18M2C2

Troubleshooting Guide

Models: D710 Series

Contents

1. Troubleshooting Overview

This chapter mainly introduces the concepts related to troubleshooting.

- Troubleshooting Instructions
- Troubleshooting Process
- Troubleshooting Approaches
- Common Methods for Fault localization

1.1. Troubleshooting Instructions

This manual mainly divides fault categories based on the location of the device in the network and the characteristics of networking applications, and based on some common typical problems. The fault categories are mainly divided according to the fault phenomenon. Common faults of 18M2C2 are divided into the following categories:

- System Class
- Interface Class
- Management Packet IP Forwarding and Routing

The above fault classification is mainly a simple classification of some common faults. In reality, some faults may be a collection of the above classification faults.

When a fault occurs, read the relevant chapters according to the fault phenomenon, and refer to the fault diagnosis process, troubleshooting steps, and related cases to handle the fault.

1.2. Troubleshooting Process

1.2.1. Fault Information Collection

This section mainly introduces the content of fault information collection, the source of fault information, and the necessity of fault information collection.

Contents of fault information collection

The fault information collected includes but is not limited to:

- Symptom of the fault;
- The time and frequency of the failure;
- The operations performed at or before the failure;
- Problem tracking when failures occur;
- Relevant output information when a fault occurs;
- Relevant alarm information when a fault occurs;
- Relevant log information when the fault occurs;
- Actions taken after a failure occurs;
- Equipment networking status;

- Software and hardware version information of the faulty device and related devices;
- Configuration information of the faulty device and related devices.

Source of fault information

The sources of fault information are generally the following:

- Fault reporting by users;
- Fault reporting by maintenance personnel of adjacent equipment; Equipment alarm output;
- Information collected using maintenance tools;
- Abnormalities found during routine maintenance or inspections.

Necessity of fault information collection

After a fault occurs, it is necessary to collect fault information, mainly because:

As the scale of networks expands and networking environments become increasingly complex, the causes of equipment failures become increasingly complex, increasing the difficulty of fault location. Therefore, effective and complete fault information collection is the key to fault location.

Generally, after a fault occurs, the fault phenomenon is reported via telephone, but the content collected in this feedback is not comprehensive and complete and may not directly reflect the nature of the fault.

In order to summarize the causes of the faults after troubleshooting and prevent the same faults from recurring, users need detailed fault information to discover the root causes of the faults.

1.2.2. Fault Diagnosis

Once the fault information has been obtained, you should use this information in conjunction with relevant product knowledge to make a fault diagnosis and identify the scope and type of the fault. In other words, you need to determine the range in which the fault has occurred and what type of fault it is.

1.2.3. Fault Location

The occurrence of a fault is singular at a specific time. That is to say, among many possible causes, only one cause causes the occurrence of the fault. This basic principle determines the basic method of fault location.

Fault location is the process of "finding the correct cause from many possible causes". It uses a series of methods and techniques to analyze possible causes of the fault, eliminate impossible factors of the fault, and finally determine the real cause of the equipment failure.

The fault location method also provides guidance and reference for troubleshooting.

1.2.4. Troubleshooting

After correctly locating the fault, it is time to take the most important step - troubleshooting.

Troubleshooting refers to the process of using the correct troubleshooting methods to eliminate the fault and restore the normal operation of the system after correctly locating the fault, such as repairing lines, replacing, modifying configurations, switching systems, resetting the entire machine, etc.

1.2.5. Fault Summary

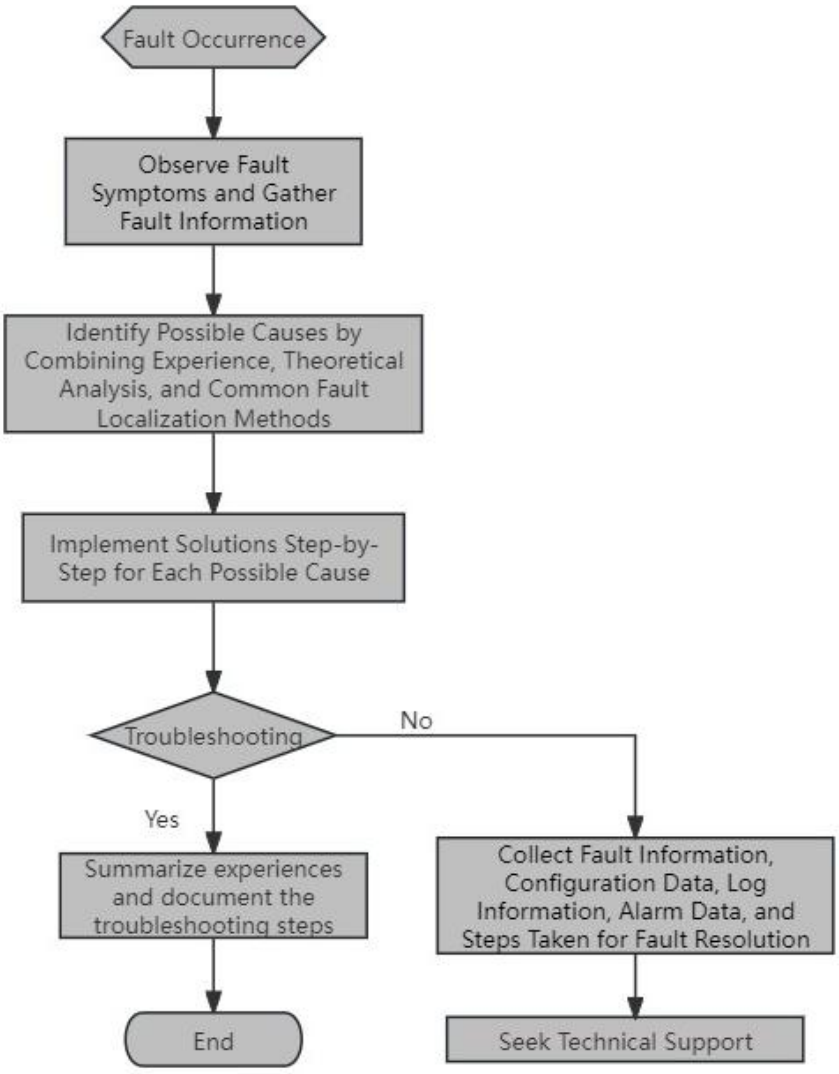
After the final troubleshooting, the last step of troubleshooting is experience summary. Experience summary is the process of documenting troubleshooting experience. This process is very necessary for the following reasons:

- The document is a summary of valuable troubleshooting experience and an important reference for future troubleshooting.
- The document records all operations and configuration changes during the troubleshooting process, which is also the basis for troubleshooting next time.

