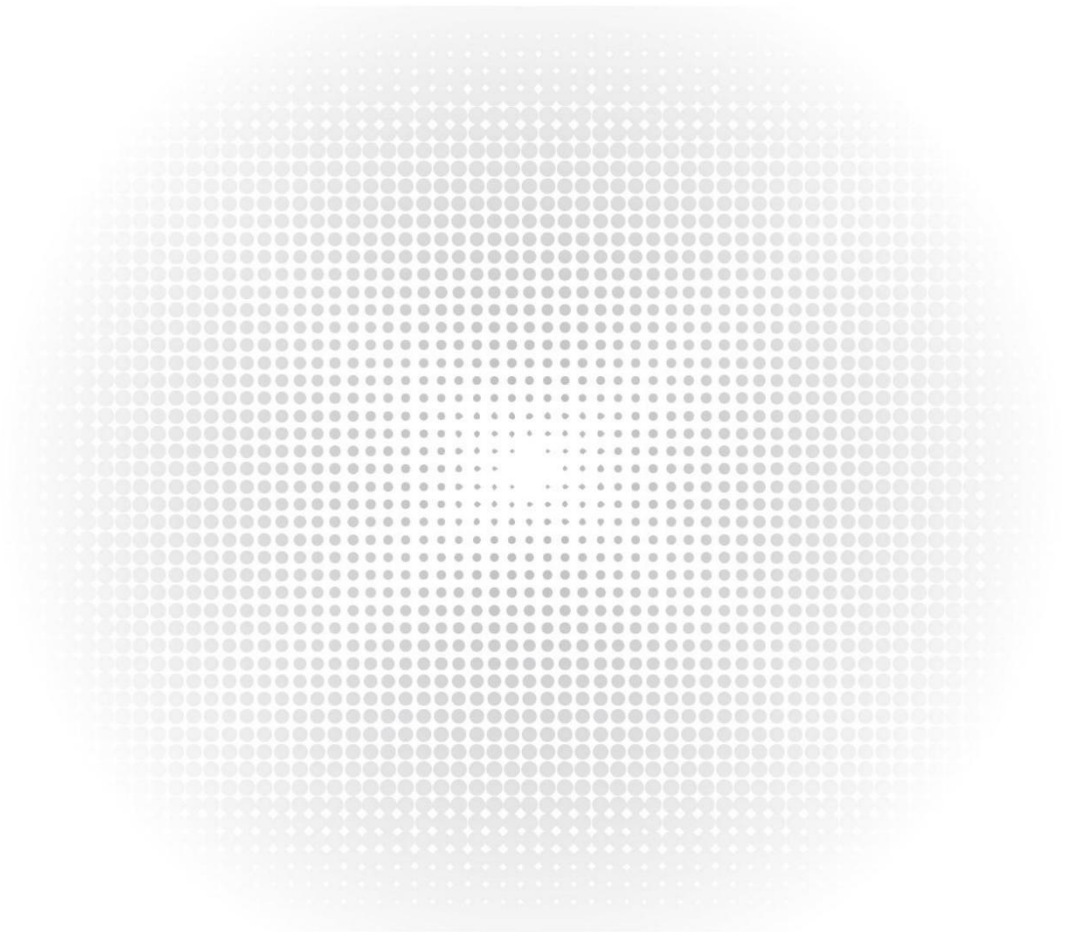
18M2C2

Management Manual

Models: D710 Series



Contents

1. Network Management Installation

1.1. Uploading Installation Files

The system supports command line installation, which requires only uploading the installation file to one server and performing one installation.

- When installing locally , you need to upload the file to the FCP MS server. When installing remotely , you need to upload the file to a Linux computer.
- The command line installation method requires that the nms_install directory in the installation file compression package be uploaded as a whole, for example, to the /usr/local directory. Then, a root user or a common user with sudo privileges can execute commands in the nms_install directory.
  - Alternatively, decompress the installation file Tar compression package on a computer and use the upload software to upload the decompressed "nms_install" directory as a whole.
  - Alternatively, use the upload software to upload the installation file compressed package, and then use the "tar –xvf compressed package file name" command to decompress it to generate the "nms_install" directory.
  - The installation file directory "nms_install" can be located in the /usr/local, /root or /home directory, but the FCP MS system installation directory must be located in the "/usr/local" directory.
- The system license file also needs to be uploaded, for example, to the /usr/local directory. In the subsequent installation process, you need to specify the directory and file name of the license file.

1.2. System Installation

1.2.1. Initial Steps

Step 1 Log in to the server as a root user or a common user with sudo privileges and go to the directory where the installation file is located, for example, /usr/local/nms_install

localhost login: root

password:

Last login: Thu Jul 12 02:55:35 2021 from 172.16.125.129

[root@localhost /]# cd /usr/local/nms_install

Step 2 Run the installation script. When you run the installation script for the first time, the system will first decompress some installation files. In non-Chinese operating system environments, you can use the sh install_en.sh command to install the system. The install_en.sh script only displays English information. Other functions are same as install.sh.

[root@localhost nms_install]# sh install.sh

Preparing the runtime environment...

Step 3 Configure the system language. The installation process and the browser interface when using the system will use this language. Or enter the language option number and click Enter, or click Enter for Chinese.

(select language)Please select the language (1: English/2: Chinese (default)):

Step 4 Configure the License Path. The filename and its case sensitivity must match the actual situation, taking /usr/local/license.xml as an example. If using an HA mode License, it will prompt "HA (High Availability Cluster)".

Please enter the license path (/usr/local/license.xml): /usr/local/license.xml

Step 5 (Optional) The NETCONF component of FCP MS is a separate component package and is applicable to devices that use the NETCONF protocol for network management. If you need to use the NETCONF component, contact technical support personnel to obtain the file and upload it to the /usr/local/ path. If only the license authorizes the NETCONF component but the component is not needed, click y to continue.

Netconf has been authorized, the component package /usr/local/netconf.tar.gz does not exist

Do you want to continue (y/n)?:

y

Step 6 Configure the system installation path. Either enter the complete directory and press Enter, or press Enter to indicate the /usr/local/nms directory.

Enter the installation path (/usr/local/nms):

Step 7 Configure the system time zone, enter the number to select the time zone of the server, and then press Enter.

Select time zone (GTM+8):

1: GTM Europe/London

2: GTM+1 Europe/Paris

3:GTM+2 Africa/Cairo

4: GTM+3 Europe/Moscow

5: GTM+4 Asia/Dubai

6:GTM+5 Indian/Maldives

7:GTM+6 Asia/Rangoon

8:GTM+7 Asia/Bangkok

9:GTM+8 Asia/Shanghai

10:GTM+9 Asia/Tokyo

11:GTM+10 Australia/Sydney

12:GTM+11 Asia/Srednekolymsk

13:GTM+12 Pacific/Auckland

14:GTM-1 Atlantic/Azores

15:GTM-2 Atlantic/South_Georgia

16:GTM-3 America/Argentina/Buenos_Aires

17:GTM-4 America/Guyana

18:GTM-5 America/New_York

19:GTM-6 America/Chicago

20:GTM-7 America/Phoenix

21:GTM-8 America/Los_Angeles

22:GTM-9 America/Anchorage

23:GTM-10 Pacific/Honolulu

24:GTM-11 Pacific/Niue

Please enter number: 9

Step 8 Configure the IP address of a third-party NTP server for system time synchronization. Enter the IP address and click Enter. This parameter should be configured with the IP address of the NTP server in the network, or left blank to indicate that no NTP server is configured. However, it cannot be configured as the IP address of the FCP MS server. Configure NTP service

Enter ntp ip:

1.2.2. Steps to Configure Deployment Parameters

After configuring the initial steps, proceed to configuring the deployment parameters .

- Installation script prompts you for deployment parameter information . You can either enter the corresponding information and press Enter, or press Enter to use the default parameters in brackets.
- Installation script displays the relevant parameters of the non-HA or HA deployment mode according to the license .
- Mass deployment mode is not currently supported.

Example for small-scale deployments

Step 1 Configure server information. The installation script displays relevant parameters based on the license.

Installation server size:

1. Small scale 2. Medium scale 3. Large scale

1

Comprehensive Server:

Enter the server (for internal use) IP: 172.16.125.210

Enter the northbound IP (172.16.125.210):

Enter the southbound IP (172.16.125.210):

Enter the SSH port (22):

Enter SSH username : root

Enter SSH password :

Note

- The northbound IP address refers to the IP address of the FCP MS northbound interface.
- The southbound IP address refers to the IP address of the southbound interface of the FCP MS .
- When configuring the northbound IP and southbound IP, either enter the IP address of the FCP MS server network card or press Enter to use the IP address in brackets. If there is no clear requirement, just press Enter.

Example for medium-scale deployments

Step 1 Configure the integrated server information. The IP addresses of the integrated server are used by the client , northbound interface, and southbound interface . The installation script displays the relevant parameters according to the license.

Installation server size:

1. Small scale 2. Medium scale 3. Large scale

2

Comprehensive Server:

Enter the server (for internal use) IP: 172.16.125.210

Enter the northbound IP (172.16.125.210):

Enter the southbound IP (172.16.125.210):

Enter the SSH port (22):

Enter SSH username: root

Enter SSH password:

Step 2 Configure Pre-deployment Database Information. The pre-deployment database is applicable in scenarios that use independent databases during the construction planning phase. This database is provided by other servers or vendors

to serve as the database for the FCP MS system. The pre-deployment database is not controlled by the FCP MS system and its normal operation must be ensured by the provider of the pre-deployment database.

- Example of not using a pre-deployment database: The database is installed along with the installation process of the FCP MS system.

Use a pre-deployment database (y/N): n
Database Server:
Enter Server (Internal Use) IP: 172.16.125.211
Enter SSH Port (22):
Enter SSH Username: root
Enter SSH Password:

- Example of using a pre-deployment database: The pre-deployment database includes 2 database instances, used for the FCP MS system and PM service, with default port numbers 23306 and 23308, respectively.

Use a pre-deployment database (y/N): y
Pre-deployment Database:
Enter Database IP: 172.16.125.220
Enter Platform Database Port (23306):
Enter Platform Database Username: admin
Enter Platform Database Password:
Enter Performance Database Port (23308):
Enter Performance Database Username: admin
Enter Performance Database Password:

Step 3 Configure the PM server. By selecting the deployment node number, you can select the server where the PM is located. Please select the same server for PM and integrated services.

- Example of deploying PM without using a pre-deployment database:
  PM Server:
  Please select the deployment node [1, 172.16.125.210; 2, 172.16.125.211]:
  Enter the number (2): 1
- Example of deploying PM on the same server with comprehensive services when using a pre-deployment database:

  PM Server:

  Please select the deployment node [1, 172.16.125.210, 2, other servers]:

  Please enter the serial number: 1

Example for small-scale HA deployment

Step 1 Configure comprehensive server information and VIP information. The installation script displays relevant parameters based on the license of the HA deployment mode.

1. Small scale 2. Medium scale 3. Large scale

1

Main integrated server:

Enter the server (for internal use) IP: 172.16.125.210

Enter the northbound IP (172.16.125.210):

Enter the southbound IP (172.16.125.210):

Enter the SSH port (22):

Enter SSH username: root

Enter SSH password:

Backup integrated server:

Enter server (internal use) IP: 172.16.125.211

Enter the northbound IP (172.16.125.211):

Enter the southbound IP (172.16.125.211):

Enter the SSH port (22):

Enter SSH username: root

Enter SSH password:

Please select VIP option

1: Create a new VIP

2: Cancel

1

Enter the virtual IP (VIP): 172.16.125.230

Bind the network card IP on the host (172.16.125.210):

Bind the network card IP on the standby machine (172.16.125.211):

Subnet mask (1~31): 24

VIP gateway: 172.16.125.231

virtual ip description: vip1

Please select VIP option

1: Create a new VIP

2: Cancel

1

Enter the virtual IP (VIP): 172.16.125.240

Bind the network card IP on the host (172.16.125.210):

Bind the network card IP on the standby machine (172.16.125.211):

Subnet mask (1~31): 24

VIP gateway: 172.16.125.241

virtual ip description: vip2

Please select VIP option

1: Create a new VIP

2: Cancel

2

Please configure internal use vip:

Optional VIPs for internal use are:

[1.172.16.125.230 2.172.16.125.240]

Please enter the serial number: 2

- Internal VIP refers to the server internal communication VIP.
- In the entire system, there must be only one internal communication VIP, and the internal communication VIP cannot be the same as the southbound VIP.
- The IP address of the northbound VIP and the southbound VIP cannot be the same as the IP address of the VIP gateway.
- The VIP must be an IP address that is not already in use on the server network .

Step 2 (Applicable to the case of using northbound VIP and southbound VIP) After configuring VIP, specify the configured VIP address for the system southbound interface or northbound interface.

Use pre-deployed database (y/N): y

The optional VIPs are: [1, 172.16.125.230 2, 172.16.125.240]

Please enter the serial number: 1

Do you want to configure southbound VIP? (y/N): y

The optional VIPs are: [1, 172.16.125.230 2, 172.16.125.240]

Please enter the serial number: 1

Example for medium-scale HA deployment

Step 1 Configure comprehensive server information. The installation script displays relevant parameters based on the license of the HA deployment mode.

Installation server size:

1. Small scale 2. Medium scale 3. Large scale

2

Main integrated server:

Enter the server (for internal use) IP: 172.16.125.210

Enter the northbound IP (172.16.125.210):

Enter the southbound IP (172.16.125.210):

Enter the SSH port (22):

Enter SSH username: root

Enter SSH password:

Backup integrated server:

Enter server (internal use) IP: 172.16.125.211

Enter the northbound IP (172.16.125.211):

Enter the southbound IP (172.16.125.211):

Enter the SSH port (22):

Enter SSH username: root

Enter SSH password:

Step 2 Configure the pre-deployment database information. The pre-deployment database is suitable for scenarios where an independent database is used in the construction plan. The pre-deployment database is provided by other servers or manufacturers as the database of the FCP MS system . The pre - deployment database is not controlled by the FCP MS system, and the provider of the pre-deployment database must ensure the normal operation of the pre-deployment database .

- Example Without Pre-Deployed Database. The database is installed during the installation of the FCP MS system .

Use pre-deployed database (y/N): n

Primary Database Server:

Enter server (internal use) IP: 172.16.125.212

Enter SSH port (22):

Enter SSH username: root

Enter SSH password:

Secondary Database Server:

Enter server (internal use) IP: 172.16.125.213

Enter SSH port (22):

Enter SSH username: root

Enter SSH password:

- Example With Pre-Deployed Database. The pre-deployed setup includes two database instances, intended for the FCP MS system and the PM service, with default port numbers 23306 and 23308, respectively.

Use pre-deployed database (y/N): y

Pre-Deployed Database:

Enter database IP: 172.16.125.220

Enter the platform database port (23306):

Enter the platform database username: admin

Enter the platform database password:

Enter the performance database port (23308):

Enter the performance database username: admin

Enter the performance database password:

Step 3 Configure the PM server. By selecting the deployment node number, you can select the server where the PM is located. Please select the same server for PM and integrated services.

- Example of deploying PM without using a pre-deployment database:

PM Server:

Please select deployment nodes [1, (172.16.125.210, 172.16.125.211), 2, (172.16.125.212, 172.16.125.213):

Please enter the serial number (2): 1

- Example of deploying PM and integrated services on the same server when using a pre-deployed database.

PM Server:

Please select deployment node [1, (172.16.125.210, 172.16.125.211), 2, other servers]:

Please enter the serial number: 1

Step 4 Configure VIP information.

Please select VIP option

1: Create a new VIP

2: Cancel

1

Enter the virtual IP (VIP): 172.16.125.230

Bind the network card IP on the host (172.16.125.210):

Bind the network card IP on the standby machine (172.16.125.211):

Subnet mask (1~31): 24

VIP gateway: 172.16.125.231

virtual ip description: vip1

Please select VIP option

1: Create a new VIP

2: Cancel

1

Enter the virtual IP (VIP): 172.16.125.240

Bind the network card IP on the host (172.16.125.210):

Bind the network card IP on the standby machine (172.16.125.211):

Subnet mask (1~31): 24

VIP gateway: 172.16.125.241

virtual ip description: vip2

Please select VIP option

1: Create a new VIP

2: Cancel

2

Please configure internal use vip:

Optional VIPs for internal use are:

[1.172.16.125.230 2.172.16.125.240]

Please enter the serial number:2

Step 5 (Applicable to the case of using northbound VIP and southbound VIP) After configuring VIP, specify the configured VIP address for the system southbound interface or northbound interface.

Configure northbound VIP? (y/N): y

The optional VIPs are: [1, 172.16.125.230 2, 172.16.125.240]

Please enter the serial number: 1

Do you want to configure southbound VIP? (y/N): y

The optional VIPs are: [1, 172.16.125.230 2, 172.16.125.240]

Please enter the serial number: 1

1.2.3. Steps to Confirm and Execute the Installation

Step 1 After configuring the relevant parameters of the deployment mode, click Enter to display the installation parameters that have been entered and are to be confirmed. After confirmation, enter y and click Enter to execute the installation. If you enter n, the installation script will exit. Here, a small-scale deployment is used as an example. The confirmation information for other deployment modes is similar, and all are the parameter information entered previously.

Input parameter confirmation

Language: Chinese (default)

license: /usr/local/license_one.xml

Installation method: Non-HA

Installed to: /usr/local/nms

NTP Server:

Time zone: Asia/Shanghai

Comprehensive Server:

Server (internal use) IP: 172.16.125.210

Northbound IP: 172.16.125.210

Southbound IP: 172.16.125.210

SSH Port: 22

SSH Username: root

SSH password:***

Confirm(Y/n):y

Step 2 The system starts to perform checks and automatically executes all installation processes.

Installation will begin

Start checking server status

172.16.125.210 ssh connection successful

172.16.125.210 Check sudo permissions

172.16.125.210 Check the configuration ip

172.16.125.210 Check the mark file /var/install_mark.json

172.16.125.210 Check the installation path /usr/local/nms

172.16.125.210 Check component uninstall remnants

172.16.125.210 Check database data files

172.16.125.210 Check disk space

172.16.125.210 Check passed

All inspections passed

172.16.125.210 ssh connection successful

172.16.125.210 /usr/local/nms/ has been created and components are installed.

…

Complete installation

Note:

If residual data of the old version is detected in the directory, the installation script will prompt and exit the installation. In this case, the user needs to manually delete all files of the old version before performing the installation.

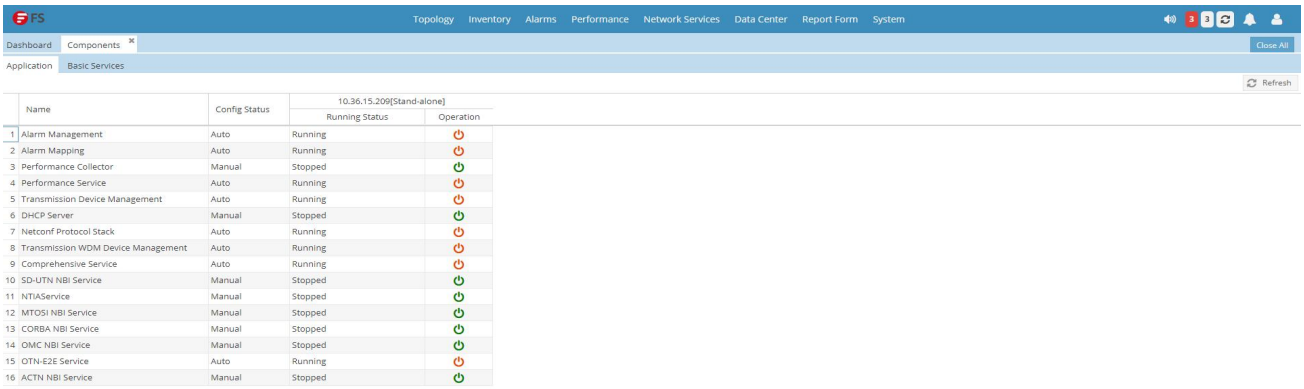
1.3. Checking the Installation Status

Step 1 Access the server IP address where the integrated service is located through a browser, and the login interface

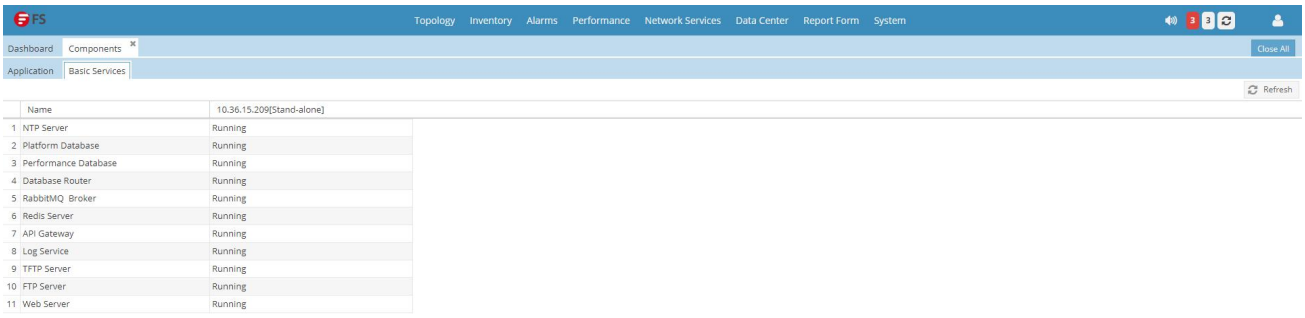
should be displayed.

Step 2 Enter the default username " administrator " and password " admin@fs.com " to log in to the system.

Step 3 In the top navigation, click <System>, then click [System Management/Component Management] in the left navigation tree, click the "Application Components " tab, and check the "Running Status" of the started components . All of them should be displayed as "Running", as shown in the following figure. Some components are stopped by default . To start a component, click < >.



Step 4 Click the Basic Services tab and check the service status, which should be displayed as Running, as shown in the following figure.



1.4. Upgrading Via the Installer

After installation and deployment, you can use the higher-version installer to install the higher-version program again, that is, upgrade the network management system through the installer.

- For network management systems in various installation and deployment modes that can operate normally, they can all be upgraded through the installation program.
- Since program files need to be processed, the network management system cannot be used during the upgrade process.

Step 1 Check the current status of the system. Before upgrading the system through the installation program, the system must be able to be used normally.

Step 2 Unzip the higher version installer to the / root/ directory.

Step 3 Use the "cd nms_instal" command to enter the decompressed program directory.

Step 4 When you run the installation script for the first time , the system will first decompress some installation files . In a non-Chinese operating system environment, you can use the sh install_en.sh command to install the system. The install_en.sh script only displays English information and its other functions are the same as install.sh .

[root@host1721668112 nms_install]# sh install.sh

Preparing the runtime environment...

Step 5 Enter 1 to configure the upgrade function.

Please select (1: Upgrade/2: Uninstall): 1

Step 6 After confirming the upgrade information, enter y and press Enter to execute the installation.

Upgrade information confirmation

Language : Chinese (default)

Installation method : Non-HA

Installed to : / usr/local/nms

IP:172.16.68.112

SSH port: 2 2

Username: admin

Current version:

systemversion : 20221212143659

platform : 2.2.0

WDM : 3.0.1

TRANS : 3.2.0

SWITCH : 2.2.0

PON : 2.2.0

PM2000 : 2.2.0

MSG : 2.2.0

Upgraded version:

systemversion : 2 0230328184331

platform : 2.2.1

WDM : 3.1.0

TRANS : 3.2.1

SWITCH : 2.2.0

PON ： 2.2.0

PM2000 : 2.2.0

MSG : 2.2.0

Confirm (Y/n): y

Step 7 The system starts to perform checks and automatically executes all installation processes.

Installation will begin

Start checking server status

172.16.68.112 ssh connection successful

172.16.68.112 Check sudo permissions

172.16.68.112 Check the configuration ip

172.16.68.112 Check the mark file /var/install_mark.json

172.16.68.112 Check the installation path /usr/local/nms

172.16.68.112 Check component uninstall remnants

172.16.68.112 Check database data files

172.16.68.112 Check disk space

172.16.68.112 Check passed

All inspections passed

172.16.68.112 ssh connection successful

172.16.68.112 /usr/local/nms/ has been created and components are installed.

...

Complete installation

2. Preparation

This chapter introduces the preparations before configuring the device through a PC.

- Configuration Process Overview
- Devices Connection
- Device Login

- Quick Start
- Configuration Examples

2.1. Configuration Process Overview

The overall configuration process of the device (i.e., document structure) is shown in the following table. It is recommended to select corresponding configuration items from the configuration category for management based on the current situation of the device.

Configuration Category / Configuration items	Preparation	Device deployment	Configuring Services and Functions	Management and maintenance
1	Connecting devices	Configuring NMS Communication	Configuring Services	Alarm Management
2	Login device	Configure basic functions	Configuration overhead	Maintenance Management
3	Creating a network element	Configuring Optical Modules and Interfaces	-	-
4	Open the configuration interface	Configuring device capabilities	-	-

2.2. Devices Connection

The host and the device are usually connected directly using a network cable. If the device has been configured with a management IP address, it can also be connected through a DCN (Data Communication Network).

- Direct connection: Either use a network cable to connect the SNMP interface of the device and the network interface of the computer, or use a configuration cable to connect the Console interface of the device and the USB interface of the computer to complete the direct connection, as shown in Figure 1-1 .
  - When connecting through the Console interface, you need to install the driver before you can perform CLI management.
  - When connecting through the SNMP interface, you need to configure the computer IP address and the device SNMP IP address to be in the same network segment, and then you can perform CLI management.
- DCN network connection: The SNMP interface of the device is connected to the DCN network, and the host accesses

the management IP address of the device through the DCN network for configuration management, as shown in Figure 1 - 2. In this case, the DCN network needs to be configured so that the route between the device and the host is reachable and the UDP port (default is 161 and 162) can be accessed normally.

