional considerations:

1. When connecting an optical port to an optical-electrical converter, it can be understood as switching to electrical port properties. For electrical ports, the protocol specifies that speeds of 1 Gigabit and above only support auto-negotiation and do not support manual configuration. In other words, when connecting a Gigabit or 10 Gigabit optical port to an optical-electrical converter, switch ports cannot disable auto-negotiation, and you should not simultaneously configure "speed 1000" and "duplex full."
2. Some optical-electrical converters support speed reduction, while others do not. For example, there are optical-electrical converters for Gigabit that support 10/100/1000 and 1000 speeds, where the former can be used for 10 Mbps and 100 Mbps, and the latter only supports 1000 Mbps. A similar situation applies to 10 Gigabit optical-electrical converters. When considering speed reduction, make sure the current optical-electrical converter supports it.

Troubleshooting Experience

Refer to former passage.

2.8 Additional Instructions for Split Ports

100G and 40G ports can mostly be split into 425G or 410G. Some models split into 25G sub-ports do not support downspeed to 10G, and some split into 10G sub-ports do not support downspeed to 1000M. You can configure the interface with 'speed 10g' or 'speed 1000' to check if the interface supports the specified speed.

Chapter 3 Operating Issue

3.1 LACP Aggregation Failure

Fault Symptom

Port configured in LACP mode for aggregation, unable to successfully aggregate with the connected peer.

Handling Method

- 1、 Check the lacpdu count on the port by show lacp counters. If the received lacpdu count is not increasing, it indicates that the port is not receiving lacpdu from the peer, and you need to check the peer's configuration.
- 2、 If the show lacp counters indicate normal counts, then check show lacp internal detail to see the member ports of the switch port, whether the Actor Oper Key is consistent. If not, seek technical support.
- 3、 Check show lacp neighbor detail to see if the Partner Oper Key of each member port is consistent. If not, there may be cases where some ports are aggregated successfully, while others fail. In this case, you need to investigate on the peer side to see if the cables are connected correctly or if there are configuration errors.

Troubleshooting Experience

After the Ethernet port is up, follow the steps outlined above to troubleshoot.

3.2 Unable to Ping

Fault Symptom

If you are unable to ping a specific IP address, follow these troubleshooting steps:

Handling Method

- 1、 Check if the configurations on both ends of the link are reasonable, such as ensuring that access and trunk modes match, and VLAN configurations are consistent.
- 2、 Based on the network topology, verify if the device entries are correct.

Examine the routing table to ensure that ping packets match the correct route.

Check the ARP table to confirm the presence of the ARP entry for the next hop.

Verify the MAC address table to ensure that MAC addresses correspond to the correct ports.
- 3、 Check for ACL rules that might be blocking the traffic.
- 4、 Utilize packet capture and policy-map statistics for precise identification. Refer to the subsequent 'CPU Packet Capture' section for more details.

Troubleshooting Experience

After unsuccessful ping attempts, you can use traceroute to identify potential points of failure, and then proceed with the troubleshooting steps mentioned earlier.

3.3 Operation Latency Issue

Fault Symptom

Operation latency is significant

Handling Method

Investigating significant latency issues involves checking the following aspects:

- 1、 If it's TCP-based business, potential issues include packet reordering and packet loss. There are various reasons for packet reordering in the network, commonly stemming from improper load balancing settings or traversing through ISP lines. If packet loss is the concern, check if it's caused by sudden bursts of excessive bandwidth.
- 2、 For business packets that require processing by the switch's CPU (e.g., DHCP relay for DHCP packets), check if there are protocol packet collisions impacting the CPU (refer to the previously mentioned 'show cpu traffic-statistics receive' command).

Troubleshooting Experience

Investigate based on the operational type.

3.4 Operation Interruptions

Fault Symptom

The business experiences interruptions intermittently; using ping tests reveals noticeable packet loss.

Handling Method

Problem of packet loss, investigate from the following points:

- 1、 Check if each entry is correct. Besides the correctness of the current 'show' results, also examine if entries are fluctuating:

For the routing table, dynamic routing entries show the time since their existence, check if it's recently learned or has been there for a long time.

For the ARP table, each entry has a timer starting from the learning of ARP; if the timer is consistently at 0, it indicates continuous receipt of ARP packets for that entry.

For the MAC address table, examine logs to see if there are logs of MAC address drifting.
- 2、 Use 'show qos buffer-monitoring interface' to check the buffer usage on the interface, and use 'show qos interface eth-0-x statistics queue' to see if there is congestion-related packet loss.
- 3、 For business packets that require processing by the switch's CPU (e.g., DHCP relay for DHCP packets), check if there are protocol packet collisions impacting the CPU (refer to the previously mentioned 'show cpu traffic-statistics receive' command).