1.3. Troubleshooting Approaches

Figure 3-1 shows the troubleshooting process.

Figure 3-1 Troubleshooting Approaches



1.4. Common Methods for Fault Location

1.4.1. Signal Fow Analysis

Signal flow analysis refers to checking each part of the equipment point by point according to the business flow. Through signal flow analysis, the fault point can be located quickly.

1.4.2. Instrument Test

Instrument testing refers to the method of directly using instruments to verify equipment failures. Its main features are:

- The fault point of the device can be verified by directly testing the device.
- The requirements for maintenance personnel are relatively high.
- Fault location has some limitations. It must be equipped with professional instruments and can only verify the working status of certain components.

Note

18M2C2 intelligent transmission network series include: optical power meter, multimeter, bit error meter, etc.

1.4.3. Alarm Analysis

Alarm refers to the alarm information output by the 18M2C2 alarm system, which is usually provided to maintenance personnel in the form of sound, screen, etc. It is characterized by simplicity and clarity and is one of the main means of fault location.

When a device fails, there will usually be a large number of alarms generated. By analyzing these data, it is possible to roughly determine the type of failure and the location where the failure occurred.

There are 3 ways to obtain alarms:

- Query the current and historical alarms of the device through the network management system.
- Obtain the alarm through the status of the indicator light on the device panel.
- Obtain alarms through device log files.

Obtain fault information through alarm analysis, and the characteristics of fault location are:

- Comprehensive: The network management alarm information includes all device information.
- Accurate: The alerts reported by the network management system include the type of alert, the time of occurrence, and can also provide historical alerts.
- The communication between the equipment network management computer and the equipment is completely dependent on normal communication. Once the communication between the network management computer and the equipment fails, the ability to obtain fault information through this channel will be greatly reduced, or even completely lost.

1.4.4. Indicator Light Analysis

Indicator light analysis refers to locating faults by looking at the indicator light status on the equipment. These indicators can be used to determine the working status of the following components:

- System working status
- Port working mode and working status
- Power supply working status

Since the indicator lights provide relatively little information, a comprehensive alarm analysis method is generally required to locate equipment faults.

18M2C2 panel indicator lights, please refer to " 18M2C2 (A) Intelligent Transmission Network Series Product Description".

1.4.5. Performance Analysis

Use the performance statistics provided by the device to analyze the performance indicators of the faulty business and locate the cause of the fault.

The system performance statistics are required to locate various faults. Different statistical information needs to be viewed for different fault types, which requires maintenance personnel to be familiar with the system structure and operation mechanism, understand what statistical information the system can provide, and understand how to view and analyze the statistical information.

For example, by showing statistic [day] { client interface - number | line interface - number } { otu | transceiver } command to view interface performance statistics to determine whether the device is running normally and services are normal.

- If the number of received errored seconds or error packets increases rapidly, it indicates that the link between devices may be abnormal, the port negotiation may be incorrect, or the port may be physically faulty.
- If a large number of frame out-of-sync seconds are found, it indicates that there is a problem with the device clock function or the entire link.

1.4.6. Switching/Resetting

Switching refers to manually switching the equipment in the primary and backup working modes. In other words, the service is switched from the primary equipment to the backup equipment. When the primary equipment fails and cannot be eliminated, if the situation is urgent, the service can be switched to the backup equipment through switching.

Reset refers to the manual restart of a working device. When a device fault cannot be eliminated quickly, you can use this extreme operation to eliminate the fault. Reset operation may lose relevant data and information of the fault, which is not conducive to locating the cause of the fault and troubleshooting, so it should be avoided as much as possible.

Compared with other methods, switching and resetting cannot accurately locate the cause of equipment failure. In addition, it may conceal the nature of the failure and bring hidden dangers to the safe and stable operation of the equipment. Therefore, this method can only be used as an emergency measure and should be used with caution when it is absolutely necessary.

When using the switching and resetting methods, pay special attention to the following points:

- Back up the device configuration in advance to prevent the loss of service configuration due to reset.
- Switching and resetting will cause service interruption, and may even cause system paralysis due to improper operation. Therefore, this method is only suitable for occasions with small impact and insensitive to service interruption. Generally, it is not recommended to use the switching and resetting methods to handle faults.

1.4.7. Replacement

Replacement refers to the method of locating the fault by replacing the faulty component with a normal component when a fault occurs. The replacement method can quickly locate the fault to a certain component of the equipment and is the most commonly used fault location method. It is generally only applicable to occasions where the cause of the fault is relatively single.

For hardware failures, the replacement method is the most efficient method, which can quickly eliminate the failure and restore business. However, when using this method, you need to be careful: the replacement operation has certain risks. For example, if the optical interface module is burned due to excessive optical power, when the replacement method is used, the new optical interface module will be burned. Therefore, when using the replacement method, you must be cautious and take the premise of preventing new failures.

2. System Fault Handling

This chapter mainly introduces the location method and troubleshooting steps of system faults.

- Telnet Login Problem
- SSH login failed

2.1. Telnet Login Issues

Fault Symptom

The administrator is unable to log into the device using Telnet, or is unable to configure the device properly after logging in.