Figure 1-1 Direct connection example

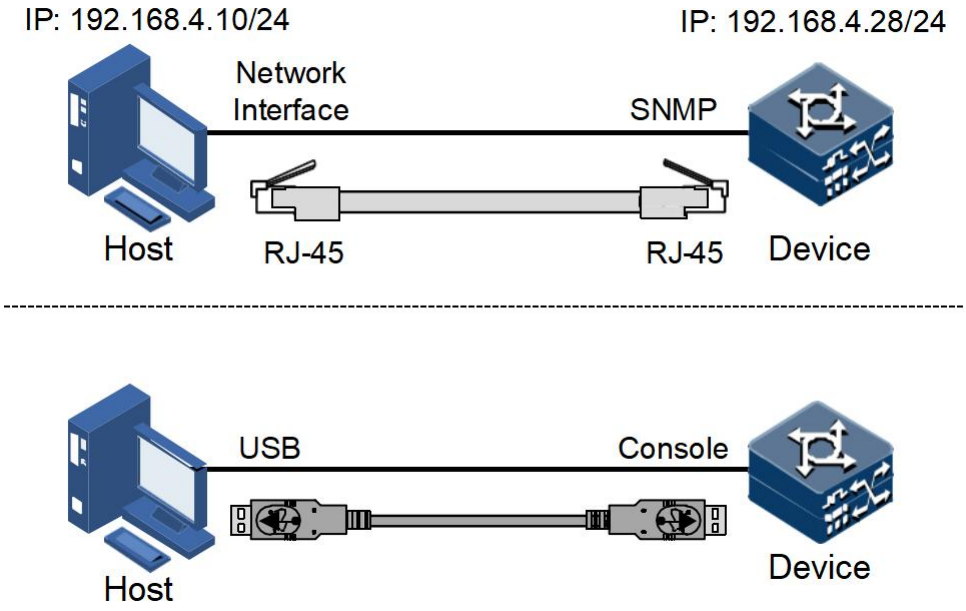
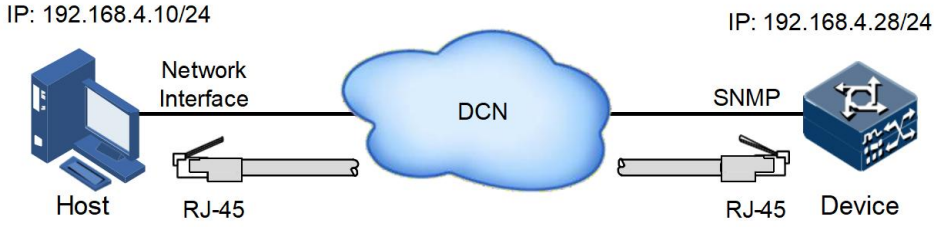


Figure 1-2 DCN network connection example



2.3. Device Login

2.3.1. Logging in Via Console Interface

The console interface is used to connect the device to a PC running a terminal emulation program. Users can use this interface to configure and manage the 18M2C2 device locally without accessing the network. If you cannot log in to the device through Telnet or SSH, you can only log in to the device through the console interface to configure it.

Note

- Device Console Interface type is USB Type A female port, converted to UART (Universal Asynchronous Receiver/Transmitter) inside the device .
- In via USB Before logging into the device , Install USB Port to UART port driver .

Step 1 Use a dual USB male configuration cable to connect the console port of the device to the USB port of the PC.

Step 2 Run a terminal emulation program on the PC, such as the HyperTerminal program included in Microsoft's Windows XP operating system. In the Connection Description dialog box, enter a connection name and click OK.

Step 3 In the "Connect to" dialog box, select "COM N (N is the COM port number converted from the USB port)" when connecting, and click <OK>.

Step 4 In the "COM N Properties" dialog box, set the communication parameters, as shown in Figure 1-3 , and click <OK>.

Figures 1-3 Schematic diagram of communication parameter configuration in "HyperTerminal"

Step 5 Enter the device configuration interface and enter the user name and password for logging into the device. The default values are both fscom .

Note

Microsoft Corporation since Windows Vista The operating system has begun to cancel the support for HyperTerminal, and it needs to be installed through Windows Vista or Windows 7. Users who log in to the device using the operating system should download the relevant program from the Internet.

2.3.2. Configuring Network Management IP Address

Through the Console After logging in to the interface, you usually need to configure the device's network management IP Address for Telnet and network management system .

- Use the SNMP interface IP address as the out-of-band network management IP address.
- Typically, use the Bridge IP address as the in-band network management IP address.

Configure SNMP IP Addresses

Out-of-band network management IP Address using SNMP Interface IP address.

Step	Configuration	Note
1	fscom**# config**	Enter global configuration mode.
2	fscom(config)**# interface smp**	Enter SNMP Interface configuration mode.
3	fscom(config-snmp)**# ip address ip-address [address-mask]**	Configuring SNMP IP address of the interface address.
4	fscom(config-snmp)**# show interface snmp**	View SNMP IP Address information.
5	fscom(config-snmp)**# exit fscom(config)# smp trap-server** ip-address [interface-id]	Configure the IP address of the network management system Address and port number, use the "no" command to delete the configuration. Configure the IP address of the network management system on the managed device The network management system can receive the SNMP of the device only if the address and port number are Trap . By default, the port number is 162 .
6	fscom(config)**# show smp trap- server**	Check the IP address of the network management system address and port number.

Configure the Bridge IP Address

Notice

- Remote 18M2C2 After the physical connection of the series of devices is completed, the Bridge IP address of the remote device can also be configured through the network management system . By default, you only need to configure the Bridge IP address of the central office device and enable the TDP topology discovery function of the central office device to configure the Bridge IP address of the remote device.
- If the remote interface of the central office adopts protection mode, or the connection between multiple devices forms a ring network: first configure the network management channel ring function of the central office device, connect the physical link, and then configure the remote network management IP address; or first connect a physical link of an interface and configure the remote network management IP address, configure the central office network management channel ring function, and then connect the physical link of another interface.
- Usually, the network management channel ring function is enabled on the central office device, and the interface of the central office device in the ring network is added to a channel ring.

The in-band network management IP address usually uses the Bridge IP address. 18M2C2 series devices all support the Bridge function . After configuring the Bridge IP address of the remote device, the local device can manage the remote device through Telnet.

- When the remote physical link connection is normal, the IP address is usually configured only on the local device. The address does not need to be configured at the remote site .
- Bridge between different devices in the network Interface IP The addresses should be in the same network segment; otherwise, the network management channel cannot be established using the Bridge interface .
- Bridge and SNMP The interface addresses cannot be in the same network segment. Users can use Bridge IP To manage the device, you do not need to configure the remote SNMP interface address.
- The IP addresses of the SNMP interfaces of non-gateway network elements must not be in the same subnet as the SNMP interface IP address of the gateway network element. Therefore, it is necessary to first modify the default SNMP IP address of the central office equipment to ensure that it is in a different subnet from the SNMP IP addresses of the

remote equipment.

Note

After configuring BridgeIP , if you need to reduce the management IP address occupied by the remote device , you can enable the NAT function of the central office device through the network management system , add port mapping rules , and then synchronize the central office network element to add the remote network element. The port mapping rule is based on the remote device BridgeIP address and two local ports (23 , 161) , to add two mapping rules to map the remote port to the central office port (it is recommended to use a port greater than F10000).

Please perform the following configuration on the local device.

Step	Configuration	Note
1	fscom# **config**	Enter global configuration mode.
2	fscom(config)# **interface smp**	Enter SNMP interface configuration mode.
3	fscom(config-snmp)#**ip address** *ip-address* [*address-mask*]	Modify the IP address of the SNMP interface of the central office device. It should be in a different network segment from the default SNMP IP address (192.168.4.28/24) of the remote device.
4	fscom(config-snmp)# **exit**	Enter global configuration mode.
5	fscom(config)# **tdp enable**	Enable the automatic topology discovery function. By default, the automatic topology discovery function is disabled.
6	fscom(config)# **show tdp device**	Check the MAC address of the remote device.
7	fscom(config)# **tdp** *mac-address* **bridge ip address** *ip-address* [*address-mask*]	Based on the MAC address of the remote device, configure Bridge IP address. The Bridge IP addresses of the remote devices must be in the same network segment.
8	fscom(config)# **bridge**	Enter Bridge interface configuration mode.
9	fscom(config-bridge)# **show info**	View the Bridge IP address information.

2.3.3. Logging in Via Telnet

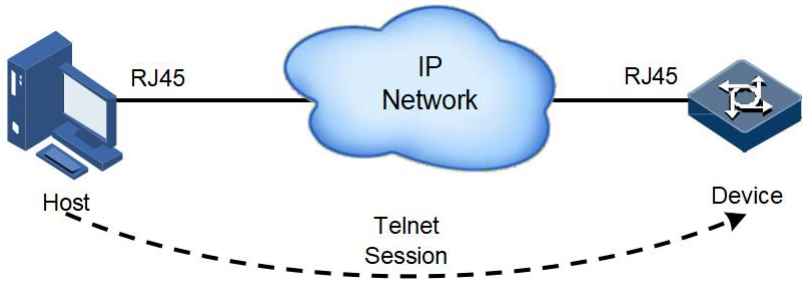
Telnet provides a way to remotely log in to a device through a PC. Users can first log in to a network device through a PC, and then remotely log in to other network devices through Telnet, without having to connect a PC to each network device.

Telnet Server

18M2C2 device acts as a Telnet Server and can provide the following Telnet services:

As shown in Figure 1 - 4 , the route between the computer and the 18M2C2 device is reachable, and the user runs the Telnet client program on the computer to log in to the device and configure and manage the device.

Figures 1 - 4 18M2C2 as Telnet Server Network Diagram



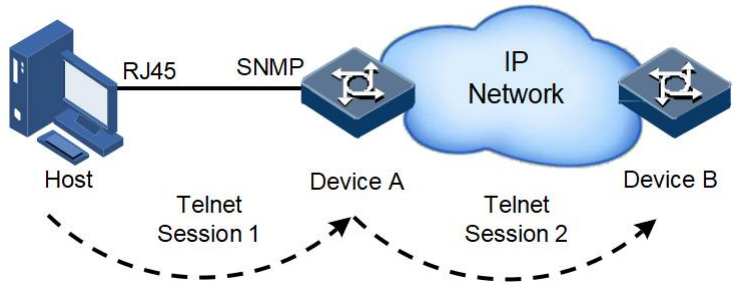
The Telnet server function is enabled by default on the device. Before logging in to the device through Telnet, you can configure the Telnet server function through the console interface and configure the IP address of the management interface such as SNMP (Simple Network Management Protocol).

Step	Configuration	Note
1	fscom**# config**	Enter global configuration mode.
2	fscom(config)**# telnet-service** { enable | disable }	(Optional) Configure the Telnet server function of the device. The default configuration is usually used and needs to be modified only when network planning requires it. By default, the Telnet server function of the device is enabled.

Telnet Client

After establishing a connection to the device through a terminal emulator or Telnet client program on a computer, users can then log in to other devices using telnet commands to configure and manage them. As shown in Figure 1-5, Device A functions both as a Telnet Server and provides Telnet Client services simultaneously.

Figures 1 - 5 18M2C2 as Telnet Client device network diagram



Step	Configuration	Note
1	fscom# **telnet** ip-address [username password] [port-number]	Log in to other devices via Telnet.
2	fscom# **show telnet- serviceinfo**	View Device Telnet Server functionality.

2.3.4. Logging in Via SSHv2

Telnet lacks a secure authentication method, and the transmission process uses TCP (Transmission Control Protocol) for plain text transmission, which poses a great security risk. Simply providing Telnet services is prone to malicious attacks such as DoS (Deny of Service) , host IP address spoofing, and routing spoofing. As people pay more attention to network security, the traditional Telnet and FTP (File Transfer Protocol) methods of transmitting passwords and data in plain text have gradually become unacceptable to users.

SSH is a network security protocol that provides secure remote login and other security services in an insecure network environment by encrypting network data , solving network security issues. It builds a secure channel on top of TCP for data exchange and.

Before logging in to the device through SSH, you need to configure the SSH function.

Step	Configuration	Note
1	fscom# **config**	Enter global configuration mode.

2	fscom(config)# **sshd key-generate** { **dsa** | **rsa** } **modulus** *modulus*	Generate a server host key.
3	fscom(config)# **sshd**	Start the SSH service. By default, the SSH service is not enabled on the device.
4	fscom(config)# **sshd key-destroy** { **dsa** | **rsa** }	(Optional) Destroy the server host key. The secret key needs to be destroyed only when network planning has relevant requirements.
5	fscom(config)# **sshd auth-maxtries** { *counts* | **default** }	(Optional) Configure the maximum number of SSH authentication failures allowed for the device. If the number of client authentication failures exceeds this limit, the device will refuse to continue authentication and disconnect the client. The default configuration is usually used and needs to be modified only when network planning requires it . By default, the device's SSH The maximum number of authentication failures allowed is 3.
6	fscom(config)# **sshd auth-timeout** { *second* | **default** }	(Optional) Configure the SSH address of the device. Authentication timeout. When the client authentication time exceeds this limit, the device will refuse to continue authentication and disconnect. The default configuration is usually used and needs to be modified only when network planning requires it . By default, the SSH authentication timeout for the device is set to 600 seconds.
7	fscom(config)# **sshd restart**	(Optional) Restart the SSH service. Restarting is required only when debugging functions.
8	fscom(config)# **show sshd**	View SSH Service information.
9	fscom(config)# **show sshd connection**	View SSH Connection information.

2.4. Quick Start

2.4.1. Understanding Default Management Parameters

When configuring a device for the first time, you need to use the device's default management parameters to add the device's network element to the network management system, and then select the network element for management. The default parameters of the device are shown in the following table.

Table 1 - 1 Device default parameters

Parameter	Default value	Note
Management IP address	• IP Address : 192.168.4.28 • Mask 255.255.255.0	The network management system uses SNMP protocol and equipment management IP address for communication.
Management Port	161	Device receiving SNMP UDP of the message Port, which is also the destination port for the network management system to send SNMP messages.
Username	fscom	The user name used when logging into the device. The default user level is "root", which is the highest level user.
Password	fscom	The password used when logging into the device.
Read-only community	public	The default read-only community does not require configuration.
Reading and Writing Community	private	The default read-write community does not need to be configured.

Note

- The UDP source port for the network management system to send SNMP management messages is randomly selected, and the default destination port is 161 .
- By default, the UDP port for receiving SNMP management messages is 161 , and the destination port for sending SNMP messages is the source port for receiving messages. The target IP address and port for sending traps are not configured, and there is no management IP address.
- By default, the device SNMP read-only community is public and the read-write community is private.

2.4.2. Creating Network Elements

- When a new device is used as a gateway NE, a single NE needs to be created.
- For devices that are managed independently through interfaces such as SNMP, you need to create a single network element.

Note

Remote devices managed through remote management functions such as zero configuration only need to synchronize the local network elements, without creating individual network elements.

Step 1 Click [Topology/Topology View] in the top navigation.

Step 2 (Optional) Right-click the subnet to which the NE belongs and click Enter.

Step 3 In the topology map, either right-click and click [Add Device], or click <  > in the shortcut toolbar and click [Add Device].

Step 4 In the topology diagram, move the mouse to the location where you want to place the network element and click it. The Add Device interface pops up as shown in the figure below and the parameters are shown in the table below.

Step 5 (Optional) After configuring the IP address, click <Detect Device Type> to verify the device status.

Step 6 After the configuration is complete, click <Save>. After the device is connected, the network management system will automatically perform resource synchronization, and then the user can configure and manage it.

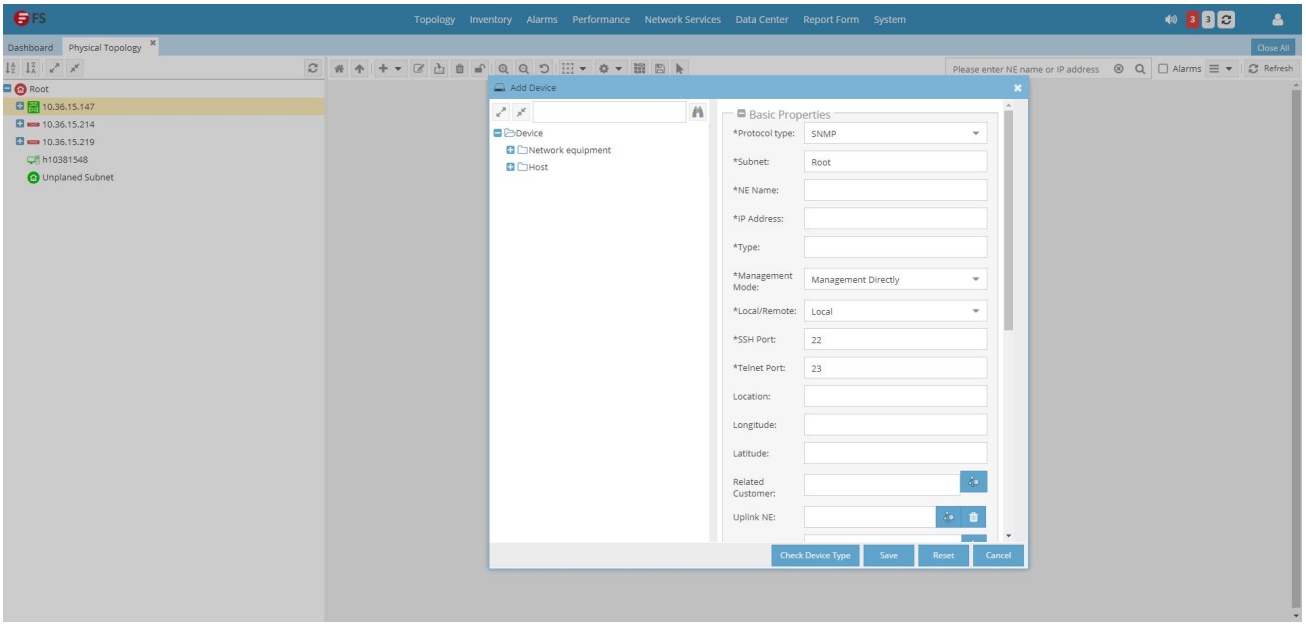


Table 1-2 Configuration parameters

Parameter	Value	Note
Basic Properties		
Protocol Type	SNMP	Configure the NE management protocol type and display the corresponding management parameters according to the protocol type . < Import from Template > at the bottom of the interface to select a protocol template. The default is SNMP .

Subnet	The subnet that initiates the operation of adding a network element	Display the subnet where the NE is located.
Network element name	0 ～ 50 Characters	Configure the NE name. The NE name is a personalized name for the NE by the user and must be unique in the network management system.
IP address	IP address	Configure the IP address of the network element address. Configuring IP After you have entered the address, click < Verify NE Type > . If the verification of the NE type is successful, the device model can be automatically configured . Otherwise, please manually select the device model.
type	Device types supported by the network management system	Configure the device model of the NE. In the device type tree on the left, click to select a device type.
Office / Remote	· Local End · remote	Configure the remote type of the NE.
SSH port	1 ~ 65535	SSH on NEs Communication port. SSH of the network management system This port is used when tools access the device . The default is 22 .
Telnet port	1 ~ 65535	Telnet of NEs Communication port. Telnet of the network management system This port is used when tools access the device . The default is 23 .
Location Information	-	Configure the location information of the network element.
longitude	- 180 ～ 180	Configure the longitude information of the physical location of the NE.
latitude	- 90 ～ 90	Configure the latitude information of the physical location of the NE.
Related clients	-	Configure the client to whom the selected NE is associated.
Online Network	-	Configure the networking element. The network element needs to have been added to the network management system. Click <  > Select the online element and click <  > to clear the parameter .
Uplink Port	-	Configure the device ports on the networking element. Click <  > to select the device port of the networking element .
Manage properties		

port	1 ~ 65535	Configure the management protocol communication port. This port must be the same as the receiving port actually used by the device . The default is 161 .
time out	1 ~ 3600	Configure the communication timeout of the network element in seconds. After the management protocol communication times out, the network management system considers that it cannot connect to the network element. The default is 5 .
Retry times	1 ～ 1000	Configure the number of communication retries of the network element, in times. After the timeout, the network management system retries to connect to the NE. After the number of retries exceeds the limit, the network management system considers that the NE is offline, that is, the NE cannot be managed. The default is 1 .
SNMP Version	V 2 c	Display the protocol version of the NE.
Read community name	0 to 64 Characters	Configuring SNMP Reading community of network element. The read community of the device and the network element must be the same for normal network management. The default is public .
Write community name	0 to 64 Characters	Configuring SNMP The read-write community of network elements. The read-write community of the device and the network element must be the same for normal network management. The default is private .
Offline detection		
Offline status monitoring	Check Unchecked	Configure the offline status monitoring function of device polling. It is checked by default.
Monitoring method	SNMP Ping ICMP Ping	Configure the monitoring protocol. The default is SNMP Ping.
Polling interval	5 min 15 minutes 30 minutes 60 minutes	Configure the device polling interval. The default is 30 minutes.

Notice

- When you delete an NE, the associated links, ports, boards, remote resources, and related alarm data will be deleted .

  The deleted data cannot be restored . Please use it with caution according to the actual situation.

- If the deleted NE is directly managed by the NMS, and other devices are managed through this NE, all NE, chassis, board, and port information of the devices managed through this NE will be deleted.

Step	Function entry	Note
Enter the overview interface	Click the Logo in the upper left corner	Enter the Overview interface.
Keep adding	After the creation is complete, a confirmation dialog box "Continue to add" will pop up.	Click <Yes> to perform the add operation again, and click <No> to close the add dialog box.
Check	· Right-click the node and click [View Properties]. · Click <  > in the shortcut toolbar of the topology map and click [Properties].	View node properties such as software version, hardware version, and MAC address.
Revise	· Right-click the node and click [Edit Properties]. · Click the node and click <  > in the shortcut toolbar .	Modify node name, comments and other properties.
Delete	· Right-click the node and click [Delete]. · Click to select multiple nodes, right-click one of the nodes and click [Delete]. · Click to select one or more nodes and click <  > in the shortcut toolbar .	A confirmation dialog box pops up and the data will be deleted only after confirmation. Topological objects such as network elements and subnets can be deleted only when they no longer need to be managed by the network management system.
Refresh	Click <Refresh> in the shortcut toolbar. · Right-click a blank area on the topology map and click [Refresh].	Refreshes information in the functional area.

2.4.3. Resource Synchronization

After the NE is connected to the NMS, the NMS automatically synchronizes the NE, board, port, alarm, and service data. If the device is changed or the previous synchronization fails, manual synchronization is supported.

Step 1 Click [Topology/Topology View] in the top navigation.

Step 2 In the topology diagram, right-click an NE and click Synchronize NE to manually synchronize resources. A small icon appears above the NE icon, indicating that synchronization is in progress.

Step 3 Wait disappears, synchronization is complete.

Note

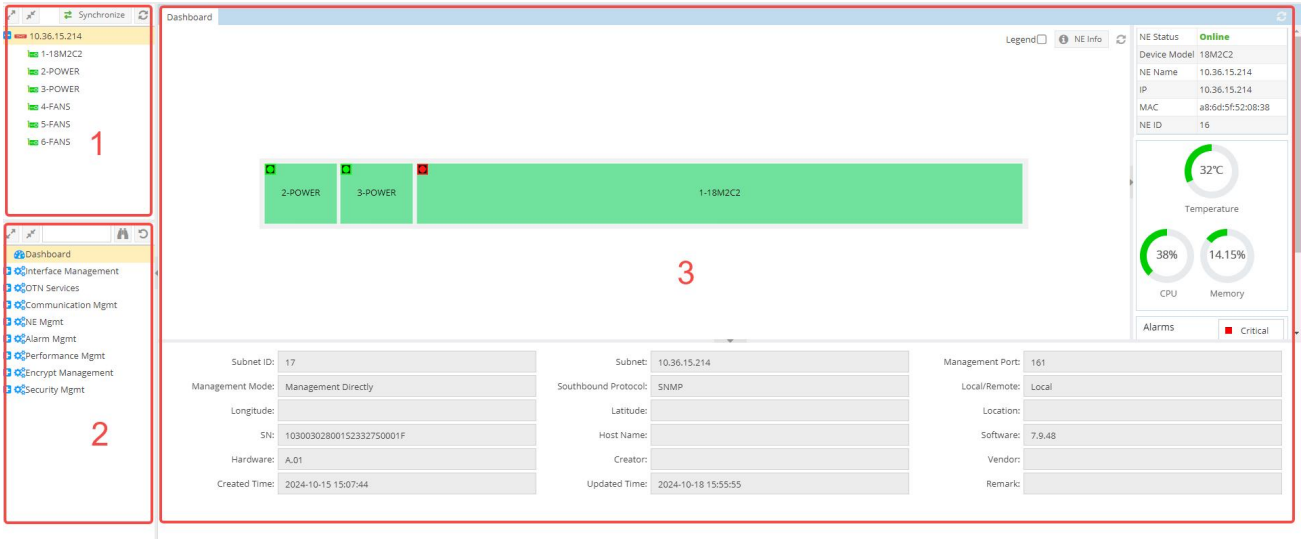
- If multiple network elements are synchronized, the synchronization icon on the waiting node changes to .
- If the synchronization operation fails, the synchronization icon on the node changes to . After checking the network connection and network management parameters, you can perform manual synchronization again.
- For zero-configuration networking applications, the synchronization of local network elements supports automatic creation of remote network elements.
- LLDP is established between network elements Link, synchronization of central office NEs supports automatic link generation. If there is an actual link between NEs , synchronize the central office NEs and remote NEs separately, and support automatic link generation.

2.4.4. Opening Configuration Interface

Step 1 Double-click the network element node in the topology diagram to enter the overview interface, as shown in the following figure.

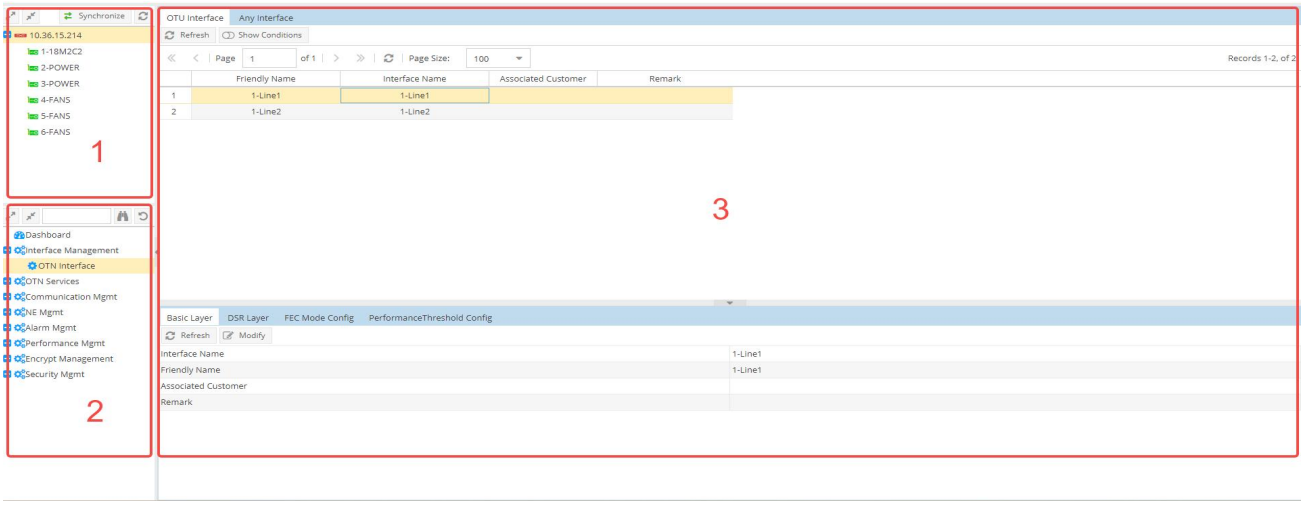
The 18M2C2 overview interface consists of 3 parts:

- Resource list: Display 18M2C2 The chassis' boards, fans, and power supplies.
- Function list: Display 18M2C2 Function list of network element nodes or boards.
- Rack diagram and network element information: Display 18M2C2 in the network management system Chassis and boards inserted in it, temperature, CPU Utilization and other network element information.