Troubleshooting Experience

Investigate based on the operational type and each entry.

Chapter 4 CPU Packet Capture

FS switches support CPU packet capture functionality, providing flexible means for network analysis.

The principle of CPU packet capture involves specifying the destination of the mirroring session as the CPU, allowing specific traffic to be mirrored to the CPU. The CPU then stores the received traffic in an internal buffer for analysis. The packets in the buffer can also be written to a flash file, which can be copied out for further analysis using Wireshark.

There are multiple packet capture methods for CPU packet capture, depending on the source of the mirroring.

4.1 Port Mirroring

Configuration Demonstration:

```
con t
```

```
monitor session 1 destination cpu - Specify the destination of the mirroring session as the CPU.
```

```
monitor session 1 source interface eth-0-16 rx - Specify the source of the mirroring session as all traffic received on port 16.
```

```
end
```

```
clear monitor cpu packet all - Clear any residual packet capture records in the buffer.
```

```
monitor cpu capture packet start - Start packet capture.
```

```
monitor cpu capture packet stop - Stop packet capture.
```

After the capture is complete, a txt file will be generated in the flash:/mirror folder.

Use the following command to convert the captured txt file to the .pcap format (note that xxx.txt corresponds to the timestamp of the recent capture):

```
Switch# pcap convert flash:/mirror/xxx.txt flash:/MirCpuPkt.pcap
```

Finally, copy the .pcap file out, and you can analyze it using Wireshark.

If you have a good understanding of packet structures, you can use the 'show monitor cpu packets all' command to view the packet structure in hexadecimal mode. An example is as follows:

```
DUT-138# show monitor cpu packet all
-----show all mirror to cpu packet info-----
packet: 1
Source port: agg1
MACDA: 0180.c200.0000, MACSA: eeee.eeee.eeee
EtherType is 0x27
Data length: 60
Data:
0180 c200 0000 eeee eeee eeee 0027 4242
0300 0002 027c 2000 001e 082c bf24 0000
07d0 4000 eeee eeee eeee 8031 0100 1400
0200 0f00 0000 0000 0000 0000
```

This method is suitable for situations with relatively low interface traffic. In cases of high interface traffic, it may not capture the desired packets accurately, and a more precise packet capture method, such as flow mirroring, might be needed.

4.2 Flow Mirroring

Compared to port mirroring, flow mirroring involves different configurations for the mirroring source, but the other steps remain the same.

ip access-list a - Configure an IP access list (ACL) to match the characteristics of the traffic:

```
permit any host 1.1.1.1 any
```

```
class-map a
```

```
match access-group a
```

```
policy-map a
```

```
class a
```

```
redirect to monitor session 1 - Specify that the matched traffic is sent to monitor session 1.
```

Finally, apply the configuration to the interface where you want to capture packets:

```
interface eth-0-16
```

```
service-policy input a
```

This means that only packets coming into port 16 with a source IP of 1.1.1.1 will be mirrored to the CPU, and other traffic will not be. Note: ACL rules should be configured with "permit" so as not to affect the normal operation of the business.

In certain scenarios, when the goal is to identify traffic based on packet counts rather than the specific, content of the packets, a slight modification to the above configuration is sufficient.

ip access-list a - Configure an IP access list (ACL) to match the characteristics of the traffic:

```
permit any host 1.1.1.1 any
```

```
class-map a
```

```
match access-group a
```

```
policy-map a
```

```
class a
```

```
statistics enable - Enable the statistics feature for the policy-map.
```

Apply this to the interface where you want to capture packets:

```
interface eth-0-16
```

```
service-policy input a
```

If traffic with the specified characteristics comes in, it will be counted in the 'show policy-map statistics input ace-based' statistics. This approach is convenient for identifying packet loss and connectivity issues. For example, you can configure an ACL to match how many packets come in and how many go out. If the number of incoming packets is equal to the outgoing packets, it indicates that there is no packet loss on this device. An example is provided below:

```
ip access-list icmp-req
```

```
permit icmp host 1.1.1.1 host 2.1.1.1 icmp-type 8
```

```
class-map req
```

```
match access-group req
```

```
policy-map req
```

```
class a
```

```
statistics enable
```

```
interface eth-0-16
```

```
service-policy input req
```

```
interface eth-0-17
```

```
service-policy output req
```

In this way, in the input direction of port 16 and the output direction of port 17, both matching ping request packets, you can specify to ping 20 packets. By using the 'show' command to check the statistics on both interfaces, you can determine

if this device has experienced packet loss.