Possible Causes

The potential causes for Telnet login issues include:

- Routing issues that prevent the establishment of a TCP connection.
- The number of users logged into the device has reached its maximum limit.
- Incorrect username or password configuration.

Fault Diagnosis Process

Omitted

Troubleshooting Steps

Note:

Please preserve the results of the following steps to facilitate quick information collection and feedback if the issue remains unresolved.

Step 1: Check Network Connectivity

Ensure that the network is stable and free from intermittent connections, such as packet loss or inconsistent login issues. Use the `ping` command on the Telnet client to assess the network connection between the Telnet client and the device. If the ping fails, the Telnet connection will also be unsuccessful. Please refer to section "6.1 Ping Connectivity Issues" for further troubleshooting to establish successful ping connectivity from the Telnet client to the device.

Step 2: Check the Device's User Limit

Log into the device via the console port and execute the command `show terminal` to check if all Virtual Terminal (VT) channels are occupied. By default, the maximum number of users allowed on VT channels is 5.

Terminal	State	Time-out	User
console	active	600sec	Not Login
1-telnet	active	600sec	fscom
2-telnet/ssh	inactive	-	-
3-telnet/ssh	inactive	-	-
4-telnet/ssh	inactive	-	-
5-telnet/ssh	inactive	-	-

Step 3: Check whether the user name and password are set correctly.

Initially, the user name and password of the device are " fscom" .

You can log in to the device from the console port and use the user username password { no - encryption | md 5 } The password command creates or modifies the username and password of a login user.

Step 4: Check whether the user name and password are set correctly.

If the above steps cannot solve the problem, please collect the following information and contact FS for technical support.

- The results of executing the above steps.
- Configuration files, log information, and alarm information of the device.

2.2. SSH Login Failed

Fault Symptom

The user failed to log in to the device through SSH .

Possible Causes

The possible causes of SSH login failure include:

- Unreachable routing, preventing TCP connection establishment.
- Mismatch between server and client SSH versions.
- SSH service is not started.
- RSA public key not configured for SSH server and client.
- The number of logged-in users has reached the device's maximum capacity.

Troubleshooting Process

Omitted

Troubleshooting Steps

Note:

Please save the results of the following steps for quick information collection and feedback if the fault persists.

Step 1: Check Network Connectivity.

Use the ping command to assess network connections. If ping fails, the SSH connection will fail as well.

Step 2: Check for unstable network connections, such as packet loss or intermittent login success.

If the network is unreachable, refer to "6.1 Troubleshooting Ping Issues" to ensure the SSH client can successfully ping the SSH server.

Step 3: Check the SSH Version on the Client.

18M2C2 only supports SSHv2, so the client needs to be switched to this version.

Step 4: Verify if the SSH Service is Running.

Log into the device via the console interface and use the command `show sshd` to check the SSH server configuration information.

fscom#show sshd

SSH protocol version: 2.0 sshd running status: running

sshd current connection number: 0

hostkey RSA status: loaded

hostkey DSA status: unloaded

sshd config:

sshd port: 22

sshd max connection: 5 sshd auth maxtries: 3

sshd auth timeout: 600 seconds

hostkey file RSA: exist

hostkey file DSA: not exist

From the above information, you can see that the SSH server is enabled (status is running). Only when the system starts the SSH service can users log in. You can execute the following command to enable the SSH server.

fscom#config

fscom(config)#sshd

Step 5: Verify Local Key Pair Configuration

When the device is functioning as an SSH server, a local key pair must be configured. Execute the `show sshd` command to check for the "hostkey RSA status: loaded" message, which indicates that the local key pair is valid.

If it is not configured, log in to the device via the console and execute the command `sshd key-generate { rsa | dsa } modulus length` to create a local key pair.

Step 6: Check if the Number of Logged-in Users Has Reached the Limit

The device supports up to 5 simultaneous SSHv2 client connections. If the number of logged-in users exceeds 5, the device will not accept new user connections.

Log in to the device via the console and execute the `show sshd connection` command to check if all SSH channels are occupied.

fscom# show sshd connection

ssh connection information

ssh-conn1

status: disconnect

ssh-conn2

status: disconnect

ssh-conn3

status: disconnect

ssh-conn4

status: disconnect

ssh-conn5

status: disconnect

Step 7: Check whether the user name and password are set correctly.

If the above steps cannot solve the problem, please collect the following information and contact FS for technical support.

- The results of executing the above steps.
- Configuration files, log information, and alarm information of the device.

3. Interface Fault Handling

This chapter mainly introduces the location and troubleshooting steps of interface faults.

- Interface LoS
- The physical layer of the interface is Down
- Frequent Interface Up / Down

3.1. Interface LoS

Fault Symptoms

After connecting the cable and the device, the interface is in a LoS (Loss of Signal) state, and the interface indicator light remains solid red.

Possible Causes

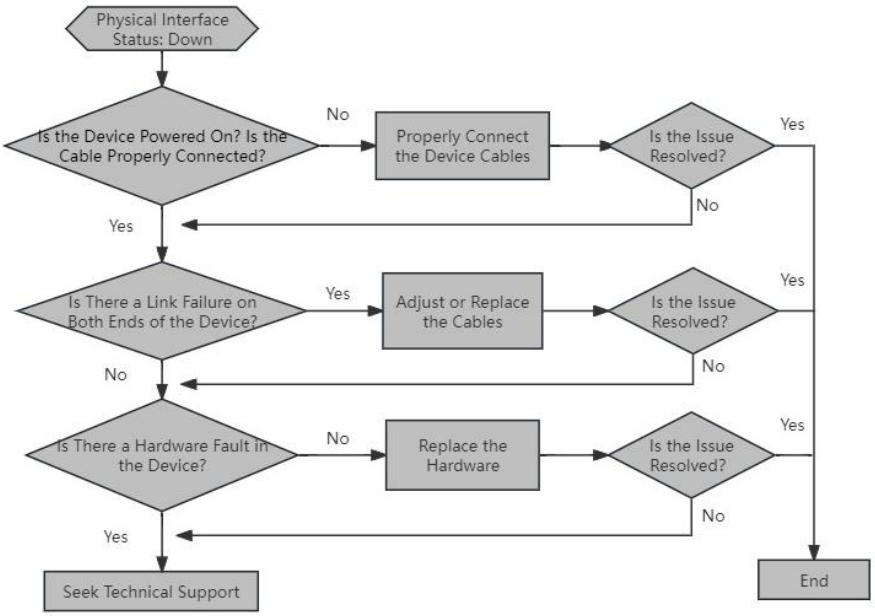
The potential causes for the interface LoS include:

- Excessive fiber length or high loss.
- Malfunctioning of the interface, interface module, or the device itself.