1 Resources List 2 Features List 3 Rack diagram and network element information

Step 2 Select the root node or board node in the resource list, and the function list will list the functions corresponding to the resource. Select a function, and the operation interface on the right side of the main view will display the corresponding configuration interface, as shown in the figure below.



1 Resource List 2 Function List 3 Configuration interface

Note

The configuration interface usually has the following characteristics.

- " * " indicates a required parameter.
- If you enter a Value that does not meet the requirements or does not match the current device conditions, a prompt message will pop up when the configuration is delivered , prompting the user that the parameter input is incorrect.

- In the parameter length limit, English and numbers occupy 1 characters, Chinese occupies 2 characters.
- In the NE management interface, usually before configuration, click the <Synchronize> button at the top or bottom of the interface , and then view and configure device parameters.
- Clicking <Synchronize> will allow you to obtain the current device information. Clicking the <Refresh> button will only refresh the interface but will not allow you to obtain the current device information.

2.4.5. Network Element Node Shortcut Menu

Select a device node in the topology map or topology tree and right-click to pop up a shortcut menu. The right-click shortcut menu contains various management function launch points for the device, as shown in Table 1 - 3. shown.

Table 1 - 3 18M2C2 Node shortcut menu

Menu Items	Functional Description
Enter	Enter the topology of this node.
Edit properties	Edit attribute information.
Modify the NE IP	the IP address of the NE on the NMS side address.
Lock coordinates	Lock the topological coordinates of the network element so that the network element node cannot be dragged.
Unlock coordinates	Unlock the topological coordinates of the network element so that the network element node can be dragged.
Move	Move the current network element to another subnet.
Delete	Delete the device node in the network management system.
View Properties	View property information.
Network element synchronization	Perform resource synchronization operations.
Alarm synchronization	Perform alarm synchronization operations.
Performance Management	Configure the performance tasks of the NE, including single-point configuration of the performance tasks of the NE, rebuilding the performance tasks according to the automatic collection template, and starting or stopping performance collection.
Related resources	View a list of related chassis, boards, ports, and more.
Alarm Management	View the current / historical alarms of the device and configure alarm filtering.

Tool	Telnet and SSH of the network management system server Function: Remotely access the device and check the device connectivity through the ICMP PING and SNMP PING functions of the network management system server .

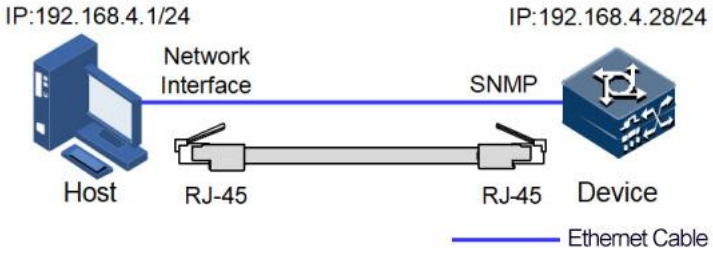
2.5. Configuration Examples

2.5.1. Initial Device Connection Example

Network Requirements

Using SNMP Interface first time to 18M2C2 The device is configured, and the network is shown in Figure 1 - 6 shown.

Figure 1 - 6 Network connections



The configuration requirements and prerequisites are described below.

- The default management IP address of the device is 192.168.4.28 and the mask is 255.255.255.255.0 .
- The host IP address is 192.168.4.1 and the mask is 255.255.255.0 .
- The device is a master device, that is, it no longer cascades to manage lower-level devices, so there is no need to modify the SNMP interface address.
- The device is already mounted in the chassis and has not yet been powered on.

Configuration steps

Step 1 Configure the host 's IP address to 192.168.4.1 and the mask to 255.255.255.0 .

Step 2 Turn on the device power switch and wait until the SYS indicator light flashes, which means the device has started normally.

Step 3 Use a network cable to connect the device SNMP port and the host network card port.

Step 4 192.168.4.28 in the host Telnet software and press Enter to display " Login : ".

Step 5 Enter the default user name fscom Click Enter and enter the default password fscom Click Enter.

Step 6 Enter the enable command and click Enter, enter the default password fscom Click Enter to enter the privileged configuration mode.

Step 7 Enter the show version command and press Enter to view the device name and version information.

Step 8 Enter the show interface snmp command and press Enter to view the IP address information of the device SNMP interface.

Step 9 IP address of the device 's SNMP interface, please refer to the following command. Here we assume that the modified IP address is 192.168.1.10 and the mask is 255.255.255.0 .

fscom #config

fscom (config)# interface snmp

fscom (config-snmp)# ip address 192 . 168 . 1 . 10 255 . 255 . 255 . 0

Check the results

The host shows that the network connection is successful.

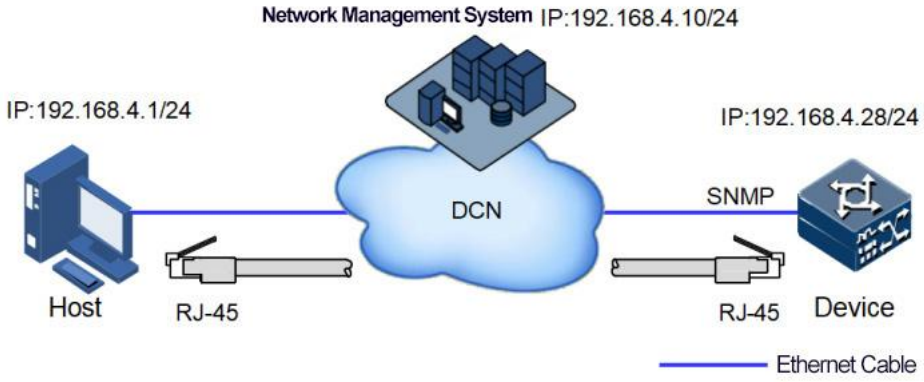
Telnet During access, SNMP LNK/ACT of the port The indicator light should be on or flashing.

2.5.2. Entering Configuration Interface Example

Network Requirements

Enter the device configuration interface through the network management system. The network is shown in Figure 1 - 7 shown.

Figures 1 - 7 Network connection



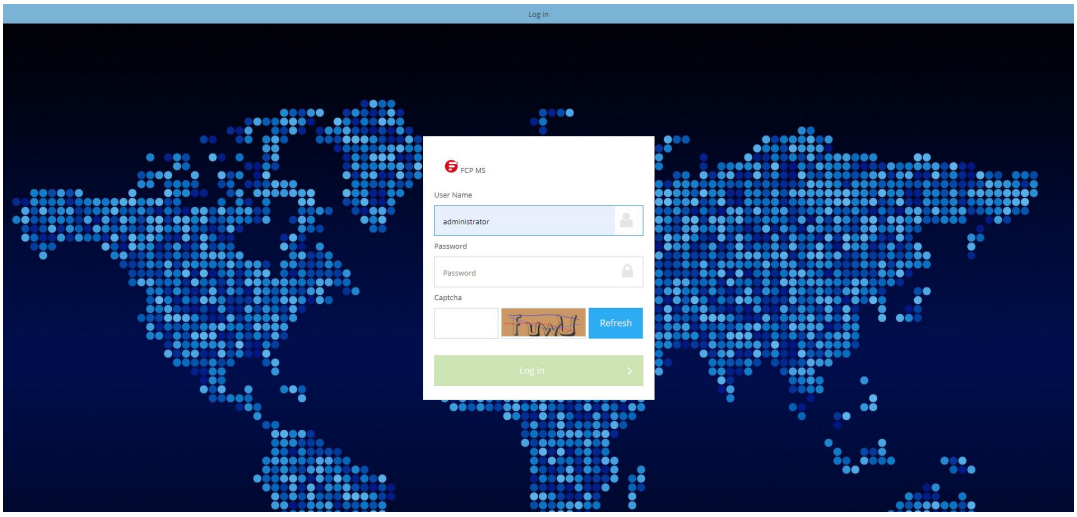
The configuration prerequisites are as follows.

- The host IP address is 192.168.4.1 and the mask is 255.255.255.0 .
- The IP address of the network management system is 192.168.4.10 and the mask is 255.255.255.0 .
- The device SNMP interface IP address is 192.168.4.28 and the mask is 255.255.255.0 .
- The network management system program has been installed and deployed, and network communication is normal.
- Use the default management user name and password to manage the device through the network management system. The default management user name is administrator and the password is admin@fs.com .

Configuration steps

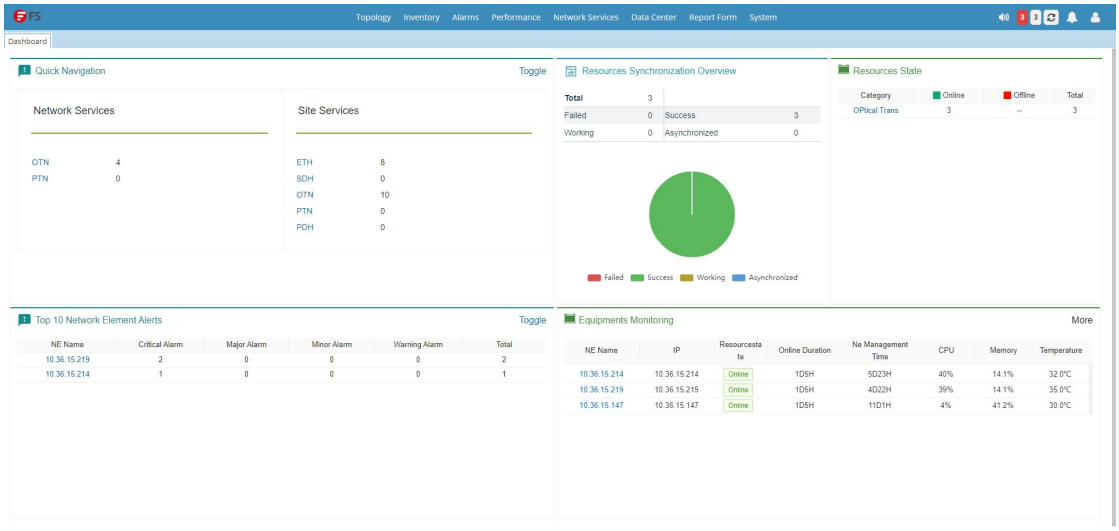
Step 1 Launch a browser on the host operating system and enter the network management system's IP address: http://192.168.4.10.

Step 2 Wait until the login interface appears, then enter your username and password as shown in the figure below.

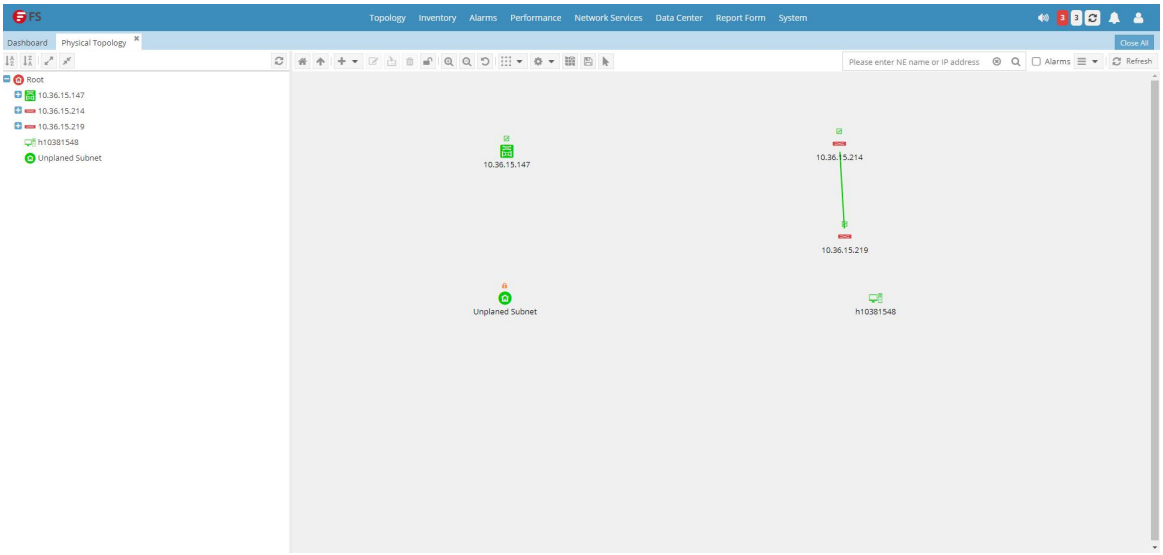


Step 3 Click <Login> or press Enter to enter the overview interface as shown below. If the host time is different from the

network management system time, a dialog box will pop up to prompt the time difference. Usually, you should modify the host time and then log in to the network management system. You can also enter the network management system without modifying the host time and click <Yes>. If you do not modify the host time, the time of logs, alarms, etc. will be different from the host time.



Step 4 In the top navigation, click [Topology/Topology View] to enter the topology interface as shown in the following figure.



Step 5 In the topology map, either right-click and click [Add Device], or click < > in the shortcut toolbar and click [Add Device].

Step 6 In the topology diagram, move the mouse to the location where you want to place the network element and click it. The Add Device interface pops up as shown in the figure below and the parameters are shown in the table below.

Step 7 (Optional) After configuring the IP address, click <Detect Device Type> to verify the device status.

Step 8 After the configuration is complete, click <Save> and the network management system will automatically perform resource synchronization.

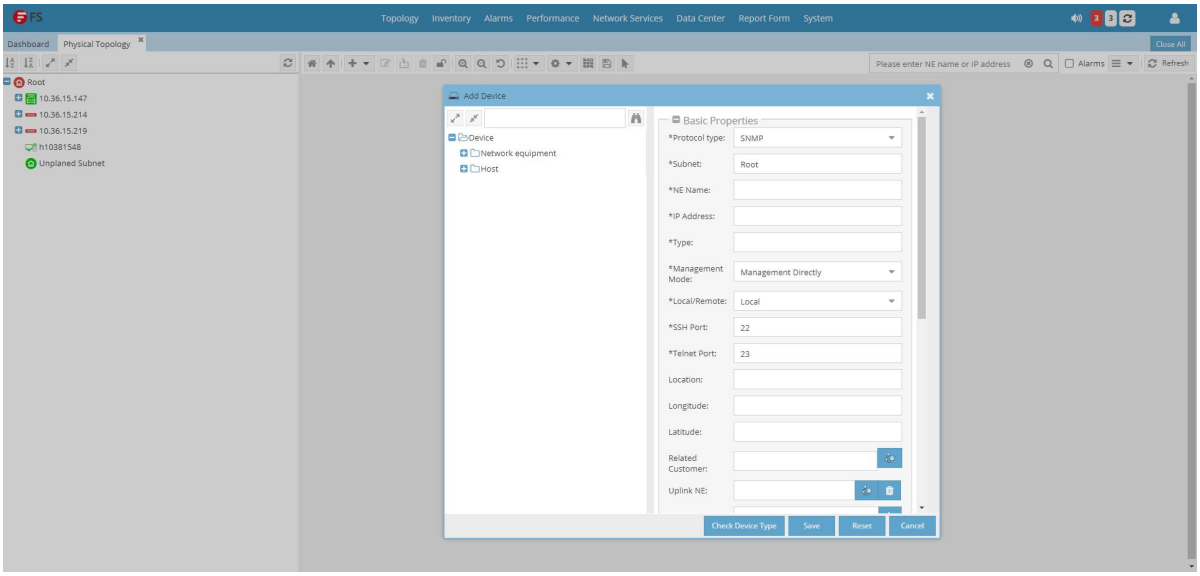
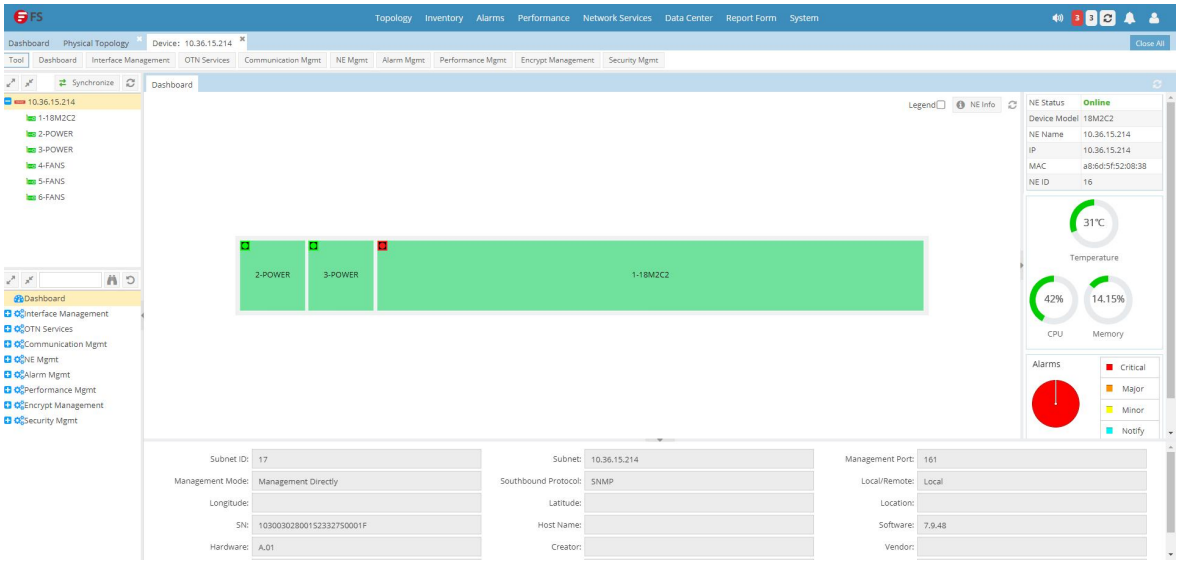


Table 1 - 4 Configuration parameters

Parameter	Value
Protocol Type	SNMP
Subnet	topo
Network element name	NE1
IP address	192.168.4.28
Type	18M2C2
Office/Remote	Central Office
SSH Port	22
Telnet Port	23
Port	161
Time out	5
Retry times	1
SNMP Version	V2c
Read community name	public
Write community name	private
Offline status monitoring	Check

Monitoring method	SNMP Ping
Polling interval	30 mins

Step 9 After synchronization is complete, double-click the network element in the topology diagram to enter the network element subnet, and double-click the network element icon again to enter the overview interface.



Check the results

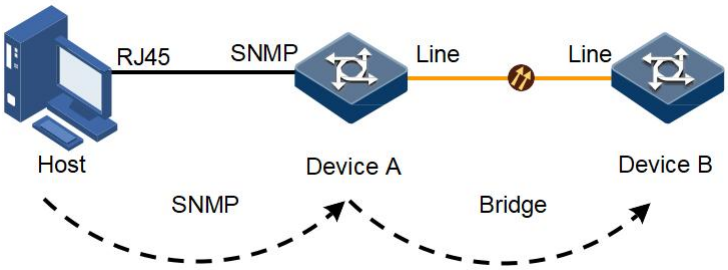
- Check whether the board in the overview interface is consistent with the actually inserted board.
- Click an NE or board in the resource tree, then click Configuration in the function list to check whether the device configuration information is displayed normally.

2.5.3. Configuring Bridge IP Management via CLI Example

Network Requirements

Set the bridge IP addresses of the remote devices Device A and Device B to 192.168.0.1/24 and 192.168.0.2/24 respectively. The network connection is shown in Figure 1-8.

Figures 1 - 8 Network connection



The configuration prerequisites are as follows.

- The host IP address is 192.168.5.1 and the mask is 255.255.255.0.
- The SNMP IP address of Device A has been configured as 192.168.5.28 and the mask is 255.255.255.0.
- Use the CMD program of the operating system to execute the Telnet function.
- Use the default management user name and password to manage the device through the CLI. The default management user name is fscom and the password is fscom .
- Device A at the local end is connected to Device B at the remote end through optical fiber.

Configuration steps

Step 1 In privileged user mode of Device A, enter global mode.

fscom #config

fscom (config)#

Step 2 Enable the automatic topology discovery function on Device A.

fscom (config)# tdp enable

Step 3 Check the MAC address of the remote device. You can identify the remote device based on the SNMP IP address.

fscom (config)# show tdp device

devt[0 x 3003] 00 : 0 E: 5 E: 2 D: 32 :DF //Local device MAC

snmp ip : 192.168.5.28/24 // Local equipment

SNMP IP bridge ip: 127.0.0.1/8 // Bridge IP of the local equipment

admin ip: any

devt[0x311c] 00 : 0E : 5E : 4F : CD:D9 // Remote device

MAC snmp ip : 192.168.4.28/24 // Remote device SNMP IP

bridge ip : 127.0.0.1/8 // remote device

Bridge IP admin ip: any

Step 4 Based on the MAC addresses of the remote devices in the office, configure the Bridge IP addresses respectively.

fscom (config)# tdp 00 : 0 E: 5 E: 2 D: 32 :DF bridge ip address 192 . 168 . 0 . 1 255 . 255 . 255 . 0

fscom (config)# tdp 00 : 0 E: 5 E: 4 F:CD:D 9 bridge ip address 192 . 168 . 0 . 2 255 . 255 . 255 . 0

Step 5 Use Telnet from Device A to access Device B.

fscom (config)# exit

fscom # telnet 192 . 168 . 0 . 2

Trying 192 . 168 . 0 . 2 ...

Connected to 192 . 168 . 0 . 2 . Exit character is '^]'.

Login:

Check the results

- After adding the route from the computer to Device B on the computer, you can use Telnet to access the Bridge IP address of Device B on the computer. An example of adding a route command is "route add 192.168.0.0 mask 255.255.255.0 192.168.5.28".
- After the network management system is installed on the computer, you can add Device A to the network management system. Right-click Device A and select [Synchronize] to add Device B.

3. Device Deployment

This chapter introduces the basic configuration of the device during deployment, such as network management, time, and network element users.

- Introduction
- Configure NMS Communication
- Configure Basic Functions
- Configure Optical Modules
- Configure Interface

- Configure Device Functions
- Configuration Examples

3.1. Overview

During the equipment deployment phase, basic configurations such as network management channels, time, fans, power supplies, and user security are required for the equipment .

3.1.1. Network Management Channel

The device supports network management functions and communicates through the SNMP interface or the ECC network management channel.

Network management channel type

- Out-of-band DCN Network management channel: SNMP Interface provides out-of-band DCN Network management channel, providing out-of-band network management based on SNMP /UDP protocol. The interface is located on the front panel and uses RJ- 45 interface.
  - Does not occupy service bandwidth.
  - When the service channel or physical line is interrupted, the network management channel will not be affected.
  - Depends on a separate DCN network.
  - SNMP management IP address of the out-of-band DCN network management channel is an important parameter for out-of-band DCN network management of devices . When the network management system manages a device out-of-band, you first need to add the device as a network element to the network management system. At this time, you need to use the SNMP management IP address of the network element , that is, the IP address used by the out-of-band DCN .
- ECC (Embedded Control Channel): A channel that carries GCC (general Communication Channel) information. It is a GCC electrical layer network management channel based on the OTN G.709 specification and processed by the device and provided by the OTN (Optical Transport Network) function.
  - Provided by OTN overhead bytes, independent of client service signals.

  - The GCC0 channel is provided by the OTUk overhead and is located in columns 11 and 12 of the first row of the OTUk frame structure, consisting of 2 bytes. GCC0 is used for communication between the two endpoints terminating the OTUk. GCC0 is terminated at electrical relay nodes, thus it cannot be managed end-to-end across electrical relay points.

- The GCC1 and GCC2 channels are provided by the ODUk overhead and are located in the bytes at columns 1, 2, and 3, 4 of the fourth row of the ODUk frame structure, respectively, consisting of 2 bytes each. GCC1 and GCC2 are used for communication between any two end-to-end network elements (provided that the network elements support processing the ODUk frame structure).
- VLAN-based network management channel: carried by the management VLAN that transmits in-band network management information. The port that processes network management information needs to be configured with the management VLAN to complete the reception and transmission of management messages.
- EXT interface-based hierarchical network pipe channel: The EXT interface provides hierarchical network pipe channel. The EXT interface is located on the front panel and uses an RJ- 45 interface.
  - Based on the NAT (Network Address Translation) and NAPT (Network Address Port Translation) functions, one management IP address is enough to manage network-managed devices.

Network management channel configuration function

- The out-of-band DCN network management channel supports the following functions.
  - SNMP management IP address.
  - SNMP management IP address mask.
- The ECC network management channel supports the following functions.
  - Supports enable/disable.
  - ECC channel supports selection of GCC0 , GCC1 , and GCC2 .
  - Supports configuration of channel management IP address and viewing of peer management IP address.
  - Supports borrowing SNMP management IP address.

- Supports PPP and the network layer protocol status and statistics of the network layer protocol it carries. PPP (Point to Point Protocol) is used to establish connections between devices. During the PPP process, LCP (Link Control Protocol) is used to establish logical link connections, and NCP (Network Control Protocol) is used to process network management information of the network layer on the established link.

- The VLAN-based network management channel supports the following functions.
  - Supports configuration of the client-side interface management VLAN that processes network management information.
  - Supports configuration of the OTN_IP interface IP address, subnet mask and VLAN list used by the management channel. Through the IP address of the OTN_IP interface, the device can communicate with the network management system and the device can communicate with the remote device.
- The EXT interface-based multi-level networking channel supports the following functions.
  - Supports enable/disable.
  - Supports configuration of channel management IP address and mask.
  - Supports configuration of external interfaces and internal interfaces.
  - Support NAT configuration Conversion rules.

3.1.2. Automatic Topology Discovery

The device supports automatic topology discovery, which can facilitate the deployment of network management functions between devices .

Function Introduction

The device supports the bridging function for network management information. Messages carrying network management information can be forwarded through the bridging module of the device as they pass through equipment on the network management network, thereby achieving the purpose of network management.The bridge function enables ECC/GCC The managed devices form a local area network.

- MAC of the message Address learning, destination MAC Address forwarding and filtering functions.
- The bridge function also supports setting MAC Learning security mode: In security mode, only the MAC

addresses of FS company devices are learned and forwarded , which improves the security of message forwarding.

- Bridge function supports ECC After the network management channel interface is added to the bridge, it can support the related functions of automatic topology discovery.

Based on neighbor discovery and topology discovery, the bridging function can support chain and ring network management, and realize one-stop configuration of network management. Usually, only the corresponding configuration of the gateway network element is required to manage other devices in the ring network, which greatly simplifies the user's operation steps.

A ring network management network uses a continuous network management channel ring to connect the devices that need network management in the network. Since the devices on the ring network can perform end-to-end transmission through two links, when a link on the ring network fails, the network management information can reach the destination host through other links.

Via FCP MS When performing network management, the discovered network element devices can be automatically added to the network management system topology, so that network management functions can be performed.

 **Note**

The network elements that the network management system can directly access through the network are gateway network elements, and the network elements that communicate with the network management system through gateway network elements are non-gateway network elements.

Configuration Process

 **Notice**

By default, the bridging function and neighbor discovery function are enabled on the device, but the topology discovery function is disabled.

- In the case of chain networking, only the physical connection is normal, ECC/GCC If the function is configured

correctly and the gateway network element enables the topology discovery function, the device can be discovered.

- Only in the case of a ring network, such as 2 Devices through 2 To connect multiple line-side ports and form a physical ring network with multiple devices , you need to configure the channel ring function, and you need to configure the channel ring function before networking .

generally, the configuration process of automatic topology discovery is as follows.

Step 1 Complete the physical connection of network devices to ensure ECC/GCC The channel is normal, so the network management information between devices can communicate normally .

Step 2 IP address of the gateway network element address.

Step 3 SNMP for non-gateway NEs. The IP address of the interface, Bridge interface , and management IP address type.

Step 4 If the link of the network management message forms a physical ring, you need to configure the network management channel ring related functions.

3.1.3. Management Communication Parameters

Regardless of the network management channel used, the network management system and the device communicate using the SNMP protocol, so the device needs to be configured with network management communication parameters.

The network management communication parameters include the network element SNMP management IP address, network management channel IP address, SNMP community, destination address for Trap sending, static routing, etc.

Network management channel IP address

The network management channel is a channel that carries network management information. The endpoints of the channel need IP addresses to communicate with each other.

SNMP Community

SNMP community is a security management parameter used by SNMP protocol to identify identity and control permissions. When managing devices, the SNMP community of the network element and the device must be consistent in order to manage the device normally.

Destination address of the Trap

The SNMP protocol Trap message is used for the device to actively send alarm/event information to the network management system. This mechanism facilitates rapid fault discovery and reduces the burden on the network management system. When using the network management system, after configuring the destination address for the device Trap to be sent, the device will send Trap messages to the destination address only when a fault occurs or the fault is restored.

Static Routing

In the network management function, static routing is used to provide routing functions for network management information communication. Static routing is suitable for the situation where devices communicate across different network segments.

- Static routing requires configuration of the target IP address and mask, and the gateway IP address (that is, the next hop IP address).
- When using embedded network management channels such as ECC/GCC, the device's gateway IP address is the IP address of the device's embedded network management channel.
- In the case of out-of-band DCN, the gateway IP address of the device is the next-hop IP address of the DCN network.
- When multiple network management channels are used at the same time, corresponding static routes need to be configured for each channel that crosses network segments.

3.1.4. NAT/NAPT Function

In hierarchical network management, after configuring the NAT/NAPT function, only one management IP address is needed to complete the network management of multiple devices.

- Usually, the SNMP interface of the gateway device of the cascade management is connected to the DCN network, and the EXT cascade interface is connected to the EXT interface of the cascade device.
- When the management message of the cascade device is sent to the gateway device, the NAT/NAPT function is used to convert the management IP address and port number of the cascade device into the "SNMP IP address + port number" of the gateway device based on the configured conversion rules.
- The network management system or Telnet client accesses the converted IP address and port number to

manage the cascaded device. On the gateway device, the following message port numbers usually need to be converted.

- The SNMP message port number 161 based on the UDP protocol is used for network management system communication.
- Telnet message port number 23 based on TCP protocol is used for Telnet management communication.

The main configuration process of NAT/NAPT function is as follows.

Step 1 Configure the management IP address of the gateway device's SNMP interface and ETH2 interface (ie, cascade interface), that is, the communication parameters of the gateway device in the network management network.

Step 2 Configure the management IP address of the ETH2 interface of the cascade device, that is, the communication parameters of the management message between the cascade interfaces. The IP address of the ETH2 interface between the gateway device and the cascade device must be in the same network segment, and the IP address of the ETH2 interface and the SNMP interface must be in different network segments.

Step 3 Configure the gateway device to enable the NAT/NAPT function.

Step 4 Configure the external interface of the gateway device to SNMP and the internal interface to ETH2. The converted management messages are forwarded through the specified external interface.

Step 5 Configure the conversion rules of the gateway device, and the management messages of the cascaded devices can be converted in the gateway device.

3.2. Configuring Network Management Communication

Notice

- The IP addresses of the network management channels of the same device cannot be in the same network segment. The IP addresses of the network management channels of the remote devices must be in the same network segment. The IP addresses of the SNMP interfaces of the remote devices cannot be in the same network segment. Otherwise, network management cannot be performed.
- By default, the device enables the automatic topology discovery function, and all ECC/GCC network

management channel interfaces are added to the bridge interface. If the automatic topology discovery function is not used, delete the network management channel interface in the bridge function or disable the bridge function before configuring the network management channel. If the bridge function is disabled, the network management interface in the bridge function will be cleared at the same time; if the bridge function is enabled again after being disabled, there will be no network management interface in the bridge function.

- the central office 18M2C2 and the remote 18M2C2 series device is normal, the central office device supports direct discovery of the remote end. Usually, you only need to configure the management IP address of the remote device and add it to the network management system through the topology automatic discovery function of the central office network element in the CLI or network management system, and then manage the remote end through GCC. For specific operations, please refer to "Configure the topology discovery function" or " 1.5.3 Example of configuring Bridge IP network management through CLI ". In this case, the network management channel does not need any configuration on the remote device site.

3.2.1. Configuring Out-of-Band DCN Management Channel

The out-of-band DCN network management channel is mainly used for the network management system to perform out-of-band network management communication through the DCN network and the SNMP interface of the device.

 Note

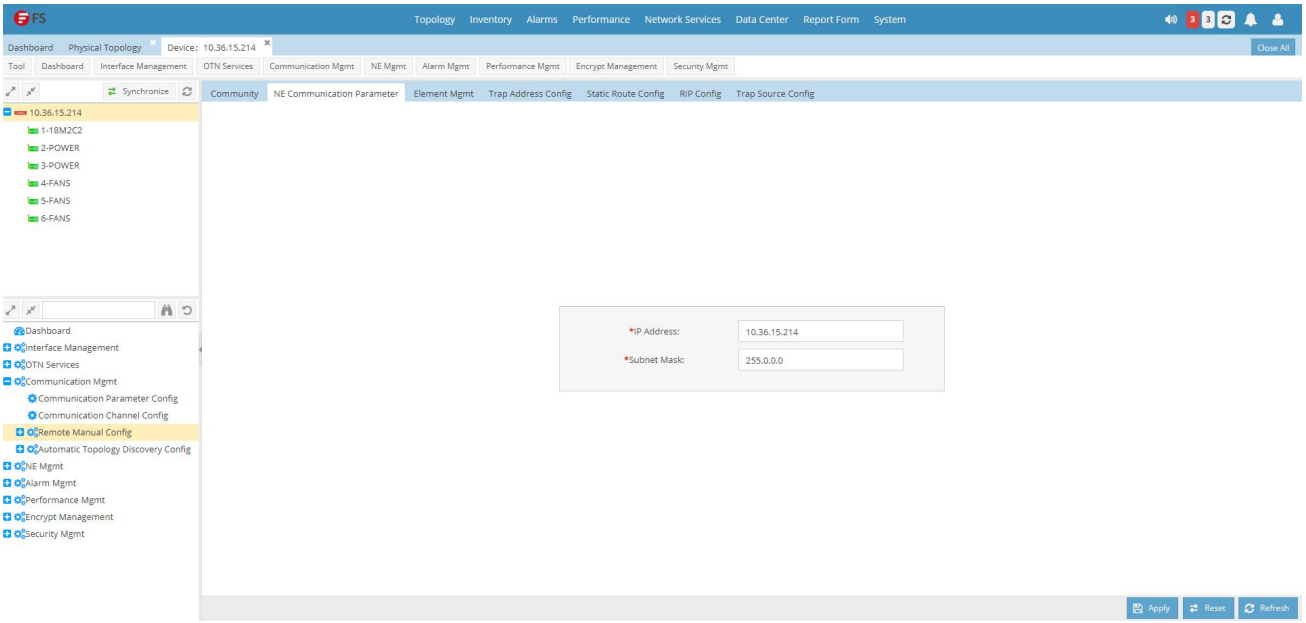
- The SNMP interface address and ECC interface IP address in the same device cannot be in the same network segment;
- The SNMP interface IP addresses of different devices connected through the ECC channel cannot be in the same network segment.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Communication Parameter Configuration].

Step 2 In the configuration interface on the right, click the NE Communication Parameters tab and configure in the

configuration panel. The interface is shown in the figure below and the parameters are shown in the table below.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.



Parameter	Value	Note
IP address	Dotted decimal IP address	Configuring NE Management IP address.
Mask	Dotted decimal IP Address Mask	Configuring NE Management IP Address mask.

Step 4 (Optional) If you do not use the out-of-band network management function, you can disable it. In the configuration interface on the right, click the Enable Out-of-Band Network Management tab. The parameters are shown in the following table.

Parameter	Value	Note
Out-of-band network management enabled	• Enable • Prohibit	Configure the out-of-band network management function. • Enable : SNMP The interface is valid. • Disable: SNMP The interface is invalid. The default is enabled.

3.2.2. Configuring ECC Management Channel

- The ECC/GCC network management channel is used for network management communication between OTUk and ODUk endpoints.

- Each client-side interface and each line-side interface supports one ECC interface.
- Each ECC interface supports one GCC channel, and the GCC channel can be configured as GCC0 , GCC1 , or GCC2 .
- The network management information carried by the ECC/GCC network management channel will be processed by the device and then sent to the DCN through the SNMP interface, or continue to be transmitted by the ECC/GCC network management channel.

 Note

- The ECC/GCC in-band network management channel and the Bridge interface-based topology automatic discovery cannot be used at the same time.
- By default, the device enables the automatic topology discovery function based on the Bridge interface, and all ECC interfaces are added to the Bridge interface. If you do not use the automatic topology discovery function and only use the ECC/GCC-based inband network management channel, you need to delete the ECC interface from the Bridge interface first, and then configure the ECC/GCC inband network management channel.
- For details on how to delete an ECC interface from a Bridge interface, see "Configuring the Bridge Function."

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Network Management Channel Management].

Step 2 In the configuration interface on the right, click the "ECC Channel Management" tab, click to select the network management channel record, and configure it at the bottom of the interface.

- Click the Protocol Configuration tab and configure channel parameters as shown in Table 2-1. After completing the configuration, click Apply to send the configuration.
- Click the "Channel Configuration" tab, select the network management channel, and the parameters are shown in Table 2-2. After the configuration is complete, click <Apply> to deliver the configuration.
- Click the Protocol Status tab to view channel status and statistics. The parameters are listed in Table 2 - 3 .

Table 2-1 Protocol Configuration

Parameter	Value	Note
Network management channel number	-	Display the number of the network management channel.
Channel Enable	• Enable • Prohibit	Configure whether the network management channel is valid. After enabling, the network management information will be processed by the device.
Using SNMP Interface IP address	• yes • no	Configuring ECC The network management channel uses the network element SNMP Manage IP address function. ECC interface using SNMP The address is used as the IP address of the channel. The specific management information is distinguished and processed by the internal functions of the device, which can reduce the IP address occupied by the device. address and facilitates configuration .
Peer IP address	Dotted decimal IP address	Display the IP address of the peer end of the network management channel The peer IP address segment must be the same as the local IP address The address segment is the same . IP address of the other end is automatically displayed .
IP address	Dotted decimal IP address	The IP address of the local end of the network management channel address.
PPP interval (Second)	1 ～ 300	Configure the interval duration for PPP reconnection in seconds.
PPP Retry times	1 to 5	Configure the number of retries when PPP connection fails.
PPP Automatic Reconnection	• Enable • Prohibit	Configure the automatic reconnection feature after PPP interruption. Once enabled, it will automatically attempt to re-establish the connection when the PPP link is interrupted.
Connection Status	• Normal • Break	Configure PPP Connection status.

Note

If the "Peer IP Address" is not displayed, or the "Channel Status" is displayed as "Disconnected", please check the following situations.

- If the network management system or device indicator shows a LOS alarm, please check whether the line-side interface connection is correct and whether the optical fiber line is normal.
- If there is no LOS alarm, but the "Peer IP Address" is not displayed, please check whether the IP address

segments of the two devices are the same.

Table 2 - 2 -channel configuration

Parameter	Value	Note
Delivery Channel	• GCC0 • GCC1 • GCC2 • Prohibit	Configure the overhead used by the channel. The ECC channel is GCC0 by default.

Note

The ECC "pass-through channel" can also be configured in the following ways, which are functionally identical.

In the resource tree on the main interface, click to select the OTN board. In the function list, click [Configuration/OTN Overhead Management]. In the configuration interface on the right, click the "GCC Overhead" tab, right-click the port record, click [Modify], and configure the "Network Management Information Transmission Channel" in the configuration panel. After the configuration is complete, click <Save> to send the configuration.

Table 2-3 Protocol Status

Parameter	Value	Note
LCP state	See Table 2 - 4	Display the protocol status of the logical link of the PPP protocol. In the network management process, it is usually OPENED state.
NCP state	See Table 2 - 4	Display the status of the network layer protocol carried by the PPP logical link. During network management, it is typically in the OPENED state.
Number of received packets	-	Display the number of received NMS messages.
Number of packets sent	-	Display the number of sent NMS messages.
Number of received	-	Display the number of received network management

error packets		message error packets.
Number of sent error packets	-	Display the number of error packets sent by the network management message.
Receive Bytes	-	Display the number of bytes of received NMS messages.
Send Bytes	-	Display the number of bytes of the sent NMS messages.

Table 2-4 LCP and NCP status description

Parameter	Note
INITIAL	In the initial state, the protocol starts to work.
STARTING	Startup state, INITIAL Status of work completed.
CLOSED	In the closed state, the link is available, but no information is transmitted through the link.
STOPPED	Stop state, CLOSED Status of work completed.
CLOSING	End state, the connection attempt is closed.
STOPPING	Stop state, CLOSING Status of work completed.
REQUEST	Request status, normal attempt to configure the parameters of the connection.
ACKRCVD	ACK receiving status, REQUEST has been received Status: Request sent, ACK received Responded, but ACK has not been sent yet Response, ready to enter OPEN state .
ACKSENT	ACK Sending status, REQUEST has been sent Status: Request sent, has been sent ACK Response, but ACK has not been received yet Response, ready to enter OPEN state.
OPENED	In the open state, the connection endpoints have sent and received ACK Response: The connection parameters have been coordinated / configured and the connection has been established, i.e. the connection is in the UP state.

Note

The states and processes of the PPP protocol follow RFC 1661 .

3.2.3. Configuring VLAN-Based Management Channel

- VLAN-based network management channels are suitable for carrying network management information through packet Ethernet services.
- The network management system or remote device communicates with the 18M2C2 client-side interface to form an in-band network management channel.
- The OTN_IP interface is used as the in-band network management interface of the 18M2C2 , and the route can reach the network management system or remote device. The VLAN associated with the IP address of the OTN_IP interface is used as the management VLAN.
- The management VLAN usually needs to meet the following requirements.
  - The interfaces of other devices in the network management channel link allow the management VLAN to pass through, and the management VLAN Tag is not stripped during the forwarding process.
  - 18M2C2 need to be configured with management VLAN for sending and receiving VLAN-based in-band network management information.
  - OTN_IP interface VLAN list of M2C2 must include the management VLAN.
  - 18M2C2 must be configured as Mapper, and the client-side interface must be a 10GE service interface.

Configure the Management IP Interface

Configure the OTN_IP management interface IP address, subnet mask, and VLAN list used by the management channel.

Step 1 In the resource tree on the main interface, click to select the network element root node, and in the function list, click [Communication Management/Remote Manual Configuration/IP Interface Configuration].

Step 2 Click the Management IP Interface Configuration tab, and the list of device management IP interfaces will be displayed.

Step 3 Click to select the IP interface record and click <Modify>. The parameters are shown in the following table.

Step 4 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value	Note
Interface IP address	Dotted decimal IP address	Configuring IP Interface address.

Interface IP Mask	Dotted decimal IP Address Mask	Configuring IP Interface address mask.
Interface VLAN List	1 ~ 4094	Configuring IP VLAN of the interface List.

Configure Management VLAN

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Interface Management/OTN Interface].

Step 2 The interface record is displayed in the configuration interface on the right. Click to select the interface with the service type of 10GE. Click the "Maintenance Configuration" tab at the bottom of the interface and click <Modify>. The parameters are shown in the following table.

Step 3 After the configuration is complete, click <Apply> to deliver the configuration.

Parameter	Value	Note
VLAN Configuration	0 ~ 4094	Configure the management VLAN of the interface . The default value is 0 , indicating no configuration.

3.2.4. Configuring Automatic Topology Discovery

The device supports the automatic topology discovery function. When using ECC/GCC for network management, the network management function between devices can be easily deployed.

The equipment's bridging, neighbor discovery, topology discovery, and network management channel ring functions work together to complete the automatic topology discovery function.

Configure the bridging function

The bridging function supports the ECC of the device. By default, all ECC interfaces are added to the bridge.

Notice

- The bridge IP addresses of different devices in the network should be in the same network segment, otherwise the network management channel cannot be established using the bridge function. The network management system

supports bridge IP addresses based on gateway network elements and automatically allocates IP addresses in the same network segment to the remote end.

- The bridge IP address and the SNMP interface IP address cannot be in the same network segment, but the device can be managed directly through the bridge IP address.
- In a ring network, the SNMP interface IP addresses of non-gateway NEs cannot be in the same network segment as the SNMP interface IP address of the gateway NE.
- The bridging function is the basis of neighbor discovery, topology discovery, and network management channel ring functions. Before configuring these functions, the relevant ECC interfaces must have been added to the bridge.

Step 1 Configure global parameters.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto-Topology Discovery Configuration/Bridge Information Configuration].
2. Click the Bridge Global Configuration tab. The parameters are shown in the following table.
3. After the configuration is complete, click <Apply> to deliver the configuration.

Parameter	Value	Note
Bridge function enabled	• Start • Stop	Configure the bridge function. The default is enabled.
MAC Learning Mode	• Normal • Safe	Configure the MAC for the bridge function Learning mode. • Normal: Learn all MACs address. • Security: Only learn the MAC addresses of FS company devices . The default is Normal.
MAC aging time (seconds)	0 ~ 3600 , measured in seconds	Configure the aging time. 0 Indicates no aging. The default value is 300
Maximum number of MAC addresses learned	0 ~ 1024	Configuring MAC Learning number limit. 0 Indicates no limit on the number of learning. The default value is 1024 .
Bridge IP address	Dotted decimal IP address	Configure the IP address of the bridge function address. Gateway network element IP of the bridging function The address must be configured via this parameter .

Bridge subnet mask	Dotted decimal IP address mask	Configure the IP address of the bridge function Address mask.

Note

- The gateway network element IP address must be configured in the [Communication Management/Topology Auto-Discovery Configuration/Bridge Information Configuration] menu and the "Bridge Global Configuration" tab interface.
- If you configure the gateway NE IP address in the "Discovered NE Configuration" tab page in the [Communication Management/Topology Auto Discovery Configuration/Topology Discovery Configuration] menu, the IP address will be restored to the default 127.0.0.1 after the gateway NE device is restarted, causing the sites under the gateway NE to be out of management .

Step 2 Configure the bridge port. The ECC/GCC ports with topology auto-discovery function need to be used as bridge ports and in the "forwarding" state before they can support neighbor discovery, topology discovery, and channel ring functions. By default, the ECC ports are configured as bridge ports.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto-Topology Discovery Configuration/Bridge Information Configuration].
2. Click the Bridge Port Configuration tab. On the right side of the configuration interface, click <Add>. The configuration parameters are shown in Table 2 - 5 .
3. After the configuration is complete, click <Add> to deliver the configuration.
4. Click to select the bridge port record, "Port Forwarding Status" should be "Forwarding", and the statistical information of the port is displayed at the bottom of the configuration interface as shown in Table 2 - 6 .
5. (Optional) When configuring ECC-based inband network management, click the ECC interface record and click <Delete> to configure the ECC interface not as a bridge port.

Table 2-5 Configuring bridge ports

Parameter	Value	Note
Network management channel type	ECC	Configure the port type to be added to the bridge.

ECC Service board port	-	Click <▪▪▪> to configure the bridge.ECC port. Applicable to port type " ECC ".

Table 2-6 Statistics

Parameter	Note
Number of Unicast Packets Received	Display the number of received unicast messages.
Number of Multicast Packets Received	Display the number of received multicast messages
Number of Broadcast Packets Received	Display the number of received broadcast messages
Number of Management Packets Received	Display the number of received management messages
Number of Unicast Packets Received and Processed	Display the number of unicast packets received and processed
Number of Multicast Packets Received and Processed	Display the number of multicast packets received and processed
Number of Broadcast Packets Received and Processed	Display the number of broadcast messages received and processed
Number of Management Packets Received and Processed	Display the number of management messages received and processed
Number of Packets Received Greater Than 1K	Display receiving greater than 1024 Number of bytes in the message
Number of Unicast Packets Sent	Display the number of sent unicast messages.
Number of Multicast Packets Sent	Display the number of sent multicast messages.
Number of Broadcast Packets Sent	Display the number of sent broadcast messages
Number of Management Packets Sent	Display the number of management messages sent.
Number of Packets Sent Greater Than 1K	Send more than 1024 Number of bytes in the message

Step 3 (Optional) Configure the port to bind the static MAC address of the device. For the ECC port that joins the bridge, you can bind the static MAC address of other devices in the channel to the port to avoid MAC address aging.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto-Topology Discovery Configuration/Bridge Information Configuration].
2. Click the "Bridge MAC Learning Configuration" tab, click <Add> on the top of the configuration interface on the right, and

the parameters are shown in the following table.

3. After the configuration is complete, click <Add> to deliver the configuration.

Parameter	Value	Note
MAC address	Hexadecimal MAC address	Configuring a Static MAC Address address.
Network management channel type	ECC	Configure the port type to be added to the bridge. The default is ECC .
Network management channel number	-	Click < ▪▪▪ > Configure the ports to be added to the bridge , That is static MAC ECC address port.
MAC Address Type	Static	Display MAC The address type is static.

Configure Neighbor Discovery

The neighbor discovery function mainly obtains device information and connection port information based on the neighbor discovery protocol. If the topology automatic discovery function is required in a network management network, all devices in the network must enable the global neighbor discovery function.

Step 1 Configure global parameters.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto Topology Discovery Configuration/Neighbor Discovery Configuration].
2. Click the Neighbor Discovery Global Configuration tab. The parameters are shown in the following table.
3. After the configuration is complete, click <Apply> to deliver the configuration.

parameter	Value	Note
Device MAC address	-	Display device MAC address. Neighbor discovery is based on the MAC address of each device. Address to work.
Protocol detection period (seconds)	1 ~ 180 ,measured in seconds	Configure the detection period of the neighbor discovery function. The detection period affects the speed of neighbor device discovery. Usually, the default value is sufficient. The default is 3 .
Neighbor discovery function enabled	• Enable • Prohibit	Configure the neighbor discovery function. If the automatic topology discovery function is required in a managed network, all devices in the network must enable the global neighbor discovery function.

		The default is enabled.

Step 2 Configure the port neighbor discovery function of the network management channel.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto Topology Discovery Configuration/Neighbor Discovery Configuration].
2. Click the Neighbor Discovery Port Enable Configuration tab, click the record of the network management channel and click <Modify>. The parameters are shown in the following table.
3. After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value	Note
Network management channel type	ECC	Display the type of the network management channel.
Network management channel number	-	Display the port number of the network management channel.
Service board port	-	Display the service board port where the network management channel is located, that is, the service board port used by the local device for communication in the network management channel .
Protocol Enablement	• Enable • Prohibit	Configure the neighbor discovery function of the service board port. If the automatic topology discovery function is required in a managed network, the neighbor discovery function must be enabled on all service board ports of devices in the managed channel of the network. The default is enabled.

Step 3 View the discovered neighbor information.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto Topology Discovery Configuration/Neighbor Discovery Configuration].
2. Click the Neighbor Discovery Information Query tab to display the discovered neighbor information. The parameters are shown in the following table.

Parameter	Value	Note
Local network management channel type	ECC	Display the network management channel type of the local device.

Local network management channel number	-	Display the network management channel number of the local device.
Local service card port	-	Display the service board port where the network management channel is located, that is, the service board port used by the local device for communication in the network management channel .
Neighbor MAC address	-	Display the MAC addresses of neighbor devices address.
Neighbor network management channel type	ECC	Display the network management channel type of the neighbor device.
Neighbor network management channel number	-	Display the network management channel number of the neighbor device.
Neighbor SNMP IP	-	Display the SNMP of neighbor devices. Out-of-band interface IP address.
Neighbor SNMP Port Mask	-	Display the SNMP of neighbor devices. Out-of-band interface IP Address mask .
Neighbor Bridge IP	-	Display the bridge IP of the neighbor device address.
Neighbor bridge mask	-	Display the bridge IP of the neighbor device Address mask.
Neighbor Management	• SNMP IP • Bridge IP • any	Display the management mode of neighbor devices. Neighbor devices report alarm traps and communicate network management messages based on the configured management mode. • SNMP IP : via SNMP Interface management. • Bridge IP : Managed via bridge. • any : Manage through any interface.

Configure the topology discovery function

The topology discovery function mainly obtains the topology connection information between devices based on the topology discovery protocol. Enable the topology discovery function for the gateway NE of the topology automatic discovery network, and configure the SNMP interface and Bridge interface IP addresses of the discovered non-gateway NEs and the management IP address type through the gateway NE.

Note

The topology discovery function works properly only after the neighbor discovery function is enabled.

Step 1 Configure global parameters.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto Topology Discovery Configuration/Topology Discovery Configuration].

2. Click the Topology Discovery Global Configuration tab. The parameters are shown in the following table.

3. After the configuration is complete, click <Apply> to deliver the configuration.

Parameter	Value	Note
TDP Function Enablement	• Enable • Prohibit	Configure the topology discovery function. If the automatic topology discovery function is required in a managed network, the gateway NEs in the network must enable the topology discovery function, and the non-gateway NEs must disable the function. The default is disabled.
TDP detection cycle (Second)	1~180 ,measured in seconds	Configure the detection period of the topology discovery function. This detection period affects the speed of topology discovery. Usually, the default value is sufficient . The default is 5 .