Troubleshooting Process

The fault diagnosis flowchart is shown in Figure 5-1.

Figure 5-1 Interface LoS fault diagnosis flowchart



Troubleshooting Steps

Note:

Please preserve the results of the following steps to facilitate quick information collection and feedback if the issue remains unresolved.

Step 1: Check whether the local and peer devices are powered on, and whether the device cables and modules are properly plugged in.

After the device is powered on and the cables are connected, if the interface status is still LoS, please perform step 2.

Step 2: Inspect both ends of the link and the interface modules for any faults.

Warning

- Exercise laser safety during all operations and maintenance. Never look directly into any optical port or fiber end, either with the naked eye or through instruments, to prevent eye damage from laser exposure.
- Before connecting a fiber, use an optical power meter to measure the current optical power. Ensure that the optical power is below the module's overload threshold before connecting; exceeding this threshold can cause errors or equipment damage, while being below the sensitivity level can interrupt services. Refer to the optical module's manual or the relevant section for technical specifications.
- Do not directly loop back with a fiber patch cord (i.e., connecting the Tx interface of an optical module directly to its Rx interface), as this can result in equipment damage.
- When using long-distance optical modules for target distances of up to 20 km, or 30 km/40 km (dual-fiber type), 40 km (single-fiber type)/60 km/80 km, and 100 km or more, always incorporate at least 5dB, 10dB, 15dB, and 20dB optical attenuators, respectively, to ensure the optical power is below the overload point but above the sensitivity threshold, before executing a loopback test with a patch cord.

Check items	Inspection Standards	Subsequent Operations
Check the correspondence between the optical module and the optical fiber.	Check whether the fiber type is correct. For the correspondence between optical module type and fiber type, see *18M2C2 Intelligent Transport Network Series Product Description* manual.	If the correspondence is incorrect, replace the optical module or optical fiber according to the actual situation.
Check whether the length of the optical fiber between devices matches the transmission distance supported by the optical module.	The length of the optical fiber is shorter than the transmission distance supported by the optical module. For the transmission distance supported by the optical module, refer to the *18M2C2 (A) Intelligent Transport Network Series Product Description* manual.	Shorten the optical fiber length or replace the optical module that supports a longer transmission distance according to the actual situation of the existing network.
Use a tester to test that the signal attenuation is within the allowable range.	For the attenuation range of optical signals, refer to the *18M2C2 (A) Intelligent Transport Network Series Product Description* manual.	If the attenuation is too large, please replace the optical fiber. If the attenuation requirement is still not met after replacing the optical fiber, please shorten the length of the optical fiber.
Use a tester or physical loopback method to check whether there is any fault at both ends of the link fiber.	When using the tester to test, the tester shows that the transmission and reception are normal. When using physical loopback, you can see that the interface indicator is off and there is no LoS alarm.	If a cable fault is found, try replacing the cable. If the fault persists after replacing the cable, try replacing the optical modules at both ends.

After performing the above steps, if the status of the interface is still LoS, perform step 4.

Step 3 Check whether the hardware of the local and peer devices is faulty.

Try connecting the cable to another interface, and if the issue persists, proceed to step 5.

Step 4 If the above steps cannot solve the problem, please collect the following information and contact FS for technical support.

- The results of executing the above steps.
- Configuration files, log information, and alarm information of the device.

3.2. The physical layer of the interface is Down

Fault Symptoms

After the cable and equipment are connected, the physical state of the interface is Down.

Possible Causes

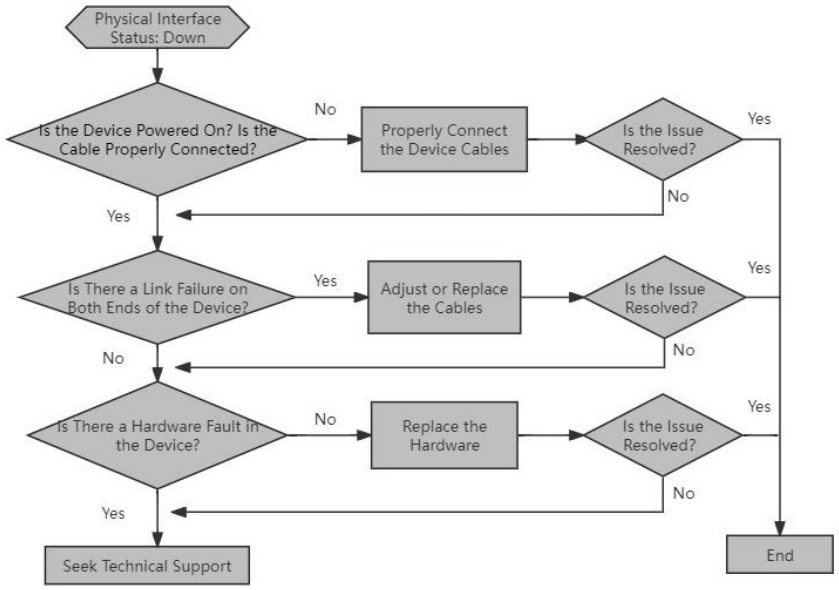
Possible reasons for the interface physical layer Down include:

- The equipment is not powered on and the cables are not connected properly.
- The interface status is Down.
- The interface duplex and rate negotiation modes are inconsistent.
- The type of connector is mismatched, the optical fiber is too long, or the loss is too large.
- Interface, interface module or equipment failure.