Step 2 Configure the management IP address of the discovered device, mainly to configure the SNMP and bridge IP addresses of the discovered network elements, and the Trap reporting method.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto Topology Discovery Configuration/Topology Discovery Configuration].
2. Click the Discovered NE Configuration tab, click the NE record and click <Auto Assign IP> to automatically assign a bridge IP address in the same network segment to the remote device based on the bridge IP address of the gateway NE. The automatic IP assignment function is applicable when the remote device Bridge interface has the default IP address (127.0.0.1) .
3. (Optional) Click the discovered NE record and click <Modify>. The parameters are shown in the following table. After the configuration is complete, click <Save> to send the configuration. If the device has been added to the network management system, after modifying the remote device IP address, you need to resynchronize the local NE to add the remote NE.
4. Click the "Not Created" record and click <Create NE> to add the discovered NE device to the network management system.

Parameter	Value	Note
Whether the network element has been created	• Created • Not Created	Indicates whether the remote device discovered by topology has completed the discovery process.
Source device MAC address	-	Display the MAC address of the remote device address.
Device Type	-	Display the device type of the remote device.

SNMP IP Address	-	SNMP for Remote Devices Interface IP address.
SNMP IP Address Mask	-	SNMP for Remote Devices Interface IP Address mask. SNMP Interface IP Address and Bridge IP The addresses must be in different network segments.
Bridge IP Address	-	Configure the remote device's bridge IP address.
Bridge IP Address Mask	-	Configure the bridging IP address mask of the remote device. The local and remote bridging IP addresses must be in the same network segment.
Management IP Address Type	• SNMP IP • Bridge IP • any	Configure the management IP address type of the remote device. The remote device reports alarm traps and performs network management message communication according to the configured management mode. SNMP IP: Management via SNMP interface Bridge IP: Managed via bridge interface any : manage through any interface

Step 3 View the topological connection relationship.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto Topology Discovery Configuration/Topology Discovery Configuration].
2. Click the Physical Connection Relationship tab to display the remote device information discovered by the topology. The parameters are shown in the following table.

Parameter	Value	Note
A-side NE MAC	-	Display the local device MAC address.
A-side Port Type	ECC	Display the network management channel type discovered by the local device topology.
A-side Port Number	-	Display the network management channel number discovered by the local device topology.
A-side service card port	-	Display the network management channel port discovered by the local device topology.
Z-side NE MAC	-	Display the MAC address of the remote device address.
Z-side Port Type	ECC	Display the network management channel type discovered by the remote device topology.
Z-side Port Number	-	Display the NMS channel number discovered by the remote device topology.
Z-side service card port	-	Display the network management channel port discovered by the remote device topology.

Configure the Network Management Channel Ring

The network management channel ring is used for network management ring networking and can provide channel protection based on the characteristics of the ring network.

Notice

- The network management channel physically forms a ring network, such as a ring network of multiple network elements or two interfaces between two network elements. In this ring network, there is one and only one device that enables channel ring detection. Usually, the gateway network element in a ring network enables channel ring detection.
- If the network management channel does not form a physical ring network, there is no need to enable channel ring detection.
- In the case of intersecting and tangent rings, a channel ring needs to be created. In each ring, there is only one network element that enables channel ring detection.
- When the devices in the ring network enable the bridging function, channel self-loop detection must be enabled to avoid looping. There is no such restriction for point-to-point services.
- The channel ring supports the self-loop detection function, which usually needs to be enabled to detect whether a loop has been formed and to view the loop information.

Step 1 Configure global parameters.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Topology Auto Discovery Configuration/Channel Ring Management].
2. Click the Channel Ring Global Configuration tab. The parameters are shown in the following table.
3. After the configuration is complete, click <Apply> to deliver the configuration.

Parameter	Value	Note
Channel ring detection function enabled	• Enable • Prohibit	Configure the channel ring detection function. The default is disabled.
Channel ring detection period (Second)	1 ~180, measured in seconds	Configure the detection period of the channel ring detection function. The detection period will affect the detection speed, and the default value is usually used. The default is 3.

Channel Ring Detection Mode	• Normal • Fast	Configure the channel ring detection mode. The default is normal.
Enable the self-loop detection function	• Enable • Prohibit	Configure the self-loop detection function, which is used to detect whether the network management message channel forms a loop. In a network management ring network, network management messages will not form a loop under normal circumstances. The default is enabled.
Self-loop detection period (seconds)	1 ~ 180, measured in seconds	Configure the detection period of the self-loop detection function. The detection period affects the detection speed. Usually, the default value is sufficient. The default is 2.

Step 2 To configure a channel ring, all network management channels corresponding to the interfaces in the channel ring network need to be added to the channel ring.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Topology Auto Discovery Configuration/Channel Ring Management].
2. Click the "Channel Ring Configuration" tab, click <Add> at the top of the configuration interface, and the parameters are shown in the following table.
3. After the configuration is complete, click <Add> to deliver the configuration.
4. Click the channel ring record at the top of the configuration interface and view the interfaces in the channel ring at the bottom of the configuration interface.

Parameter	Value	Note
Channel Ring Index	1 to 48	Configure the channel ring number.
ECC aisle	-	Click <  > Configure ECC in channel ring aisle .
Channel ring description information	-	Configuration description information, only English and numeric characters are supported

Step 3 View the channel ring port information.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto-Topology Discovery Configuration/Channel Ring Configuration].

2. Click the Channel Ring Port Information tab. The channel ring port information is displayed at the top of the configuration interface. The parameters are shown in Table 2 - 7 .

Table 2 - 7 -channel ring port information

Parameter	Value	Note
Network management channel type	ECC	Display the type of the network management channel in the channel ring.
Network management channel number	-	Display the port number of the network management channel.
Service card port	-	Display the service board port where the network management channel is located, that is, the service board port used by the device for communication in the network management channel.
Loopback status	• Loopback • Not looped back	Display whether the loopback function is enabled on the port of the network management channel.
Forwarding Status	• Forward • Block • Disconnect	Display the port forwarding status of the NMS channel.
Communication fault status	• Normal • Alerts	Display whether there is a communication fault on the port of the network management channel.
Is there a ring network?	• yes • no	Display whether the port of the NM channel belongs to the NM channel ring.
Is there a self-loop?	• yes • no	Display whether a self-loop occurs on the port of the network management channel.

3.2.5. Configuring Management Communication Parameters

Notice

Network management can only be performed normally when the network element and the network management communication parameters of the device match. If network management can be performed normally, please do not configure the network management communication parameters at will. Incorrect configuration of network management communication parameters will cause the device to be unable to perform network management. Please use it with caution according to the actual situation.

Configure SNMP Community

The device uses SNMP community authentication. If community authentication fails, the device cannot be managed through the network.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Communication Parameter Configuration].

Step 2 In the configuration interface on the right, click the Read-Write Community tab and click <Add>. The parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value	Note
Name	Up to 16 Characters	Configure the community name. The community name in the same device cannot be repeated.
Permissions	Read-only Read / Write	Configure community permissions.

Note

SNMP community parameters do not support modification. You can modify them by deleting first and then adding.

The device supports a maximum of 10 communities and provides the following default communities. The default communities cannot be deleted.

- public: Read-only permission.
- private: read and write permissions.

Configure Trap destination address

The device supports configuring up to 8 Trap target addresses. When the device generates an alarm, it will send SNMP Trap information to the Trap target address, and the network management system will parse the generated alarm based on the received Trap information.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Communication Parameter Configuration].

Step 2 In the configuration interface on the right, click the "Trap Target Configuration" tab, click <Add>, and the parameters are shown in the following table.

Step 3 configuration is completed, click <Save> to deliver the configuration.

Parameter	Value	Note
Target Address	Dotted decimal IP address	Configuring Traps Destination IP address. The target address in the same device cannot be repeated.
Port	1 ~ 65535	Configure the target port for Trap transmission. Trap information is sent using the UDP protocol, so it is necessary to configure the port of the network management system to receive Traps. The default is 162 .

Configure Static Routes

When the network management system communicates with the device through routing, you need to add static routes for device management messages.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Communication Parameter Configuration].

Step 2 In the configuration interface on the right, click the Static Route Configuration tab and click <Add>. The parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value	Note
Target IP address	Dotted decimal IP address	Configure the destination IP of the route address.
Target subnet mask	Dotted decimal IP Address Mask	Configure the routing subnet mask.
Gateway IP address	Dotted decimal IP address	Configure the device's gateway IP address.

Configure RIP

The device supports the use of RIP to route data between various network management channels.

Note

Bridging forwarding is only for forwarding at Layer 2 instead of Layer 3, which speeds up the forwarding time. However, the learning of routing information still depends on RIP. Therefore, when using bridging to forward messages, it is also necessary to start

the RIP routing function.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Communication Parameter Configuration].

Step 2 In the configuration interface on the right, click the "RIP Configuration" tab. The parameters are shown in the following table.

Step 3 After the configuration is complete, click <Apply> to deliver the configuration.

Parameter	Value	Note
RIP Enable	Enable Prohibit	Configure the RIP function.
Message update time (seconds)	20 to 500, measured in seconds	Configure the RIP route update timer. At this time interval, the device broadcasts its routing table to the network connected to it and updates the routing information. The default is 30.
Route failure time (seconds)	120 to 180, measured in seconds	Configure the RIP route invalidation timer. If a routing entry is not confirmed after this time, the device considers the routing entry invalid. The default is 180.
Route clearing time (seconds)	120 to 500, measured in seconds	Configure the RIP route deletion timer. If the routing entry is not confirmed after this time, the device deletes the routing entry from the routing table. The default is 120.

Configure Trap Source Address

The device supports configuring the IP source address used when sending traps. The IP address of the device network element in the network management system must be the same as the Trap source address so that the network management system can correctly receive alarms.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Communication Parameter Configuration].

Step 2 In the configuration interface on the right, click the Trap Source Configuration tab. The parameters are shown in the

following table.

Step 3 After the configuration is complete, click <Apply> to deliver the configuration.

Parameter	Value	Note
IP address	Dotted decimal IP address	Configure the IP source address used when sending Traps.

3.2.6. Configuring NAT/NAPT

The NAT/NAPT function is only applicable to management messages of the hierarchical network management, not to business messages.

Configure Global Features

Step 1 In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Remote Manual Configuration/NAT/NAPT Configuration].

Step 2 Click the Global Configuration tab and configure the parameters as shown in the following table.

Step 3 After the configuration is complete, click <Apply> to deliver the configuration.

Parameter	Value	Note
NAPT Function Enablement	• Enable • Prohibit	Configuring NAT/NAPT Global function. Disabled by default.

Configure IP interface type

The IP interface type is mainly used to configure the external and internal IP interfaces of the device.

Step 1 In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Remote Manual Configuration/NAT/NAPT Configuration].

Step 2 Click the "Port Configuration" tab, click <Add>, and configure the parameters as shown in the following table.

Step 3 After the configuration is complete, click <Add> to deliver the configuration.

Parameter	Value	Note

NAPT Interface Name	• SNMP • Bridge • ECC • Eth 2	Configuring the device IP Interface type.
NAPT Interface number	Value and IP Interface type related : • SNMP : 1 • Bridge: 1 • ECC : 1 ~ 768 • Eth 2 : 1	Configuring IP Sequence number of the interface.
NAPT Interface properties	• External • Internal	Configuring IP Interface type. • External: The external IP interface is used to connect to the converted network management network. • Internal: The internal IP interface is used to connect to the network management network before conversion.

Note

The NAPT Interface Name and NAPT Interface Number together specify the IP interface.

- For the external IP interface, the local equipment communicates with the network management system through the IP interface.
- For the internal IP interface, the local equipment performs conversion according to the conversion rules and then communicates with the network management system.

Configure Conversion Rules

Note

When configuring multiple translation rules, the port numbers after translation cannot be the same.

Step 1 In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Remote Manual Configuration/NAT/NAPT Configuration].

Step 2 Click the "Rule Configuration" tab, click <Add>, and configure the parameters as shown in the following table.

Step 3 After the configuration is complete, click <Add> to deliver the configuration.

Step 4 (Optional) Click the Mapping Query tab to view the status information of the currently communicating TCP and UDP protocol sessions.

Parameter	Value	Note
NAPT Rules and protocols	• TCP • UDP	Configure the conversion protocol, that is, the protocol type of the port number .
NAPT Internal global port number	10000 ～ 65535	Configure the port number after conversion.
NAPT Internal local IP address	Dotted decimal IP address	IP before configuration conversion address, which will be converted to "external public IP address + converted port number" for communication.
NAPT Internal local port number	1 ~ 65535	Configure the port number before conversion.

3.3. Configuring Basic Functions

3.3.1. Configuring Device Time

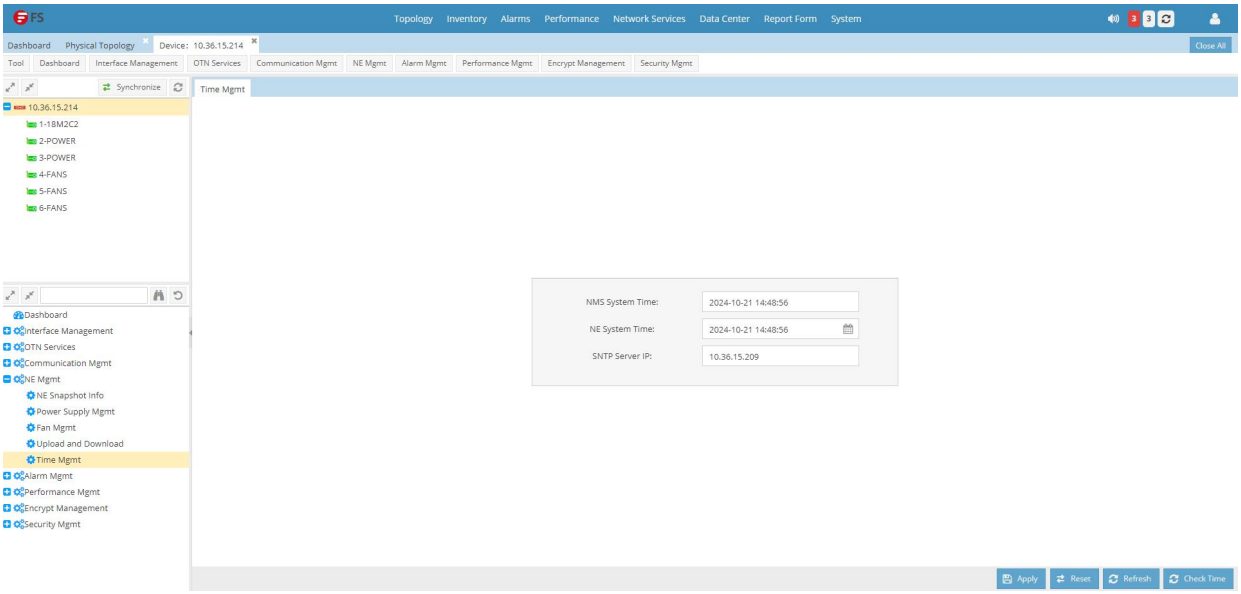
The device time supports time calibration through the network management system, manual time configuration, and obtaining time from the SNTP server.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [NE Management/Time Management], as shown in the following figure.

Step 2 (Optional) Click <Time Adjustment> at the bottom of the interface to send the network management system time to the device for configuration.

Step 3 In the configuration interface on the right, you can manually configure the time or obtain the time through the SNTP server. The parameters are shown in the following table.

Step 4 After the configuration is complete, click <Apply> to deliver the configuration.



Parameter	Value	Note
Network management system time	-	Display the current time of the computer where the network management system is located. The format is "year-month-day hour: minute: second".
NE system time	-	Manually configure the device time. Click this parameter to display the date and time selection box, select the time, and click <OK>. The format is "year-month-day hour:minute:second".
SNTP server address	Dotted decimal IP address	Configure the IP address of the SNTP server. After configuring this parameter, the device obtains time from the SNTP server.

3.3.2. Checking Power Supply

In the resource tree on the main interface, click to select the NE root node. In the function list, click [NE Management/Power Management] to view the power status of all power slots.

Parameter	Value	Note
Power supply slot	-	Display the slot where the power supply is located.
Power supply working status	• Normal • Abnormal	Display the power supply working status.

3.3.3. Configuring Fans

Notice

When you manually configure the fan speed, if the chassis temperature rises and the device generates a temperature alarm, you must increase the speed. Otherwise, services may be interrupted or the device may be damaged.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click NE Management/Fan Management.

Step 2 Click the Global Configuration and Fan List tabs. The parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value	Note
Global Configuration		
Current chassis temperature (℃)	-	Display the temperature of the chassis in degrees Celsius.
Control Mode	• Intelligent • Non-intelligent	Configure the fan control mode. • Intelligent: The fan automatically controls the speed of each blade according to the current situation . • Non-intelligent: The fan operates at a manually configured speed .
Fan speed	• full speed • high speed • Medium speed • Low speed	In non-intelligent control mode, manually configure the fan speed.
Chassis temperature high threshold	-127 ～ 127	Configure the chassis temperature threshold in degrees Celsius. When the temperature exceeds this threshold, the device reports a chassis temperature alarm.
Chassis temperature low threshold	-127 ～ 127	Configure the chassis temperature warning threshold in degrees Celsius. When the temperature is lower than the threshold, the device will report a chassis temperature alarm.
Fan List		
Fan ID	-	Display the fan number.
Fan Control Mode	• Intelligent • Non-intelligent	Configure the fan control mode. • Intelligent: The fan automatically controls the speed of each blade according to the current situation .

		• Non-intelligent: The fan operates according to the manually configured speed.
Fan speed level	• Full speed • High speed • Medium speed • Low speed	In non-intelligent control mode, manually configure the fan speed.
Fan speed	-	Display the fan speed.
Fan slot	-	Display the fan slot number.

3.3.4. Configuring Zero Performance Suppression

Zero performance suppression means that when monitoring performance, if the performance data value is zero, no performance data will be reported. Zero performance suppression can reduce invalid data and reduce the burden on network management operations.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click Performance Management/Zero Performance Suppression.

Step 2 On the right side of the configuration interface, the enable status of zero performance suppression is displayed. The parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value	Note
Zero performance inhibition	• Enable • Prohibit	Configure the zero performance suppression feature.

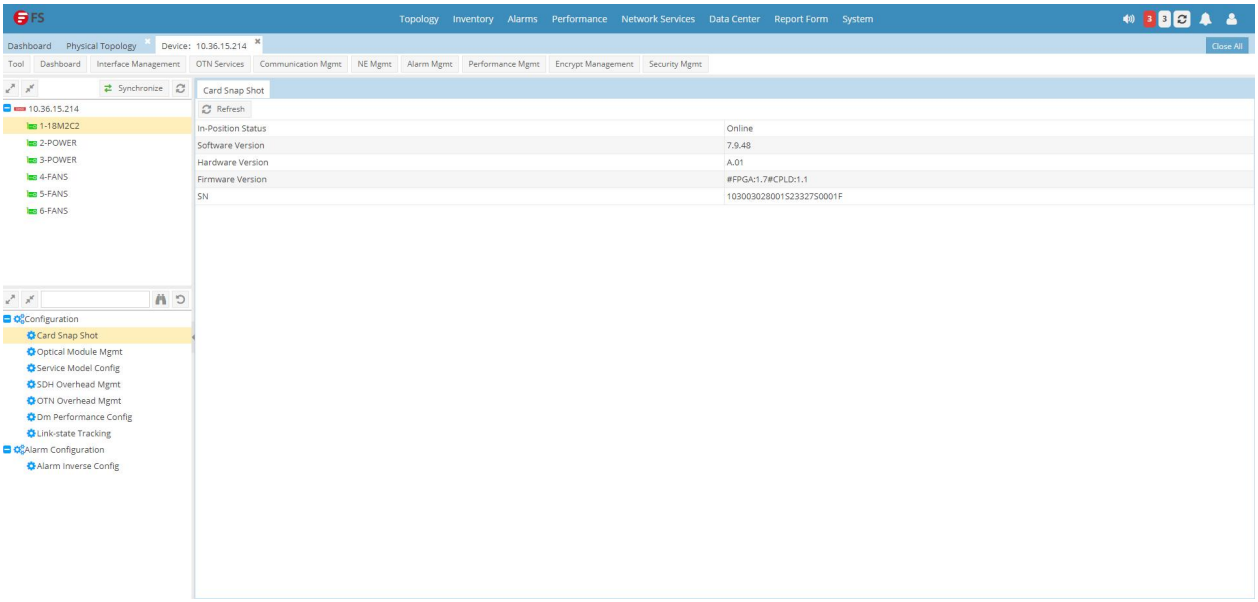
3.3.5. Viewing Board Snapshot

The board snapshot supports displaying information such as software and hardware versions and serial numbers.

Step 1 In the resource tree of the main interface, click to select a board. In the function list, click [Configuration/Board Snapshot], as shown in the following figure. The parameters are shown in the following table.

Step 2 Click <Modify> to configure the board description information.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.



Parameter	Value	Note
In-position status	• In place • Not in place	Indicate whether the board is in place.
Software Version	-	Display the board software version.
Hardware version	-	Display the board hardware version.
Firmware version	-	Display the board firmware version.
Serial Number	Up to 50 Bytes	Configure serial number information.

3.3.6. Viewing Service List

The service list supports displaying the service information of network elements in the network management system, and supports functions such as querying records and configuring service-related parameters.

Step 1 Click [Business Services/Single-Site Business] in the top navigation.

Step 2 Click the "OTN Service" tab to view the service information in the network management system, as shown in Figure 2-1.

Step 3 Click <Show Query Conditions> to query business information.

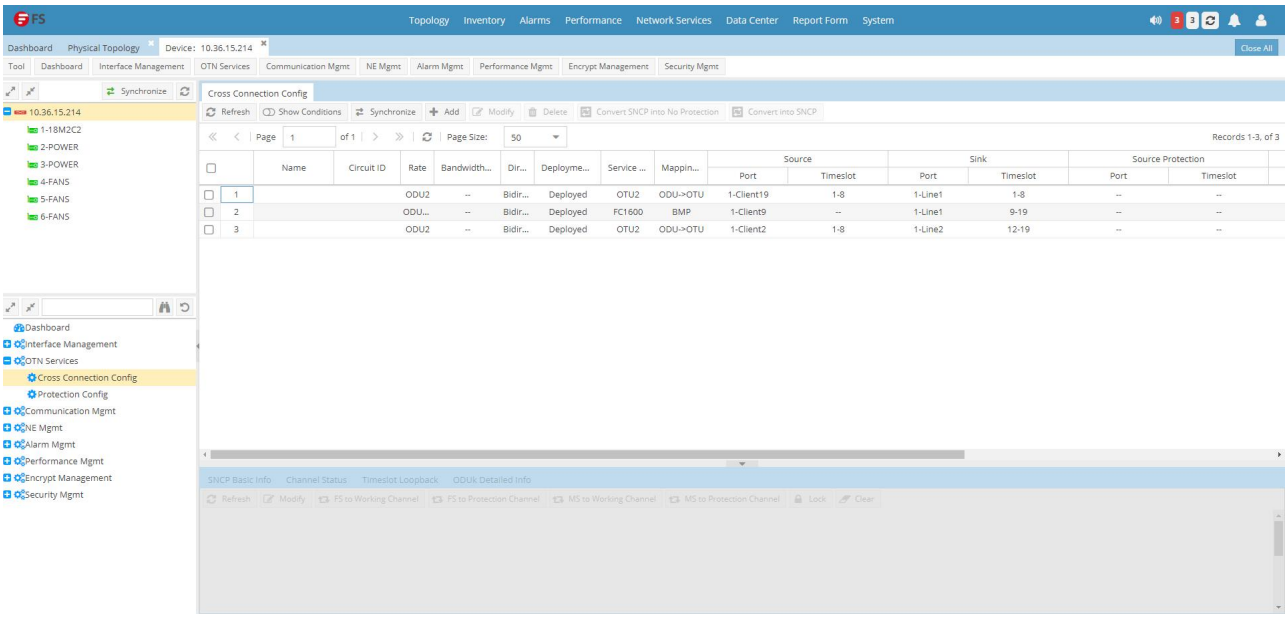
Step 4 Click Record at the top of the interface and click the relevant button in the shortcut toolbar to configure the business function.

Step 5 Click Record at the top of the interface and click the relevant tab at the bottom of the interface to view and

configure business-related parameters.

Step 6 (Optional) Right-click a record at the top of the page and click Topology Locate to display the related NE nodes on the topology page.

Figure 2-1 OTN service list



3.4. Configuring Optical Modules

Warn

- During any operation or maintenance, attention should be paid to laser safety. It is strictly forbidden to look directly at the optical port or optical fiber end with the eyes or through the instrument to prevent laser damage to the eyes.
- Before connecting an optical fiber, you should use an optical power meter to measure the current optical power of the optical fiber. The optical power can be connected only when it is less than the overload point of the optical module. If the optical power is greater than the overload point, it will cause bit errors or equipment damage. If it is less than the sensitivity, it will cause service interruption. For the technical specifications of the optical module, refer to the optical module manual or this section.
- When using an optical module, it is prohibited to directly use a jumper hard loopback (that is, directly connect the Tx interface of the optical module to the Rx interface with an optical fiber), otherwise the device will be damaged.
- with target distances of 20 km or less, 40 km (dual-fiber model), 30 km/ 40 km (single-fiber model)/ 60 km/ 80 km, 100 km or more, at least 5 dB, 10 dB, 15 dB, and 20 dB fiber attenuators must be added respectively to make the optical power less

than the overload point and greater than the sensitivity before using fiber jumper hard loopback.

Notice

- Do not stretch the optical fiber forcefully, and do not allow excessive bending of the optical fiber. Before connecting the optical fiber, you must use a dust-free cotton swab to clean the interface of the optical module and use a fiber optic cleaning box to clean the optical fiber connector. After connecting the optical fiber, the optical fiber should be straight or moderately bent (the bending diameter must be greater than 40 mm). At the same time, a water drop bend should be reserved on the fiber cable to prevent accidental water or liquid from entering the device along the fiber cable.
- In the cabinet, the fiber pigtails are routed in the direction determined by the location of the components. When connecting the optical fiber, a certain margin needs to be left under the cabinet and the excess pigtail reel needs to be placed properly.
- Ensure that the TX and RX ends of the interface are connected correctly. Ensure that the optical connector is clean and plug in the dust cap when not in use.
- The pigtails should be tied with Velcro. Do not tie the optical fibers too tightly to avoid affecting the signal transmission quality.
- When connecting optical fibers, make sure the end faces of the connected optical fibers are clean. If there is dust or particles on the end faces of the optical fibers, laser irradiation will cause uneven heating and damage the end faces of the optical fibers, thereby increasing losses and affecting transmission.
- To clean optical modules and optical fiber connectors, you must use special cleaning tools and materials, which can be purchased from the optical fiber/cable manufacturer.

Note

- You can configure the optical module only after it is inserted and working properly.
- Use an optical power meter to measure the luminous power of the installed optical module as P 1 . Compare P 1 with the optical module specifications to confirm that the optical module is working properly. For the optical module specifications, refer to the product description or the optical module manual.
- Connect the optical fiber on one side of the ODF rack connected to the device to the optical power meter and measure the

optical power as P 2 . The difference between P 2 and P 1 is less than 1 dB, indicating that the optical fiber connection is normal .