Fault Diagnosis Process

The fault diagnosis flowchart is shown in Figure 5-2.

Figure 5-2: Fault diagnosis flowchart for the Down fault of the interface physical layer



Troubleshooting Steps

Note:

Please preserve the results of the following steps to facilitate quick information collection and feedback if the issue remains unresolved.

Step 1: Verify that both the local and remote devices are powered on, and that all cables and modules are properly connected.

If the devices are powered on and the cables are securely connected, but the interface status remains Down, proceed to Step 2.

Step 2: Check for any faults in the link or interface modules on both ends of the connection.

Warning

- Exercise laser safety during all operations and maintenance. Never look directly into any optical port or fiber end, either with the naked eye or through instruments, to prevent eye damage from laser exposure.
- Before connecting a fiber, use an optical power meter to measure the current optical power. Ensure that the optical power is below the module's overload threshold before connecting; exceeding this threshold can cause errors or equipment damage, while being below the sensitivity level can interrupt services. Refer to the optical module's manual or the relevant section for technical specifications.
- Do not directly loop back with a fiber patch cord (i.e., connecting the Tx interface of an optical module directly to its Rx interface), as this can result in equipment damage.
- When using long-distance optical modules for target distances of up to 20 km, or 30 km/40 km (dual-fiber type), 40 km (single-fiber type)/60 km/80 km, and 100 km or more, always incorporate at least 5dB, 10dB, 15dB, and 20dB optical attenuators, respectively, to ensure the optical power is below the overload point but above the sensitivity threshold, before executing a loopback test with a patch cord.

Check items	Inspection Standards	Subsequent Operations
Check the correspondence between the optical module and the optical fiber.	Check whether the optical fiber type is correct. For the correspondence between optical module types and optical fiber types, refer to the *18M2C2 Intelligent Transport Network Series Product Description* manual.	If the correspondence is incorrect, replace the optical module or optical fiber according to the actual situation.
Check whether the length of the optical fiber between devices matches the transmission distance supported by the optical module.	The length of the optical fiber is shorter than the transmission distance supported by the optical module. For the transmission distance supported by the optical module, refer to the *18M2C2 (A) Intelligent Transport Network Series Product Description* manual.	Shorten the optical fiber length or replace the optical module that supports a longer transmission distance according to the actual situation of the existing network.
Use a tester to test that the signal attenuation is within the allowable range.	For the attenuation range of optical signals, refer to the *18M2C2 (A) Intelligent Transport Network Series Product Description* manual.	If the attenuation is too large, please replace the optical fiber. If the attenuation requirement is still not met after replacing the optical fiber, please shorten the length of the optical fiber.
Use a tester or physical loopback method to check whether there is any fault at both ends of the link fiber.	When using the tester to test, the tester shows that the transmission and reception are normal. When a physical loopback is used, you can see that the interface is Up.	If a cable fault is found, try replacing the cable. If the fault persists after replacing the cable, try replacing the optical modules at both ends.

After performing the above steps, if the interface status is still Down, perform step 4.

Step 3 Check whether the hardware of the local and peer devices is faulty.

Try connecting the cable to another interface, and if the issue persists, proceed to step 5.

Step 4 If the above steps cannot solve the problem, please collect the following information and contact FS for technical support.

- The results of executing the above steps.
- Configuration files, log information, and alarm information of the device.

3.3. Frequent Interface Up/Down

Fault Symptom

The interface frequently Up/Down.

Possible Causes

Possible reasons for frequent Up/Down of the interface include:

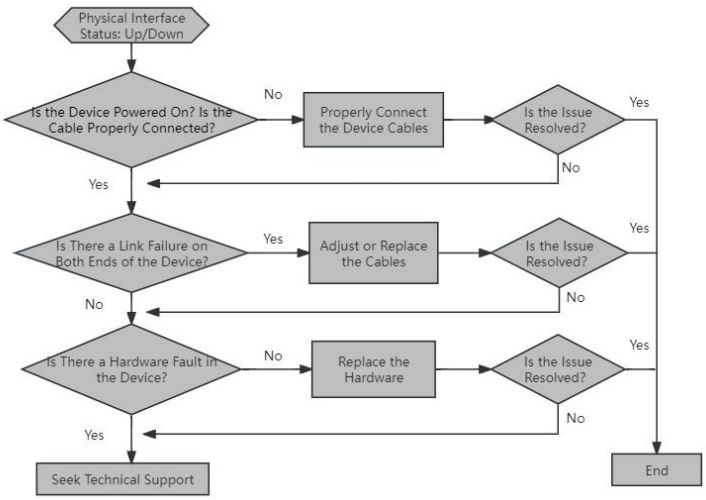
- Unreachable routing, preventing TCP connection establishment.
- Mismatch between server and client SSH versions.
- SSH service is not started.
- RSA public key not configured for SSH server and client.
- The number of logged-in users has reached the device's maximum capacity.

Troubleshooting Process

Fault diagnosis process

The diagnosis process for frequent Up/Down faults of the interface is shown in Figure 5-3.

Figure 5-3: Flowchart for diagnosing frequent Up/Down interface failures



Troubleshooting Steps

Note:

Please preserve the results of the following steps to facilitate quick information collection and feedback if the issue remains unresolved.

Step 1: Verify that both the local and remote devices are powered on, and that all cables and modules are properly connected.

If the devices are powered on and the cables are securely connected, but the interface status remains Down, proceed to Step 2.

Step 2: Check for any faults in the link or interface modules on both ends of the connection.

Warning

- Exercise laser safety during all operations and maintenance. Never look directly into any optical port or fiber end, either with the naked eye or through instruments, to prevent eye damage from laser exposure.
- Before connecting a fiber, use an optical power meter to measure the current optical power. Ensure that the optical power is below the module's overload threshold before connecting; exceeding this threshold can cause errors or equipment damage, while being below the sensitivity level can interrupt services. Refer to the optical module's manual or the relevant section for technical specifications.
- Do not directly loop back with a fiber patch cord (i.e., connecting the Tx interface of an optical module directly to its Rx interface), as this can result in equipment damage.
- When using long-distance optical modules for target distances of up to 20 km, or 30 km/40 km (dual-fiber type), 40 km (single-fiber type)/60 km/80 km, and 100 km or more, always incorporate at least 5dB, 10dB, 15dB, and 20dB optical attenuators, respectively, to ensure the optical power is below the overload point but above the sensitivity threshold, before executing a loopback test with a patch cord.

Check items	Inspection Standards	Subsequent Operations
Check the correspondence between the optical module and the optical fiber.	Check whether the optical fiber type is correct. For the correspondence between optical module types and optical fiber types, refer to the *18M2C2 Intelligent Transport Network Series Product Description* manual.	If the correspondence is incorrect, replace the optical module or optical fiber according to the actual situation.
Check whether the length of the optical fiber between devices matches the transmission distance supported by the optical module.	The length of the optical fiber is shorter than the transmission distance supported by the optical module. For the transmission distance supported by the optical module, refer to the *18M2C2 (A) Intelligent Transport Network Series Product Description* manual.	Shorten the optical fiber length or replace the optical module that supports a longer transmission distance according to the actual situation of the existing network.
Use a tester to test that the signal attenuation is within the allowable range.	For the attenuation range of optical signals, refer to the *18M2C2 (A) Intelligent Transport Network Series Product Description* manual.	If the attenuation is too large, please replace the optical fiber. If the attenuation requirement is still not met after replacing the optical fiber, please shorten the length of the optical fiber.
Use a tester or physical loopback method to check whether there is any fault at both ends of the link fiber.	When using the tester to test, the tester shows that the transmission and reception are normal. When a physical loopback is used, you can see that the interface is Up.	If a cable fault is found, try replacing the cable. If the fault persists after replacing the cable, try replacing the optical modules at both ends.

After performing the preceding steps, if the interface status still frequently changes from Up to Down , proceed to step 3.

Step 3 Check whether the hardware of the local and remote devices is faulty.

Try connecting the cable to another port. If the fault persists, proceed to step 4.

Step 4 If the above steps cannot solve the problem, please collect the following information and contact FS for technical support.

- The results of executing the above steps.
- Configuration files, log information, and alarm information of the device.

4. Management Message IP Forwarding and Routing Fault Handling

This chapter mainly introduces the location methods and troubleshooting steps for IP forwarding and routing faults.

- PING failure problem
- Traceroute is not working
- Unable to learn the peer ARP entry

4.1. PING Failure

Fault Symptom

The ping fails to reach the peer device.

Possible Causes

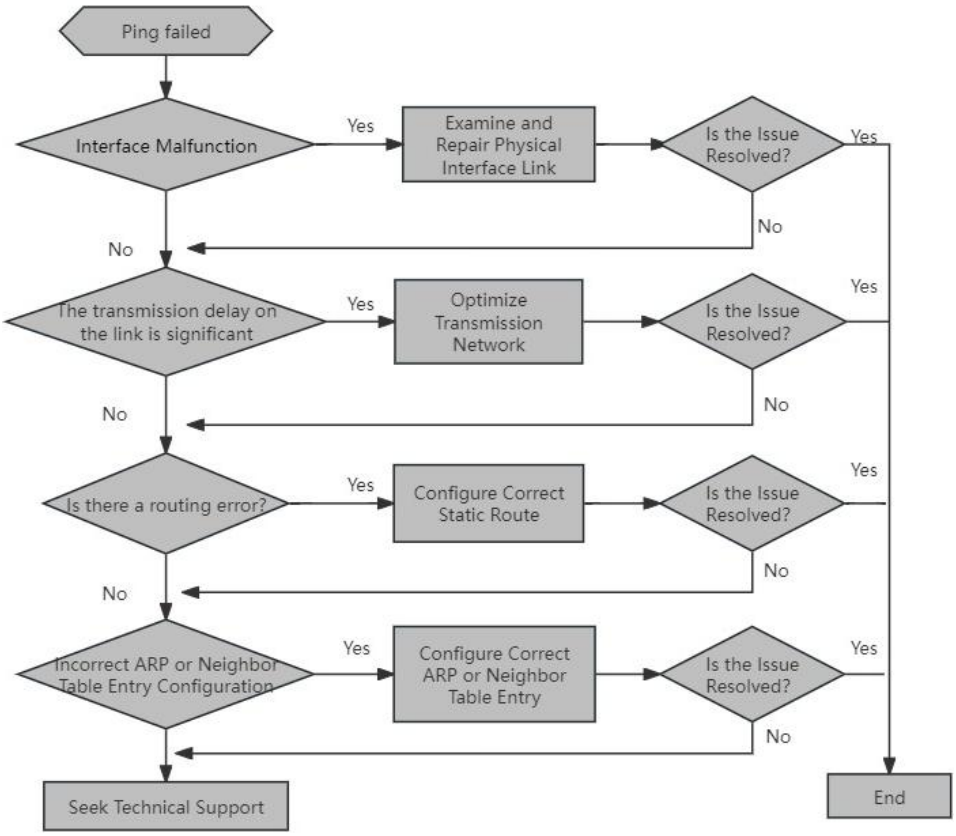
Possible reasons for being unable to ping the peer device include:

- Link problem.
- Routing problem.
- RP entries cannot be learned normally.

Troubleshooting Process

The Troubleshooting process is shown in Figure 6-1.

Figure 6-1 Troubleshooting process for PING failure



Troubleshooting Steps

Note:

Please preserve the results of the following steps to facilitate quick information collection and feedback if the issue remains unresolved.

Step 1 Check the physical layer status of the interface.