3.4.1. Configuring Optical Modules

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [Configuration/Optical Module Management]. The list displays the functions and parameter information of the optical module, as shown in the following figure and Table 2 - 8 .

Step 2 Click to select a record, click the Optical Module Status tab at the bottom of the interface, and click <Modify> to configure parameters as shown in Table 2 - 9 .

Step 3 After the configuration is complete, click <Save> to send the configuration.

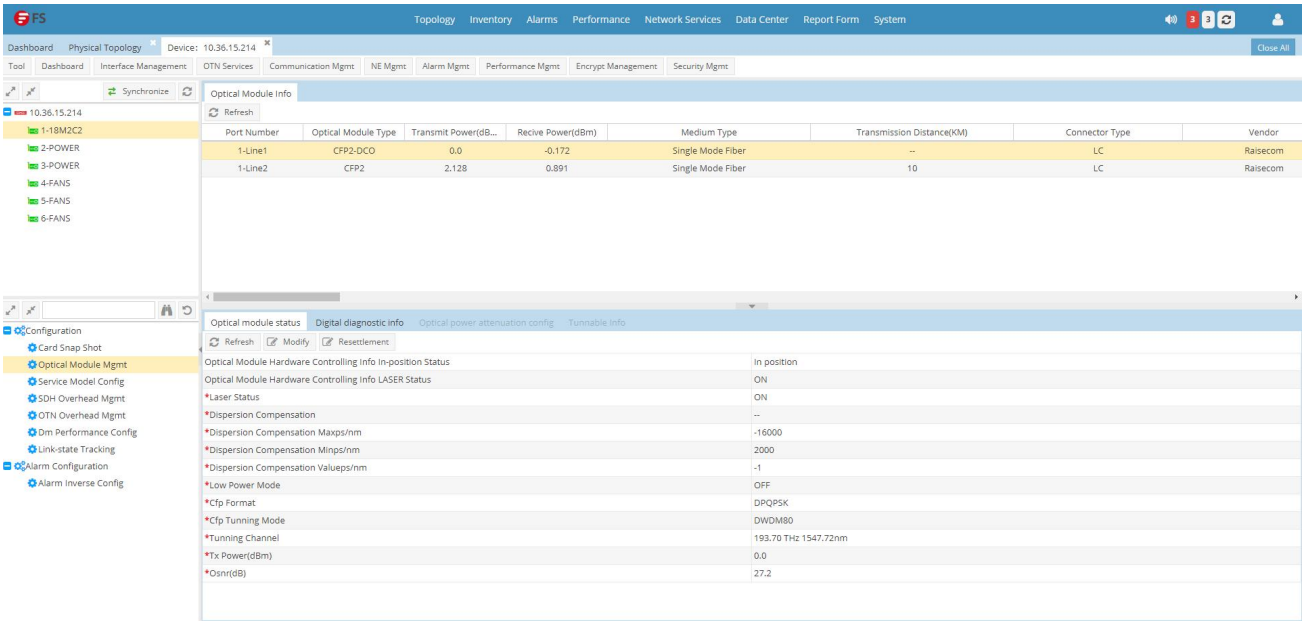


Table 2 - 8 Optical module functions and parameter display information

Parameter	Value	Note
Port Number	-	Display the port where the optical module is located.

Optical module type	• GBIC • SOLDERED • SFP • SFP+ • XBI • XENPAK • XFP • XFF • XFP- E • XPAK • X 2 • unknown	Display the optical module type.
Transmission medium	• Single mode fiber • Multimode Fiber E 50 • Multimode fiber 50 • Multimode fiber 625 • Copper wire	Display the transmission medium of the optical module.
Transmission distance (KM)	• -	Display the transmission distance of the optical module.
Connector Type	• SC • Fibre Channel Connectors DB 9 • Fibre Channel Connectors HSSDC • BNC/TNC • Fibre Channel Coaxial Header • Fiber Optic Socket • LC • MT- RJ • MU • SG • Fiber Optic Pigtail • MPO-Parallel- Optic • HSSDCII • Copper wire • RJ45	Display the connector type of the optical module.

	• unknown	
Supplier Name	-	Display the optical module vendor name.
Optical module model	-	Display the optical module model.
Whether to support digital diagnosis	• Support • Not supported	Indicates whether the optical module supports the digital diagnosis function.
Whether to support RSSI	• Support • Not supported	Indicates whether the optical module supports RSSI Function.
Version	-	Display the version of the optical module.
Serial Number	-	Display the optical module serial number.
Calibration Type	• Internal calibration • External calibration • Unknown	Display the optical module calibration type.
Maximum rate (Mbps)	- (The value is determined by the specific optical module)	Display the maximum rate supported by the optical module.
Minimum rate (Mbps)	- (The value is determined by the specific optical module)	Display the minimum rate supported by the optical module.
Wavelength (nm)	-	Display the operating wavelength of the optical module.
Wavelength tolerance (nm)	-	Display the wavelength tolerance of the optical module.
Supported business types	-	Display the supported service types.
Whether to support CDR	• Support • Not supported	Indicates whether the optical module supports CDR Function.
Laser Type	• VCSEL 850 nm • VCSEL 1310 nm • VCSEL 1550 nm • FP 1310 nm • DFB 1310 nm • DFB 1550 nm • EML 1310 nm • EML 1550 nm • Copper-Others • Others	Display the laser type of the optical module.
Is an external clock required?	• Need • Unnecessary	Indicates whether the optical module requires an external clock.

Whether it can be refrigerated	• Refrigeration • No refrigeration	Indicates whether the optical module supports the cooling function.
Is it tunable?	• Tunable • Not tunable	Indicates whether the optical module supports the tuning function.
Light detector type	• PIN • APD • OMA	Display the optical detector type of the optical module.
Whether line loopback is supported	• Support • Not supported	Indicates whether the optical module supports the line loopback function.
Support XFI Loopback	• Support • Not supported	Indicates whether the optical module supports XFI Loopback function.
Does it support VPS?	• Support • Not supported	Indicates whether the optical module supports VPS Function.
Whether to support software control transmitter switch	• Support • Not supported	Indicates whether the optical module has software-controlled laser switch function.
Whether to support software controlled standby	• Support • Not supported	Indicates whether the optical module supports the software-controlled standby function .
Does it support VPS? Internal buck	• Support • Not supported	Indicates whether the optical module supports VPS Internal step-down function .
Does it support VPS? External buck	• Support • Not supported	Indicates whether the optical module supports VPS External buck function .
Whether to support FEC	• Support • Not supported	Indicates whether the optical module supports FEC Function.
Support CMU	• Support • Not supported	Indicates whether the optical module supports CMU Function.
Received optical power detection type	• OMA • MEAN	Display the detection type of the received optical power of the optical module.
Module power consumption	• 3.5W • 2.5W • 1.5 W • > 3.5 W • Power Class 1	Display the power consumption of the optical module.

Wavelength control	• Support • Not supported	Indicates whether the optical module supports the wavelength control function.
Transmit optical power detection type	• OMA • MEAN	Display the detection type of the transmit optical power of the optical module.
Whether to support CDR	• Support • Not supported • With EDC CDR • No EDC CDR	Display the CDR of the optical module Function.
Whether to support sending direction CDR	• Support • Not supported	Display the sending direction CDR function of the optical module.
Whether to support CDR in the receiving direction	• Support • Not supported	Display the receiving direction CDR function of the optical module.
Whether to support host path loopback	• Support • Not supported	Display the host side loopback function of the optical module.
Whether to support host path PRBS	• Support • Not supported	Display the host-side PRBS of the optical module Function.
Whether network path loopback is supported	• Support • Not supported	Display the network-side loopback function of the optical module.
Whether to support network path PRBS	• Support • Not supported	Display the network-side PRBS of the optical module Function.
CFP Modulation format	• Support • Not supported	Display CFP Modulation function of the optical module.
CFP Signal pattern	• 16 QAM • QPSK • 8 QAM	Display CFP Code type of the optical module.
Number of channels	-	Display the number of channels of the optical module.

Table 2-9 Optical module configuration parameters

Parameter	Value	Note
Optical module hardware control information status	-	Display the status of the optical module.
Optical module hardware control information Laser status	• Open • Close	Configure the laser working state of the optical module. When it is turned on, the optical module can work normally. The default is turned on.

Laser status	• Open • Close	Display the laser working status of the optical module. When it is turned on, the optical module can work normally. The default is turned on.
Dispersion compensation mode	Automatic	Display the dispersion compensation mode of the optical module. Applicable to DCO optical modules.
Minimum value of automatic dispersion compensation (ps/nm)	-	Display the minimum value of the automatic dispersion compensation of the optical module. Within the range of minimum and maximum values, the optical module supports automatic dispersion compensation. Applicable to DCO Optical module.
Maximum value of automatic dispersion compensation (ps/nm)	-16000 ～ 0	Configure the maximum value of the automatic dispersion compensation of the optical module. Applicable to DCO optical modules. The default is -16000 .
Automatic dispersion compensation value (ps/nm)	-	Configure the dispersion compensation value of the optical module. This is applicable to manually configuring dispersion compensation to meet planning requirements. Applicable to DCO Optical module.
Low Power Mode	• Open • Close	Configure the low power consumption mode of the optical module.
Modulation format	• DP 16QAM • DP QPSK • DP 8QAM	Configure the modulation mode of the optical module. • DP16QAM: DP-16QAM (Dual Polarization 16-ary Quadrature Amplitude Modulation) is a modulation scheme suitable for line-side interfaces in 200G mode. • DP QPSK: DP-QPSK (Dual Polarization Quadrature Phase Shift Keying) is a modulation scheme suitable for line-side interfaces in 100G mode. • DP 8QAM: DP-8QAM (Dual Polarization 8-ary Quadrature Amplitude Modulation) is a modulation scheme suitable for line-side interfaces in 200G mode.
Tuning Mode	• DWDM 40 • DWDM 80 • DWDM 48 • DWDM 96	Configure the wavelength type of the optical module.

Tuning frequency band	-	Configure the channel of the optical module. • 40 Channel DWDM System : The frequencies of channels 1 to 40 are 192.15 THz to 196.05 THz , and the channel spacing is 0.1 THz • 80 Channel DWDM System : The frequencies of channels 1 to 80 are 192.10 THz to 196.05 THz , and the channel spacing is 0.05 THz • 48 Channel DWDM System : The frequencies of channels 1 to 48 are 191.40 THz to 196.10 THz , and the channel spacing is 0.1 THz • 96 Channel DWDM System : The frequencies of channels 1 to 96 are 191.35 THz to 196.10 THz , and the channel spacing is 0.05 THz
Transmitting output optical power (dBm)	- 500 ～ 100	Configure the transmit optical power of the optical module with EDFA function. The unit is dBm, and the step size is 0.01dBm. The specific value range is also related to the actual optical module used.
ODNR (dB)	-	Display the estimated value of OSNR (Optical Signal to Noise Radio).

Note

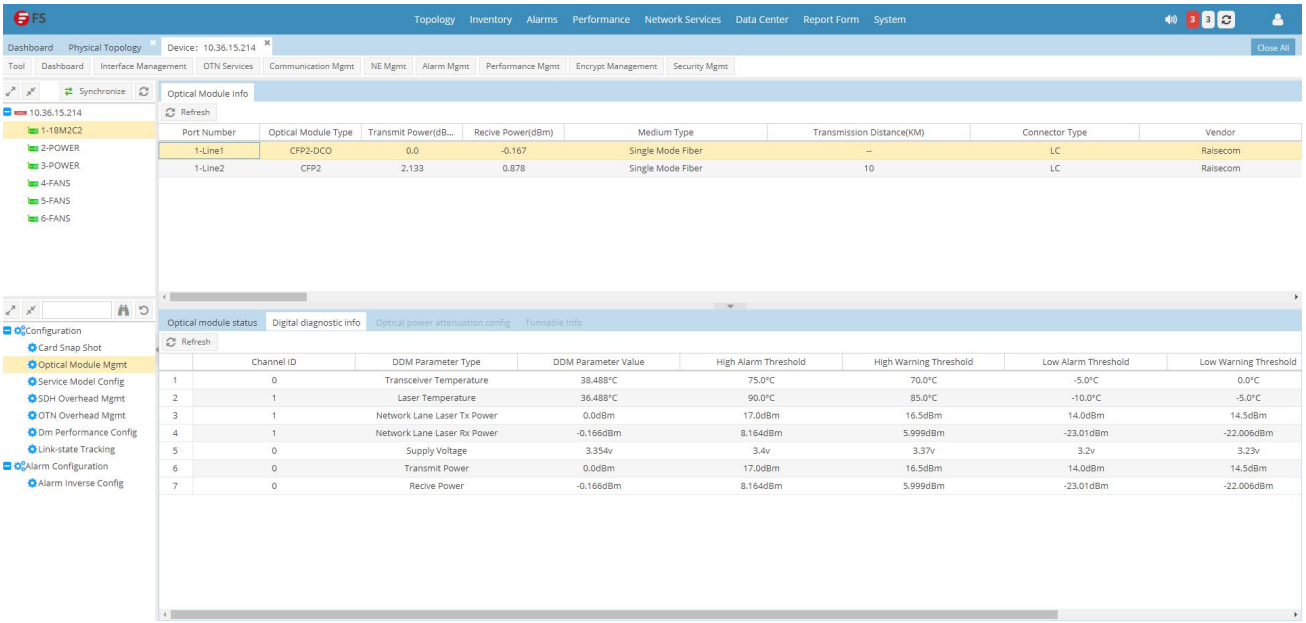
- The optical module parameters can be configured only after the optical module is inserted and working properly.
- The optical module actually inserted may only support some parameters. The interface only displays the parameters supported by the current optical module.

3.4.2. Viewing Digital Diagnostic Information

View the digital diagnostic information of the optical module

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [Optical Module Management/Optical Module Management].

Step 2 Click a record and click the Digital Diagnostic Information tab at the bottom of the page to view the digital diagnostic information of the optical module, as shown in the following figure. The parameters are listed in the following table.



Parameter	Value	Note
Network management channel number	-	Display number.
Parameter Type	- (The value is determined by the specific optical module)	Display the type of digital diagnostic parameters. Usually includes the following types: • Voltage related: APD supply voltage, + 5v voltage,+3.3v voltage, + 1.8v voltage, - 5.2v voltage • Current related: TEC current, + 5v current, +3.3v current, + 1.8v current, -5.2v current, transmit bias current • Power related: Transmitted optical power, received optical power • Laser temperature • Laser wavelength
Value	-	Display Values.
High alarm threshold	-	Display the upper alarm threshold. The severity level of an alarm is higher than that of a warning.
High warning threshold	-	Display the upper warning threshold.
Low alarm threshold	-	Display the lower alarm threshold.
Low warning threshold	-	Display the lower warning threshold.
Alarm status	• Normal • High Alarm • High warning • Low Alarm • Low warning	Display the alarm status of the optical module.

Valid status	• Valid • Invalid	Indicates whether the optical module is valid.

3.5. Configuring the Interface

Note

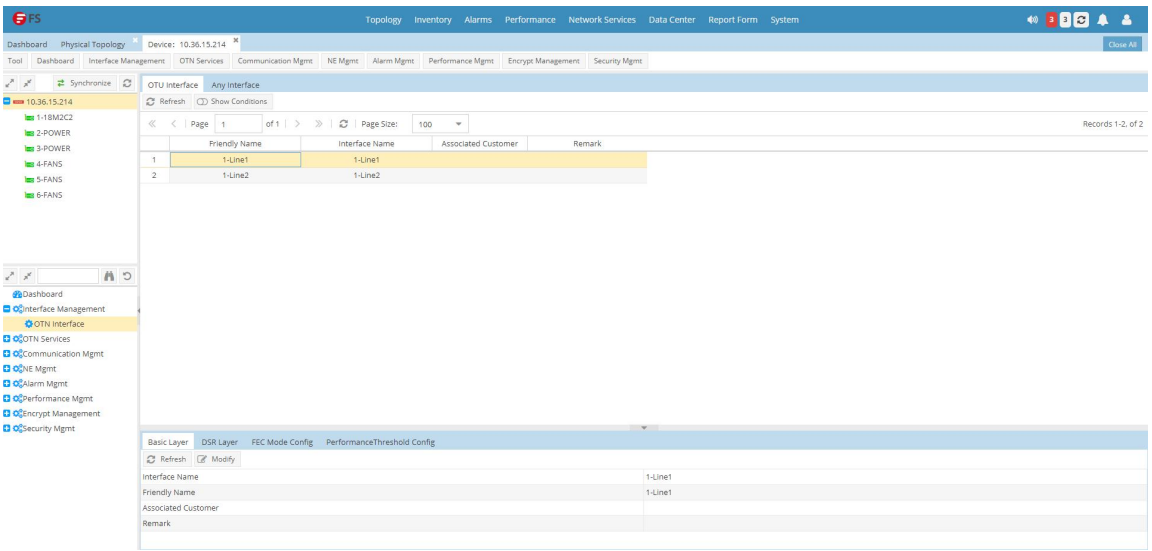
The device actually used may only support some functions and parameters. Please refer to the actual display of the network management system.

3.5.1. Configuring Basic Interface Functions

Step 1 In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Interface Management] and its submenus. The interface records of the board are displayed in the list, as shown in the following figure.

Step 2 Click to select the interface record, click the "Basic Layer" tab at the bottom of the interface, click <Modify>, and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.



Parameter	Value	Note
Interface Name	-	Display the interface name.
Friendly Name	0 to 64 Characters	Configure an interface friendly name.
Related clients	-	Click < ▪▪▪ > , select the client associated with the service .
Port Description	0 to 255 Characters	Configure interface description information.

3.5.2. Configuring OTN Interface

Note

Before configuring an Any interface, configure a cross-connection to determine the service type of the interface.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Interface Management/OTN Interface]. The list displays related interface records.

Step 2 Click the "OTU Interface" or "Any Interface" tab, click the interface record, click the "DSR Layer" tab at the bottom of the interface, click <Modify>, and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value	Note
ALS Enable	• Enable • Prohibit	Configure ALS on an Interface Function. Enable ALS After that, the interface will not emit light when there is no signal received , to avoid laser damage to workers. Both ends of the link must support ALS function, otherwise the interface may not light up. The default is disabled.
Maintenance signal insertion	• Normal • OTUk_AIS • ODUk_AIS • ODUk_OCI • ODUk_LCK	Configure the maintenance signal insertion function of the interface, which is applicable to OTU service interfaces. • Normal means that the insertion maintenance signal function is not executed . • Other types indicate that the interface is executing the corresponding insertion maintenance signal function.

Loopback status	• Not looped back • Inner Ring • Outer Ring	Configure the interface loopback function. The default is no loopback.

Step 1 Click the Any Interface tab, click to select the interface record with the service type of 10GE, click the Maintenance Configuration tab at the bottom of the interface, click Modify, and the parameters are shown in the following table.

Step 2 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value	Note
VLAN Configuration	0 ~ 4094	Configure the management VLAN of the interface . The default value is 0 , indicating no configuration.

Step 3 Click the Any Interface tab, click the client-side Ethernet service interface record, and click the Port Statistics tab at the bottom of the interface. The parameters are shown in the following table. Click <Clear> at the bottom of the interface to clear the statistics.

Parameter	Note
Number of normal messages received	Display the number of normal received messages.
Number of normal messages sent	Display the number of normal packets sent.
Receive CRC Number of error messages	Display received CRC Number of packets with checksum errors.
Number of received packets	Display the number of received packets.
Number of unicast messages received	Display the number of received unicast packets.
Number of broadcast messages received	Display the number of received broadcast messages.
Number of multicast messages received	Display the number of received multicast packets.
Number of packets sent	Display the number of sent packets.
Number of unicast messages sent	Display the number of sent unicast packets.
Number of broadcast messages sent	Display the number of sent broadcast messages.
Number of multicast messages sent	Display the number of sent multicast packets.

Step 4 Click the Any Interface tab, click the client-side Ethernet service interface record, and click the RMON Statistics Status tab at the bottom of the interface. The parameters are shown in the following table. Click <Clear> at the bottom of

the interface to clear the statistics information.

Parameter	Note
Number of bytes received	Display the number of bytes in received messages.
Number of received packets	Display the number of received packets.
fragment Number of packages	Display is too small and FCS Number of error packets
1519 ~ max Byte Packet Number	The displayed message length is 1519 Number of packets above byte
undersize Number of packages	Display the number of undersized packets
jabber Number of packages	Display too large and FCS Number of error packets
65～127 Byte Packet Number	Display the number of packets with a message length of 65-127 bytes
oversize Number of packages	Excessive number of packages displayed
512～1023 Byte Packet Number	Display the number of packets with a message length of 512-1023 bytes
1024～ 518 Byte Packet Number	Display the number of packets with a message length of 1024-1518 bytes
256~511 Byte Packet Number	Display the number of packets with a message length of 256-511 bytes
128～255 Byte Packet Number	Display the number of packets with a message length of 128-255 bytes
Number of dropped packets	Display the number of dropped packets

Step 5 Click the Any Interface tab, click the client-side Ethernet service interface record, and click the MIB Statistics Status tab at the bottom of the interface. The parameters are shown in the following table. Click <Clear> at the bottom of the interface to clear the statistics.

Parameter	Note
Number of multicast messages sent	Display the number of sent multicast packets.
Number of sent error packets	Display the number of sent error packets.
Number of bytes sent	Display the number of bytes in sent messages.
Number of bytes received	Display the number of bytes in received messages.
Number of multicast messages received	Display the number of received multicast packets.
Number of unicast messages sent	Display the number of sent unicast packets.
Number of unicast messages received	Display the number of received unicast packets.
Number of broadcast messages sent	Display the number of sent broadcast packets.
Number of broadcast messages received	Display the number of received broadcast packets.
Number of received error packets	Display the number of received error packets.

Step 6 Click the Any Interface tab, click the service interface record of 10GE, 10G FC, 40GE, 100GE on the client side that uses GFP-F encapsulation, and click the GFP-F Statistics Status tab at the bottom of the interface. The parameters are shown in the following table. Click <Clear> at the bottom of the interface to clear the statistics information.

Parameter	Note
FCS Number of error packets	Display FCS Frame check sequence error packets
Number of bytes sent	Display the number of bytes sent.
Number of frames sent	Display the number of sent frames.
Receive Bytes	Display the number of bytes received.
Uncorrected FEC mistake	Display the number of packets that have not been corrected by the cHEC core header error check.
Number of received frames	Display the number of received frames.
Correction FEC mistake	Displays the number of cHEC core header error correction packets.

Step 7 Click the Any Interface tab, click the client-side 8G FC service interface record, and click the Interface Statistics tab at the bottom of the interface. The parameters are shown in the following table. Click <Clear> at the bottom of the interface to clear the statistics.

Parameter	Note
Coding Violations	Display the number of encoding violation packets.
FCS Number of error packets	Display FCS Frame check sequence error packets
Number of received frames	Display the number of received frames.
Receive words	Display the number of received character sets.
Number of frames sent	Display the number of sent frames.
Send words	Display the number of character sets sent.

Step 8 Click the Any Interface tab, click the client-side SDH service interface record, click the Threshold Configuration tab at the bottom of the interface, click Modify, and the parameters are shown in the following table.

Parameter	Value	Note
Regenerator Section Bit Error Rate Degradation Threshold	• 1.0E - 6 • 1.0E - 7 • 1.0E - 8 • 1.0E - 9	Configure the Regenerator Section Bit Error Rate Degradation Threshold. Applicable to SDH services. Default is 1.0E-6.

Regenerator Section Bit Error Rate Exceeding Threshold	1.0E - 5	Configure the Regenerator Section Bit Error Rate Exceeding Threshold. Applicable to SDH services. Default is 1.0E-5.

3.6. Configuring Device Functions

3.6.1. Configuring Service Mode

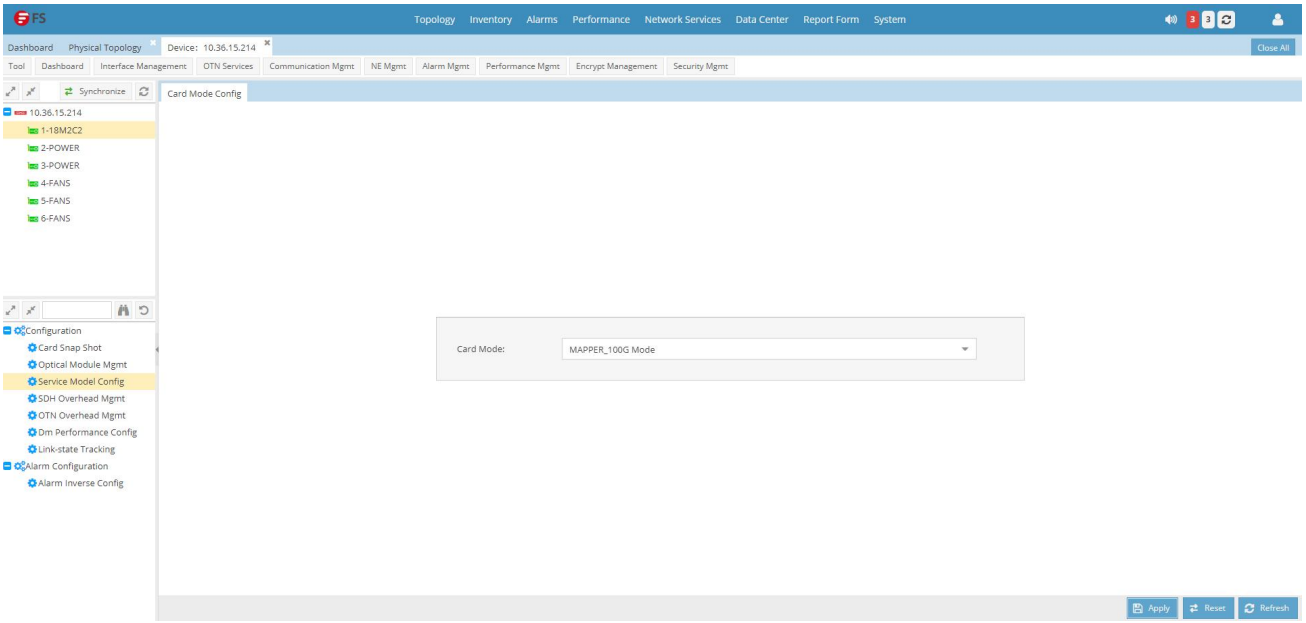
Note

- Please configure the client-side service mode first, and then configure functions such as cross-connection and protection group.
- If you have configured functions such as cross-connection and protection group, you need to delete the existing configuration before changing the client-side service mode.
- Client services support multiple modes, and can only be configured in one mode at a time. The maximum total bandwidth of all client interface services is 200 G. Table 3-2 shows the client services applicable to different modes, available panel interfaces, matching optical modules, and client ODUk cross - connection functions .
- The line side service supports 100G mode and 200G mode, and can only be configured in one mode at a time. The line side of the 100G mode is 2 100G interfaces, each of which supports the transmission of 1 OTU4 service ; the line side of the 200G mode is 1 200G interface , which supports 2 transmission channels, and each transmission channel supports 1 OTU4 service.

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [Configuration/Service Mode Configuration], as shown in the following figure.

Step 2 Click the "Board Mode Configuration" tab. The parameters are shown in the following table.

Step 3 After the configuration is complete, click <Apply> to deliver the configuration.



Parameter	Value	Note
Board Mode	• OTN mode • MAPPER mode • MIx Mode • OTU4 mode • 100GE mode • 40GE mode • OTN_100G mode • OTN_OTU4 mode • MAPPER_ 100G mode • MAPPER_OTU4 mode • MAPPER_6 FC 3200 mode	Configure the client-side service mode. • The client-side business model is shown in Table 3-2. • LINE200G indicates that the line side is configured in 200G mode on top of various existing modes. The default value is OTN mode.
	• MAPPER_ 40GE mode	
	• OTN_LINE 200G mode	
	• MAPPER_LINE 200G mode	
	• Mix _LINE 200G mode	
	• OTU4 _LINE 200G mode	
	• 100GE_LINE 200G mode	
	• 40GE_LINE 200 G mode	
	• OTN_100G_LINE 200G mode	
	• OTN_OTU4 _LINE 200G mode	
	• MAPPER_ 100 G_LINE 200G mode	
	• MAPPER_OTU4 _LINE 200G mode	
	• MAPPER_ 6 FC 3200 _LINE 200G mode	

	• MAPPER_ 40GE_LINE 200G mode	
	• 40GE_ 100GE mode	
	• 40GE_ 100GE_LINE 200G mode	
	• MAPPER_3 FC 3200 mode	
	• MAPPER_ 3 FC 3200 _LINE 200G mode	

3.6.2. Configuring DM Delay Measurement

Note

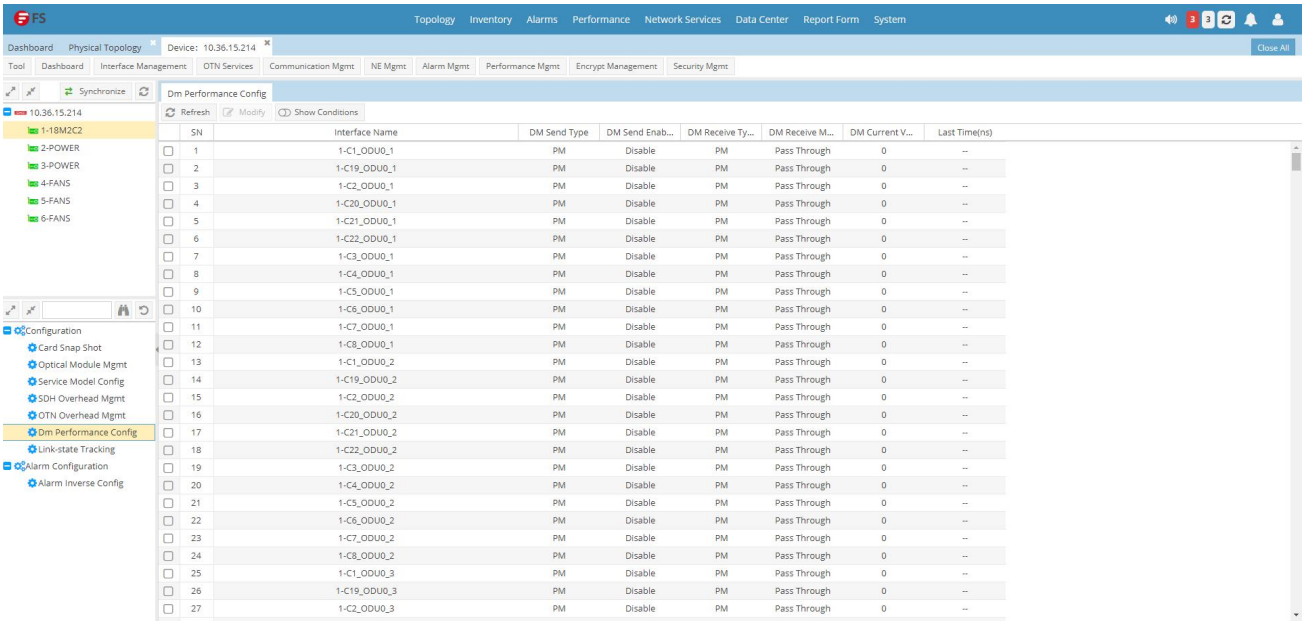
- Configure a cross-connection before configuring delay measurement for the interfaces related to the cross-connection.
- At the same time, the same cross-connection can only enable the delay measurement of one interface.

After the performance monitoring function is enabled, the DM (Delay Measure) function is supported between the two devices. The port of one device acts as the sender to send test packets, and the port of the other device acts as the receiver to loop back packets. The receiver calculates the packet delay to complete the delay measurement function between interfaces.

Step 1 In the resource tree of the main interface, click to select a board. In the function list, click [Configuration/DM Performance Configuration], as shown in the following figure.

Step 2 Click the record and click <Modify>. The parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.



Parameter	Value	Note
Port Name	-	Display the port name.
DM Send Type	• PM • TCM 1 to TCM 6	Configuring DM Type of measurement message sent . The default is PM .
DM Send Enable	• Enable • Prohibit	Configuring DM Send measurement message function. Disabled by default.
DM Receiving Type	• PM • TCM 1 to TCM 6	Configuring DM Type of received measurement message . The receiving type of the receiving end should be the same as the sending type of the sending end. The default is PM .
DM Receive Enable	• Feedback • Transparent transmission	Configuring DM Receive measurement message function. • Return: Applicable to the receiving end. • Transparent transmission: Applicable to non-receiving end. The default is backhaul.
DM Real-time value (us)	-	Show DM Real-time measurements.
Duration (ns)	-	Display the measurement duration.

3.6.3. Configuring Failover

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [Configuration/Failover]. The parameters are shown in the following table.

Step 2 After the configuration is complete, click <Apply> to send the configuration.

Parameter	Value	Note
Failover	• Enable • Prohibit	Configure the failover function. Disabled by default.

3.6.4. Configuring SDH Overhead

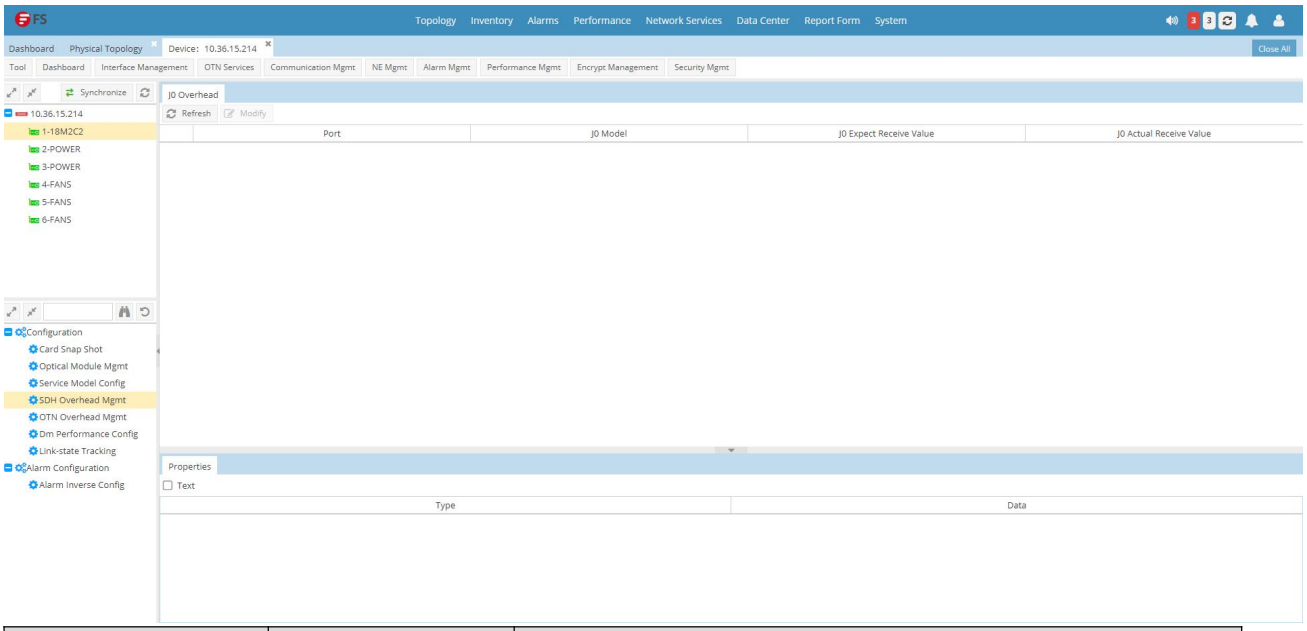
After the OTN cross-connection is configured on the interface accessing the SDH service, the SDH overhead can be configured.

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [Configuration/SDH Overhead Management].

Step 2 Click the J0 Overhead tab. The port records that support the configuration of overhead bytes are listed in the configuration interface, as shown in the following figure.

Step 3 Click the record and click <Modify>. The parameters are shown in the following table .

Step 4 After the configuration is complete, click <Save> to deliver the configuration.



Parameter	Value	Note
Port	-	Display port information.
Model	• 1 byte • 16 byte	Configure the trace character mode. 1 Byte mode does not require configuration of send values and expected receive values. The default value is 16 byte.
J0 Expected Received Value	-	Configure the trace characters you expect to receive. Chinese characters are not supported . Suitable for 16 Byte mode.

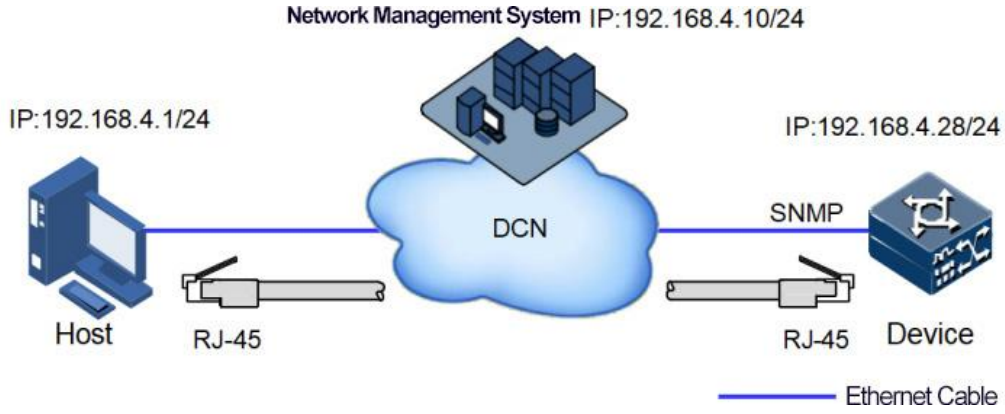
3.7. Configuration Examples

3.7.1. Example for configuring out-of-band DCN network management

Network Requirements

The network management system has added device network elements through out-of-band DCN, and the network is shown in Figure 2-2 .

Figure 2 - 2 Network connection



The configuration requirements and prerequisites are described below.

- The device network element has been added to the network management system. For specific operations, please refer to " 1.5.2 Example of entering the configuration interface".
- The device's Trap destination address needs to be configured. When a fault occurs, the device will send alarm information to the network management system to improve maintainability. The network management system Trap receiving port uses the default port 162 .

Configuration steps

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Communication Parameter Configuration].

Step 2 In the configuration interface on the right, click the "Trap Target Configuration" tab, click <Add>, and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value
Target Address	192 . 168 . 4 . 10
Port	162

Check the results

- Through verification operations such as plugging and unplugging cables and restarting devices, the network management system can receive alarms from device network elements.
- In the network management system, enter the configuration interface, click the network element or board in the resource tree, and then click the configuration menu in the function list to check whether the device configuration information can

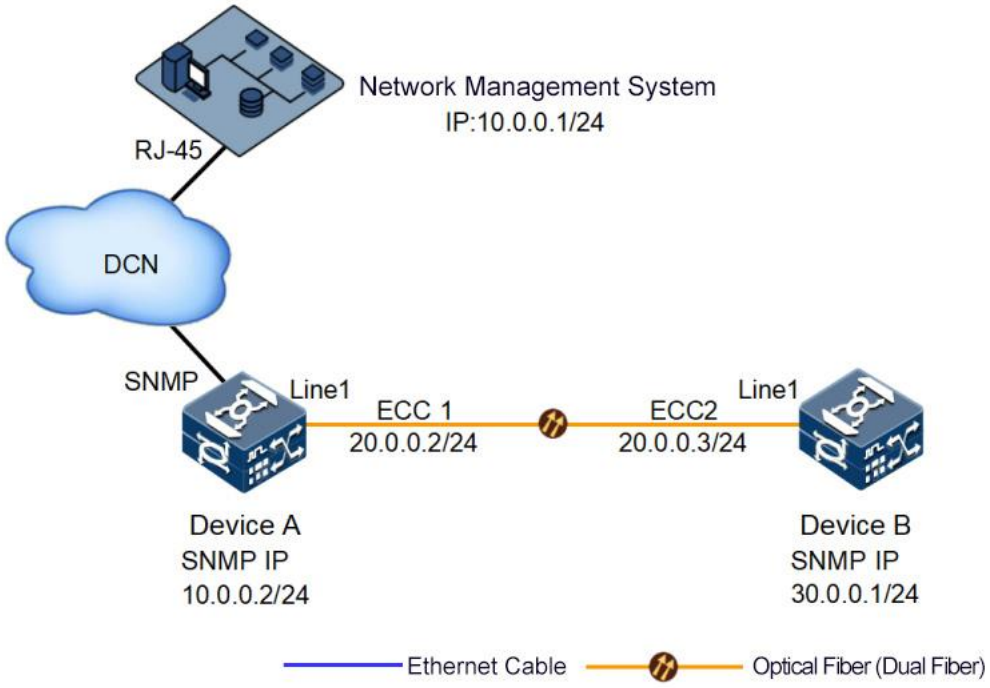
be displayed normally.

3.7.2. Example of configuring ECC network management

Network Requirements

Configure the ECC IP address network management function of the device. The network connection is shown in Figure 2 - 3 .

Figure 2 - 3 Network connections



The configuration requirements and prerequisites are described below.

- The network management system needs to manage Device B through the ECC channel.
- The Line1 interfaces of Device A and Device B are connected through optical fibers, and the default is GCC0 overhead to transfer network management information.The network management system has added Device A and Device B network elements.
- IP address planning is shown in Table 2 - 10. The SNMP management address of each NE must be in different network segments, the SNMP and ECC addresses of the same NE must be in different network segments, and the ECC channel IP addresses of the NEs at both ends of the ECC channel must be in the same network segment.
  - Because the ECC channel IP address and the SNMP management IP address of the device network element are not in

the same network segment, static routes need to be configured on Device A and Device B.

- Because the SNMP address of Device B and the IP address of the network management system host are not in the same network segment, you need to configure a static route on the network management system host.

Table 2-10 IP address planning

Parameter	Device A	Device B
NE SNMP Management IP Address and mask	• IP : 10.0.0.2 • Mask : 255.255.255.0	• IP : 30.0.0.1 • Mask : 255.255.255.0
ECC Channel IP Address and mask	• IP : 20.0.0.2 • Mask : 255.255.255.0	• IP : 20.0.0.3 • Mask : 255.255.255.0

Configuration steps

Step 1 Configure the bridge port.

1. In the resource tree on the main interface, click to select the root node of the network element. In the function list, click [Communication Management/Auto-Topology Discovery Configuration/Bridge Information Configuration].
2. Click the Bridge Port Configuration tab, click the ECC interface record and click <Delete> to configure the ECC interface not as a bridge port.

Step 2 Configure the ECC network management channel.

1. In the resource tree on the main interface, click to select the NE root node, and in the function list, click [Communication Management/Network Management Channel Management].
2. In the configuration interface on the right, click the ECC Channel Management tab, click Port Record, and configure at the bottom of the interface.
3. Click the Protocol Configuration tab and configure channel parameters as shown in Table 2-11. After completing the configuration, click Save to deliver the configuration.
4. Click the Channel Configuration tab and select the cost of the channel. The parameters are shown in Table 2-12. After the configuration is complete, click Save to deliver the configuration.

Table 2-11 Protocol Configuration

Parameter	Device A	Device B
Network management channel number	1	1

Channel Enable	Enable	Enable
Peer IP address	20.0.0.2	20.0.0.1
IP address	20.0.0.1	20.0.0.2
PPP Automatic reconnection	Enable	Enable

Note

The interface parameters not mentioned in the above table all use the default configuration.

Table 2 - 12 -channel configuration

Parameter	Device A	Device B
Delivery Channel	GCC0	GCC0

Step 3 Configure the GCC overhead function to be enabled.

1. In the resource tree on the main interface, click to select the 18M2C2 board. In the function list, click [Configuration/OTN Overhead Management].
2. In the configuration interface on the right, click the GCC Overhead tab, click the port record and click <Modify>. Configure in the configuration panel. The configuration parameters are shown in Table 2-13 .
3. After the configuration is complete, click <Save> to deliver the configuration.

Table 2-13 GCC overhead functions

Parameter	Device A	Device B
Port ID	Line 1	Line 2
Network management information transmission channel	GCC0	GCC0

Step 4 Configure static routes.

1. In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Communication Parameter Configuration].
2. In the configuration interface on the right, click the Static Route Configuration tab, click <Add>, and configure in the

configuration panel. The configuration parameters are shown in Table 2 - 14 .

3. After the configuration is complete, click <Save> to deliver the configuration.

Table 2-14 Configure static routes

Parameter	Device A To B Routing	Device B Routing to the Network Management System
Target IP address	30 . 0 . 0 . 1	10 . 0 . 0 . 1
Target subnet mask	255 . 255 . 255 . 0	255 . 255 . 255 . 0
Gateway IP address	20 . 0 . 0 . 2	20 . 0 . 0 . 1

Note

- Because Device A needs to forward management messages from the network management system, you need to configure a static route from Device A to Device B.
- Because Device B needs to communicate with the network management system, you need to configure a static route from Device B to the network management system.
- The above routes need to be forwarded through the ECC channel, so the "Gateway IP Address" needs to be filled in with the next hop address of the ECC channel.

Step 5 Configure the Trap destination address.

1. In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Communication Parameter Configuration].
2. In the configuration interface on the right, click the Trap Target Configuration tab, click <Add>, and configure in the configuration panel. The configuration parameters are shown in Table 2 - 15 .
3. After the configuration is complete, click <Save> to deliver the configuration.

Table 2-15 Configure Trap target address

Parameter	Device A	Device B
Target Address	10.0.0.1	10.0.0.1
Port	162	162

Step 6 Configure a static route to Device B on the NMS host. The destination address is the SNMP address of Device B, and

the next hop address is the SNMP address of Device A.

1. Open the CMD command line tool.
2. Enter the following command and press Enter.

   route add 30 . 0 . 0 . 1 mask 255 . 255 . 255 . 0 10.0.0.2

Check the results

Step 1 In the network management system, click the NE or board in the resource tree, then click the Configuration menu in the function list to check whether the device configuration information can be displayed normally.

Step 2 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Communication Management/Network Management Channel Management].

Step 3 In the configuration interface on the right, click the ECC Channel Management tab and select a board in the resource tree.

Step 4 Click Port Record and select the "Protocol Status" tab at the bottom of the interface to view the channel status and statistical data. If the configuration is correct, the parameters should be as shown in Table 2 - 16 .

Table 2-16 View the protocol status of Device A and B

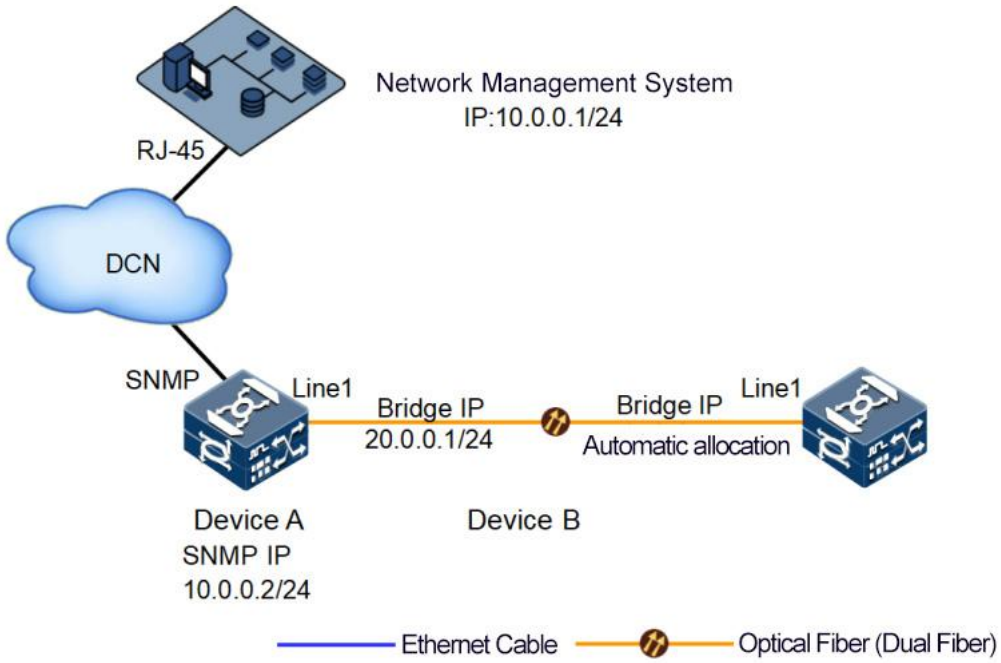
Parameter	Value	Note
LCP state	OPENED	Display the protocol status of the logical link of the PPP protocol. In the network management process, it is usually OPENED state.
NCP state	OPENED	show ppp The state of the network layer protocol carried by the logical link. In the network management process, it is usually in the OPENED state.
Send Bytes	-	Display the number of NMS message bytes sent. After refreshing, the sent bytes should increase.
Sending a message	-	Display the number of sent NMS messages. After refreshing, the number of sent messages should increase.
Receive Bytes	-	Display the number of network management message bytes received. After refreshing, the received bytes should increase.
Receiving messages	-	Display the number of received NMS messages. After refreshing, the number of received messages should increase.

3.7.3. Topology Auto-Discovery Configuration

Network Requirements

Based on the topology automatic discovery function and Bridge IP address to manage remote devices, the network connection is shown in Figure 2 - 4 .

Figure 2 - 4 Network connections



The configuration requirements and prerequisites are described below.

- The local device Device A and the remote device Device B are physically connected.
- The network management system has managed Device A through out-of-band DCN. Device A, as a gateway network element, forwards the network management information of Device B, a non-gateway network element.
- The parameters of the automatic topology discovery function of the remote devices in the office are at the default values.
- topology automatic discovery function to add remote devices to the network management system for network management. The bridge IP address of the local device needs to be configured as 20.0.0.1/24 , and the bridge IP address of the remote device uses the IP address automatically assigned by the network management system.

Configuration steps

Step 1 Configure the bridge IP address of Device A.

1. In the resource tree on the main interface of Device A, click to select the root node of the network element. In the function list, click [Communication Management/Auto-discovery Configuration of Topology/Bridging Information Configuration].
2. Click the Bridge Global Configuration tab and configure the parameters as shown in the following table.
3. After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value
Bridge IP address	20 . 0 . 0 . 1
Bridge subnet mask	255 . 255 . 255 . 0

Step 2 Enable the TDP function on Device A.

1. In the resource tree on the main interface of Device A, click to select the root node of the network element. In the function list, click [Communication Management/Auto Topology Discovery Configuration/Topology Discovery Configuration].
2. Click the Topology Discovery Global Configuration tab and configure the parameters as shown in the following table.
3. After the configuration is complete, click <Apply> to deliver the configuration.

Parameter	Value
TDP Function Enablement	Enable

Step 3 Configure the management IP address of Device B.

1. In the resource tree on the main interface of Device A, click to select the root node of the network element. In the function list, click [Communication Management/Auto Topology Discovery Configuration/Topology Discovery Configuration].
2. Click the Discovered NE Configuration tab, click an NE record and select [Auto-assign IP]. Based on the bridge IP address of the gateway NE, a bridge IP address in the same network segment is automatically assigned to the remote end.
3. Click the "Not Created" record and click <Create NE> to add the discovered NE device to the network management system.

Check the results

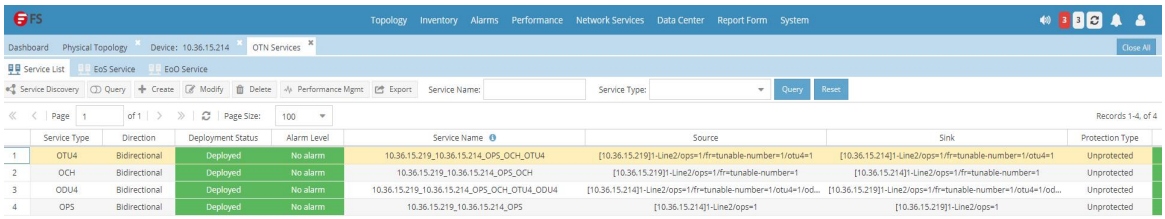
- In the top navigation, click Topology/Topology View to view the added Device B.
- Double-click Device B, and then click the Configuration menu in the Function List to check whether the device configuration information can be displayed normally.