Log in to the device and execute the show interface snmp command in global configuration mode to check the physical layer status of the interface.

```
fscom# config
fscom(config)# show interface snmp Interface:snmp
    Administration Status : up Operation Status : up
    Description: snmp
    Internet address: 172.16.125.121 Netmask: 255.255.255.0
    Inet6: FE80::20E:5EFF:FE00:AA prefixLen 64
    Ethernet address: 00:0e:5e:00:00:aa
    Duplex:full-duplex                    Speed:100baseT
    Autonegotiation:enable
```

- **If it is displayed as Down, refer to "5.2 Interface Physical Layer Down" for troubleshooting.**
- **If it is displayed as Up, proceed to step 2.**

Step 2: Check if the failure to PING is caused by a long link transmission delay.

The principle of the PING process is that if a response message is received within a specified time, it indicates that the PING is successful; otherwise, it indicates a failure to PING. Therefore, if packet loss is caused by a long transmission delay, it may also lead to a failure to PING.

Execute the ping ip-address [count count] [size size] [timeout time] command in privileged mode to set the timeout for waiting for a response message from the destination, confirming whether the issue is due to a long link transmission delay. By default, the number of Ping probe packets is 4, the size is 64 bytes, and the timeout is 3 seconds.

- If the PING is successful when the timeout is set to a larger value (up to 255 seconds), it indicates a long link transmission delay, and optimization of the transmission network should be considered.
- If the PING still fails, proceed to Step 3.

Step 3: Check the routing.

Execute the show ip route command in privileged mode to check the routing tables of each device and verify the existence of complete outbound and inbound routes.

- If the corresponding routing table entry information cannot be found by executing the above command, please check whether the routing protocol configuration is correct.
- If the corresponding routing table entry information can be found, proceed to Step 4.

Step 4: Check if the destination address ARP or neighbor table entry has been learned.

Execute the show arp command in privileged mode to check if the ARP or neighbor table entry for the peer IP address has been learned.

- If the ARP or neighbor table entry for the peer IP address has not been learned, please troubleshoot the issue based on the localization approach outlined in "6.3 Failure to Learn Peer ARP Table Entries".
- If the ARP or neighbor table entry for the peer IP address has been learned, proceed to Step 5.

Step 5 If the above steps cannot solve the problem, please collect the following information and contact FS for technical support.

- The results of executing the above steps.
- Configuration files, log information, and alarm information of the device.

4.2. Traceroute Failure

Fault Symptom

Traceroute fails to reach the peer device.

Possible Causes

Possible reasons for Traceroute failure to the peer device include:

- For the same reason as PING not working, please refer to the positioning ideas in "6.1 PING not working" for more details.
- UDP message is restricted.

Troubleshooting Process

Omitted

Troubleshooting Steps

Note:

Please preserve the results of the following steps to facilitate quick information collection and feedback if the issue remains unresolved.

Step 1: Perform the same troubleshooting steps as for the PING problem.

For detailed steps, please refer to the positioning idea in "6.1 PING problem".

Step 2: Check whether UDP message transmission is prohibited in the network.

Step 3: If the above steps cannot solve the problem, please collect the following information and contact FS for technical support.

- The results of executing the above steps.
- Configuration files, log information, and alarm information of the device.

4.3. Inability to Learn Peer ARP Entries

Fault Symptom

The 18M2C2 client-side interface is connected to the peer Ethernet service device, and based on VLAN mode, it is managed in-band. It was found that the ARP entries of the peer device could not be learned.

Possible Causes

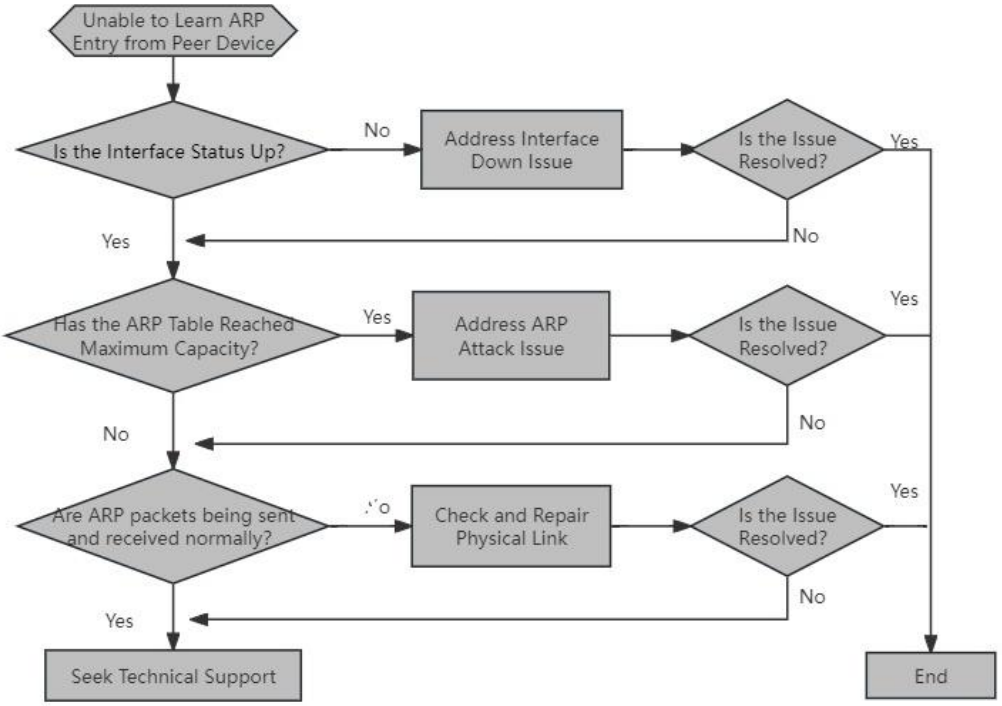
Possible reasons for not being able to learn the ARP entry of the peer include:

- The physical layer of the interface is not up normally.
- The device is under ARP attack.
- The link transmission is unstable or the optical power is insufficient.

Troubleshooting Process

The troubleshooting process is shown in Figure 6-2.

Figure 6-2: Flowchart for diagnosing the failure of the ARP entry on the peer side that cannot be learned



Troubleshooting Steps

Note:

Please preserve the results of the following steps to facilitate quick information collection and feedback if the issue remains unresolved.

Step 1: Check the physical layer status of the interface.

Log in to the device and execute the show interface command in the Client interface mode to view the physical layer status of the interface.

fscom# config

fscom(config)# interface client 1

fscom(config-client/1)# show interface The current Port mapping lan10glan:

link status : link up

ALARM status:

auto negotiation status enable : disable

transmit packet : 3701 received packet : 3453

transmit unicast packet : 3078 received unicast packet : 2963

transmit broadcast packet : 254 received broadcast packet : 139

transmit multicast packet : 369 received multicast packet : 351

transmit normal packet : 3701 received normal packet : 3453

received crc error packet : 0

RMON:

56587 octets, 3701 packets

0 undersized, 0 oversize packets

0 fragments, 0 jabbers

# of dropped packet events: 0

packet number according to length:

min-64:0,	65-127:562,	128-255:1535
256-511:1256,	512-1023:23,	1024-1518:234
1519-max:0		

IFMIB:

transmit octets : 56587 received octets : 65655

transmit error packet : 0 received error packet : 0

transmit unicast packet : 3078 received unicast packet : 2963

transmit multicast packet : 254 received multicast packet : 139

transmit broadcast packet : 369 received broadcast packet : 351

Port loopback status : no loopback

The above display information shows that the interface has been linked up.

- If it is displayed as Link Down, please refer to the positioning idea of "5.2 Interface Physical Layer Down" for handling.
- If it is displayed as Link Up, please perform step 2.

Step 2: Check whether the number of entries in the ARP mapping table has reached the maximum specification.

Execute the command show arp in privileged mode to view the current number of ARP entries in the device, and check whether it reaches the specified number of entries for the device.

fscom# show arp arp aging-time 1200 s

arp count = 25/(1000)

LINK LEVEL ARP destination	TABLE mac-addr	Interface	Flags
172.16.67.1	00:0e:5e:00:d1:32	mottsec0	UHL
172.16.67.38..	bc:30:5b:b3:ca:25	mottsec0	UHL

- If the maximum number of specifications is reached, it may be due to an ARP attack. In this case, you need to contact the network administrator to handle the ARP attack issue, or execute the arp add ip-address mac-address command in global configuration mode to configure a static ARP entry. Manually add the ARP entry for the peer device to 18M2C2.
- If the maximum number of specifications is not reached, please continue to step 3.

Step 3 Check that the ARP message is sent normally between devices.

Execute the ping ip-address command in privileged mode to ping the IP address of the peer device, which is used to trigger the local device to send an ARP request message.

- If the PING is abnormal, please check the link quality between devices, such as whether there is unstable transmission or insufficient optical power.
- If the PING is normal, please proceed to step 4.

Step 4 If the above steps cannot solve the problem, please collect the following information and contact FS for technical support.

- The results of executing the above steps.
- Configuration files, log information, and alarm information of the device.

5. Appendix

This chapter introduces the commonly used maintenance record forms and the terms and abbreviations used in this document.

- **Terminology**
- **Abbreviations**

5.1. Terminology

A	
Alarm	Information reported by a device or network management system when a fault is detected .
B	
Back Borad	A backplane is an electronic circuit board that includes wiring and sockets. Electronic devices on circuit cards can be plugged into wires and sockets. In computer systems, backplane is synonymous with or subordinate to motherboard .
C	
Current Alarm	The current alarm is defined according to the alarm operation status. Alarm events that are not filtered out become current alarms .
D	
Data Center	In the network management system, the data center is a program that provides auxiliary functions. The data center provides backup, upgrade, and Version maintenance and other functions .
E	
ES	Any second in which a bit error occurs (even if only 1 bit) is called an errored second (ES) .
F	
Frame	Data is transmitted on the network in small units called frames. A frame consists of several parts, and different parts perform different functions .
H	
History Alarm	Historical alarms are all cleared or filtered alarms .
L	
Loopback	The process of a signal returning to its original location after being sent can be used to detect Detect and analyze possible faults in the ring network .
Light Amplification by Stimulated Emission of Radiation	A device that uses external energy to maintain population inversion, provides positive feedback in an optical resonant cavity, and produces coherent light radiation through stimulated emission and amplification .

M	
Message	In the data communication field, the message structure is fixed. The header defines the destination address, and the text is the actual message, which can also include information indicating the end of the message.
Mapping	A virtual data correspondence
N	
Network Element	Network devices are managed as network elements in the network management system .
O	
Optical Power	The work done by light per unit time. The unit of optical power is milliwatt (mW) And decibel milliwatt (dBm), mW is a linear unit, dBm is a logarithmic unit, the relationship between the two is shown in the following formula. P (dBm) = 10Log (P (mW) / 1mW)
Optical Fiber	A thin filamentary optical waveguide made of dielectric material used to guide electromagnetic energy in the form of light waves .
P	
Protection Groundwire	The cable connecting the device and the protective ground is usually a yellow-green coaxial cable. To ensure that the equipment has good lightning protection, electric shock protection and anti-interference performance, grounding is required on the cabinet and the metal casing of various equipment in the cabinet .
S	
Syslog	The device log complies with the Syslog protocol format defined in RFC3164 .

5.2. Abbreviations

A	
ARP	Address Resolution Protocol
E	
ESD	Electro Static Discharge
I	
IP	Internet Protocol

R	
RH	Relative Humidity
RMON	Remote Network Monitoring
S	
SSH	Secure Shell
SSHv2	Secure Shell version 2
T	
TCP	Transmission Control Protocol
U	
UDP	User Datagram Protocol
V	
VLAN	Virtual Local Area Network