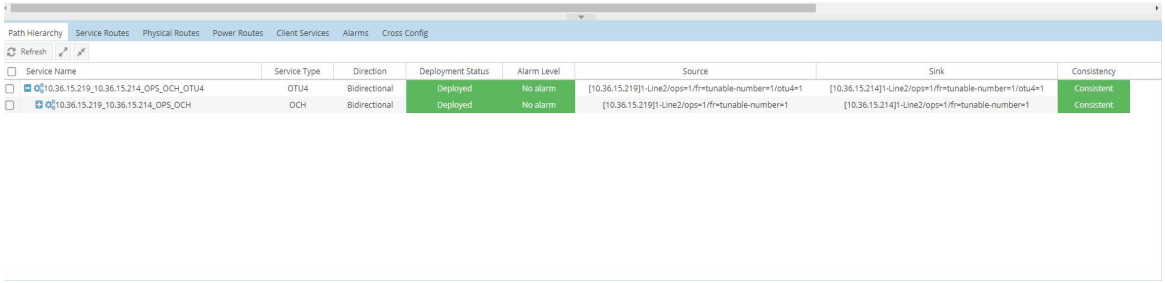
3.7.4. Configuring End-to-end Services

Network Requirements

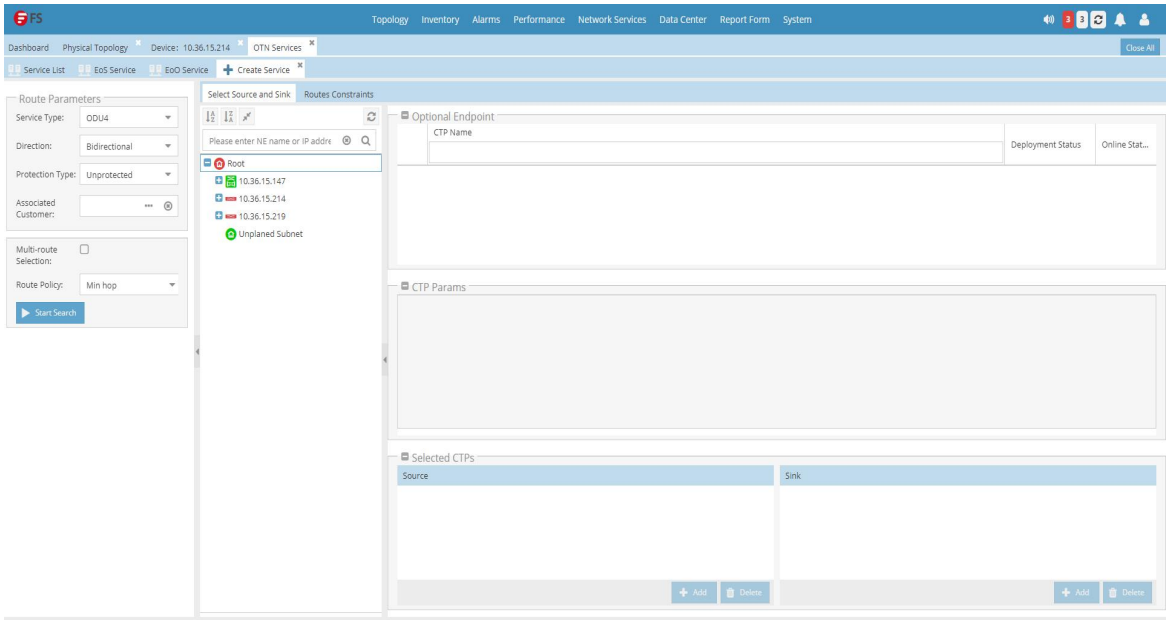
Configuration steps

Step 1 Go to the Service/End-to-End Service/OTN Service page and view the Service List.

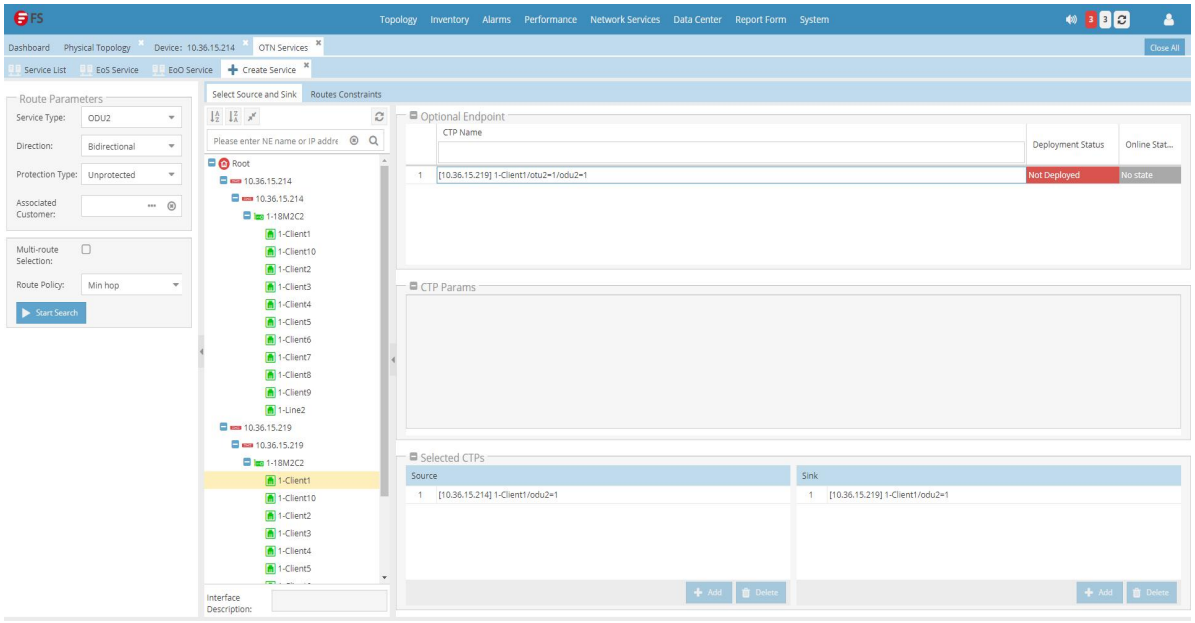


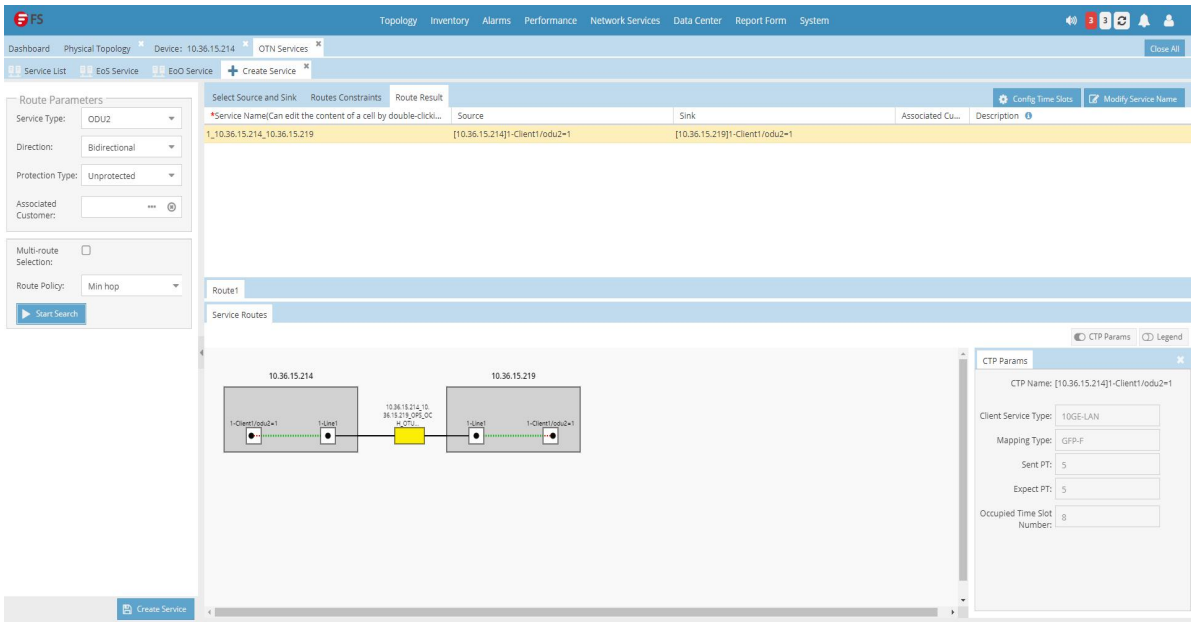


Step 2 Click "Create Service" to create a new service connection.

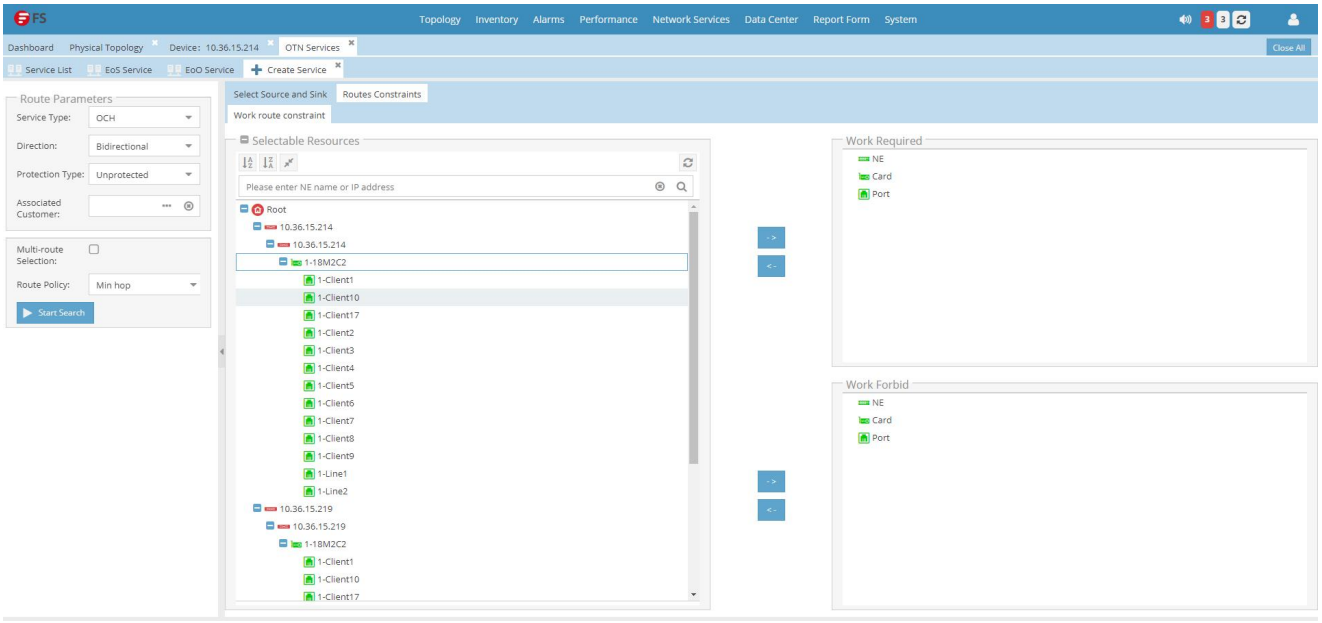


Step 3 Select "Service Type" as ODUk service, choose the corresponding source endpoint, click "Initiate Search," and "Create Service."



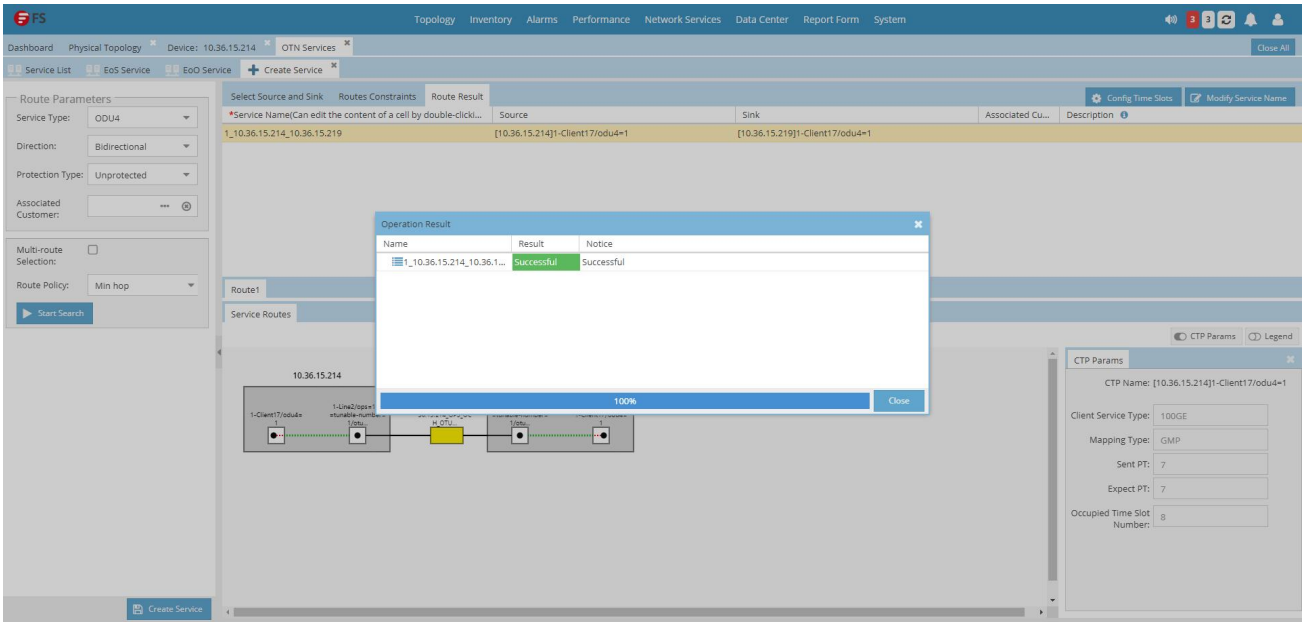


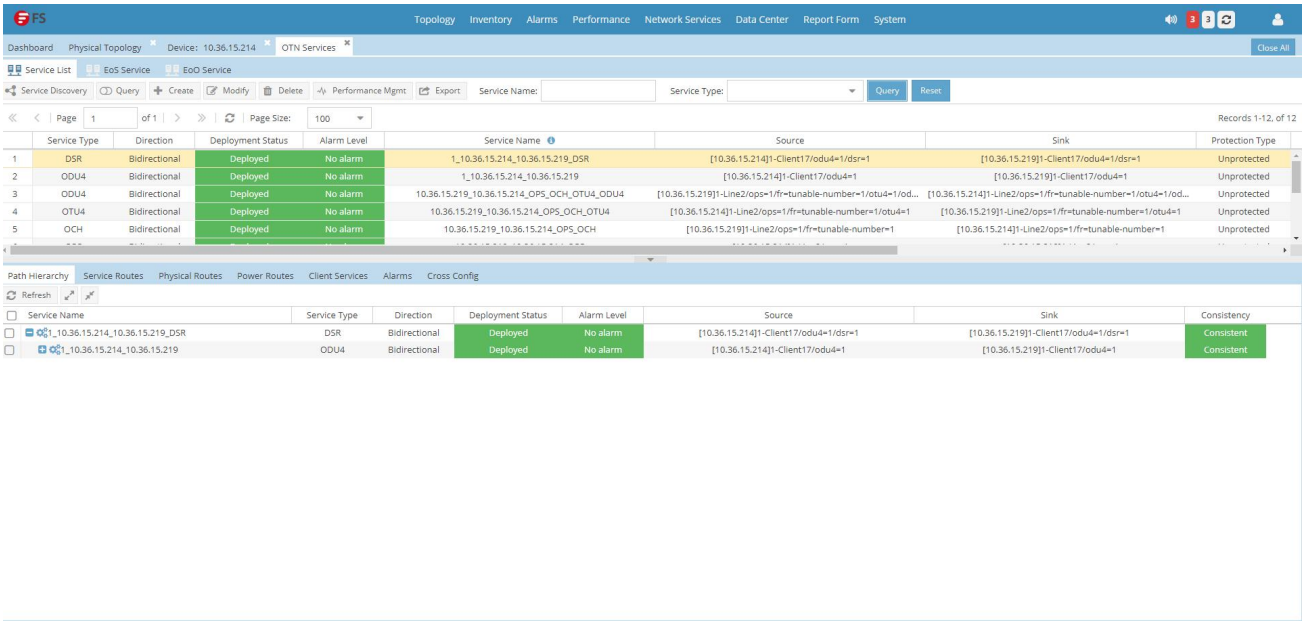
Step 4 (Optional) Click Routing Constraints and select the network elements/boards/ports that the link must pass through or that are prohibited from working.



Check the results

- The result of the service creation operation is successful.
- The newly created service is added to the service list, and the link information can be viewed normally.
- You can view the created service cross-connection on the "Device/OTN Service/Cross-connection Configuration" page.





4. OTN Services

This chapter introduces how to configure the OTN service-related functions of the device.

- Overview
- Configure OTN Services
- Configuration Overhead
- Configuration Examples

4.1. Overview

4.1.1. Default Configuration

The default configuration supported by 18M2C2 is shown in Table 3-1 .

Table 3-1 Default Configuration

Configuration items	18M2C2
In-band network management channel	• Enable GCC0 for both L1 and L2 • Integrate GCC0 of both L1 and L2 into the Bridge interface to support automatic topology discovery

Client-side mapping mode	OTN mode

Note

- By default, no cross-connection or protection function is configured on the device.
- The interfaces and services supported by the client-side mapping mode are shown in Table 3-2 .
- Client services support multiple modes, and can only be configured in one mode at a time. The maximum total bandwidth of all client interface services is 200G. Table 3-2 shows the client services applicable to different modes, available panel interfaces, matching optical modules, and client ODUk cross-connection functions .
- The line-side service supports both 100G and 200G modes, but only one mode can be configured at a time. In the 100G mode, the line side has two 100G interfaces, each supporting the transmission of one OTU4 service. In the 200G mode, there is a single 200G interface, which supports two transmission channels, with each channel supporting one OTU4 service.10G Any services include 10GE /OTU 2 /OTU2E/STM- 64 / 8G FC/ 10G FC (Fiber Channel) services.
- Panel interface 17 uses a QSFP+ PSM 4 optical module and an MPO-LC branch fiber, it supports fanning out 4 (port numbers 19 to 22) 10G Any service SFP+ ports.

Table 3-2 Client - side business model

Mode	Client Services	Panel Interface	Optical Module Encapsulation Type	Client-Side ODUk Cross-Connect
100GE	• 100GE	17 and 18	QSFP28	Not supported
40GE	40GE	17 and 18	QSFP+	Not supported
	16 G FC	5 to 16	SFP+ (must support 16G FC , up to 6 channels)	
	10G Any	5 to 16	SFP+	
40GE_ 100GE	40GE	17	QSFP+	Not supported
	• 100GE • OTU4	18	QSFP+	
	16G FC	1 to 6	SFP+ (must support 16G FC , up to 4 channels)	
	10G Any	1 to 6	SFP+	
40GE_ 16 × 10GE	40GE	17	QSFP+	Not supported

	10G Any	1 to 16	SFP+	
Mix Mode	16 G FC	9 to 16	SFP+ (must support 16G FC , up to 6 channels)	Not supported (i.e. Mapper model)
	10G Any	9 to 16	SFP+	
	OTU 2	1 to 8	SFP+	Support (ie OTN model)
		17 (corresponding to 4 Fan-out interfaces 19 to 22)	QSFP+ PSM 4	
Mapper	16G FC	1 to 8	SFP+ (must support 16G FC , up to 6 channels)	Not supported
		9 to 16	SFP+ (must support 16G FC , up to 6 channels)	
	10G Any	1 to 16	SFP+	
		17 (corresponding to 4 Fan-out interfaces 19 to 22)	QSFP+ PSM 4	
Mapper_ 100GE	• 100GE	17	QSFP28	Not supported
	10G Any	1 to 10	SFP+	
Mapper_ 3 × 32G FC	32G FC	9-11	SFP28	Not supported
	16 G FC	• 1 to 8 • 12 to 15	SFP+ (must support 16G FC , up to 6 channels)	
	10G Any	• 1 to 8 • 12 to 15	SFP+	
Mapper_ 6 × 32G FC	32 G FC	9 to 14	SFP 28	Not supported
Mapper_OTU4	OTU4	17	QSFP28	Support
	10G Any	1 to 10	SFP+	Not supported
OTN	OTU 2	1 to 16	SFP+	Support

		17 (corresponding to 4 Fan-out interfaces 19 to 22)	QSFP+ PSM 4	
OTN_100GE	• 100GE	17	QSFP28	Not supported
	OTU 2	1 to 10	SFP+	Support
OTN_OTU4	OTU4	17	QSFP28	Support
	OTU 2	1 to 10	SFP+	
OTU4	OTU4	17 and 18	QSFP28	Support

Note

- QSFP+ is a 40GE optical module that uses optical fiber with an LC (Little Connector) interface.
- QSFP+ PSM 4 is a 4 × 10GE optical module that uses optical fiber with MPO (Multiple-Fiber Push-On) interface.
- QSFP+ PSM 4 fan-out means that when the QSFP+ PSM 4 optical module uses MPO-LC branch fiber, 1 MPO interface fiber is converted into 4 dual-fiber LC interface fibers to connect 4 SFP+ optical modules.
- ODUk cross-connect type supports client side to line side and line side to line side.

4.1.2. OTN Services

OTN services are transmitted as services in WDM networks, supporting single wavelengths with high bandwidths of 10 Gbit/s, 40 Gbit/s and 100 Gbit/s, and then multiplexed through WDM networks to fully utilize optical fiber resources.

OTN rate characteristics

The equipment complies with the OTN bit rate and tolerance range specified in G.709 . In OTN, the OPUk frame is designed to accommodate STM N frames or multiple low -rate ODUi (i<k) frames, especially for the characteristics of SDH. For example, OPU 1 and OPU 2 correspond to STM- 16 (or 2.5G) and STM- 64 (or 10G), respectively. OTU is processed on the basis of OPU, so the rate is also related to STM N.

OTN uses fixed-length variable-frequency transmission to control the rate and capacity by changing the transmission frequency.

- In terms of frame length:
  - One OTU frame is fixed to 4080 columns × 4 rows, which converts to 255 × 16 × 4 .

- The payload portion of an OPU frame is 3824 columns (i.e., 4080 columns minus 256 columns occupied by FEC) minus 16 columns of overhead bytes, multiplied by 4 rows, i.e., (3824 - 16) × 4 , which converts to 238 × 16 × 4 .

- In terms of frequency:
  - The OTU 1 /ODU 1 / OPU 1 frequency is 48.971 us.
  - Frequency of OTU 2 /ODU 2 / OPU 2 is 12.191 us.
  - OTU 3 /ODU 3 / OPU 3 is 3.035 us .
  - Frequency of OTU4 /ODU 4 / OPU 4 is 1.168 us.

OTN Rate List

OTN rates comply with the G.709 standard , and the specific values are shown in Table 3-3, Table 3-4, and Table 3-5 . The tolerance of all rates in the table is ± 20 ppm .

Table 3-3 OTUk rate

OTUk	Nominal rate	Approximate value of nominal rate	Rate Abbreviation
OTU 1	255 / 238 × 2488320 kbit/s	2666057 . 143 kbit/s	2.5 G
OTU 2	255 / 237 × 9953280 kbit/s	10709225 . 316 kbit/s	10 G
OTU 3	255 / 236 × 39813120 kbit/s	43018413 . 559 kbit/s	40 G
OTU4	255 / 227 × 99532800 kbit/s	111809973 . 568 kbit/s	100 G

Table 3-4 ODUk rate

ODUk	Nominal rate	Approximate value of nominal rate	Rate Abbreviation
ODU 0	1244160 kbit/s	-	1.25 G
ODU 1	239 / 238 × 2488320 kbit/s	2498775 . 126 kbit/s	2.5 G
ODU 2	239 / 237 × 9953280 kbit/s	10037273 . 924 kbit/s	10 G
ODU 3	239 / 236 × 39813120 kbit/s	40319218 . 983 kbit/s	40 G
ODU 4	239 / 227 × 99532800 kbit/s	104794445815 kbit/s	100 G

Table 3-5 OPUk rate

OPUk	Nominal rate	Approximate value of nominal rate	Rate Abbreviation
OPU 0	238 / 239 × 1244160 kbit/s	1238954 . 310 kbit/s	1.25 G
OPU 1	2488320 kbit/s	2488320 kbit/s	2.5 G
OPU 2	238 / 237 × 9953280 kbit/s	9995276 . 962 kbit/s	10 G
OPU 3	238 / 236 × 39813120 kbit/s	40150519 . 322 kbit/s	40 G

OPU 4	238 / 227 × 99532800 kbit/s	104355975330 kbit/s	100 G

OTN rate calculation method

Tips

The simple algorithm for OTN rate is as follows: when k takes the value of 1 , 2 , or 3 , the corresponding STM N is STM- 16 , STM-64 , or STM- 256 .

- OTUk: 255 /(239 -k)×STM N. " 255 /(239 -k)" represents the ratio of "number of bytes after FEC check" to "number of bytes before FEC check".
- ODUk: 239 /(239 -k) × STM N. " 239 /(239 -k)" represents the ratio of "ODUk byte number" to "OPUk payload excluding padding bytes". ODU0 cannot be calculated using the above formula. The ODU0 rate is half of STM-16 .
- OPUk: 238 /(239 -k) × STM N. " 238 /(239 -k)" represents the ratio of "OPUk payload" to "OPUk payload without padding bytes". OPU0 can also be calculated using the above formula, but " 238 /(239 - 0)" represents the ratio of OPU0 payload to the number of ODU0 bytes.

Taking OTU 2 as an example, the formula for calculating the rate is as follows.

- First, calculate the rate of OPU 2 : OPU 2 includes 16 columns of fixed stuffing bytes (cannot transmit services), so to meet the STM- 64 rate, "OPU 2 rate × ((238 × 16 × 4) - (16 × 4)) / (238 × 16 × 4) = STM- 64 rate". Through the equation conversion, the OPU 2 rate can be converted to "OPU 2 rate = STM- 64 rate / (((238 × 16 × 4) - (16 × 4)) / (238 × 16 × 4))", which is 238 / 237 times the STM- 64 rate.
- Then calculate the rate of OTU 2 : As mentioned above, " 1 OTU frame is fixed at 4080 columns × 4 rows, which is converted to 255 × 16 × 4 ", and 1 OTU frame relative to the OPU frame "OTU rate × ((238 × 16 × 4) - (16 × 4)) / (255 × 16 × 4)" should be equal to the STM- 64 rate, that is, 255 / 237 times the STM- 64 rate.

Note

The rate calculations for other OTUks are similar. It should be noted that OPU 1 is equal to the rate of STM-16 , i.e., there is no padding byte; the fixed padding byte of OPU 3 is 32 columns.

Uplink service type and rate

- OTU1 : The first -order optical channel transmission unit rate, OTU 1 rate is (255 / 238 × 2488320 kbit/s≈2666057.143kbit/s,

or 2.5 Gbit/s). OTU 1 can be used as a service layer to carry low-rate multiplexed services, or as a higher-level client layer service for further multiplexing .

- OTU2 : The second -order optical channel transmission unit rate, OTU 2 rate is (255 / 237 × 9953280 kbit/s≈10709225.316 kbit/s, or 10 Gbit/s). OTU 2 can be used as a service layer to carry low-rate multiplexed services, or as a higher-level client layer service for further multiplexing.
- OTU4 : The rate of the 4th -order optical channel transmission unit is (255 / 227 × 99532800 kbit/s≈ 111809973.568 kbit /s, or 100 Gbit/s). OTU4 can be used as a service layer to carry low-rate multiplexed services.

Access service type and encapsulation

The client side of the OTN board supports access services that are lower than the capacity of OTU4. These low-speed services are mapped to the ODU interface and multiplexed into OTU4 on the line side through cross-connection .

- 100GE services are mapped to ODUflex or OPU 4 through GFP-F (Frame mappedGEneric Framing Procedure) .
- 100GE services are mapped to OPU 4 through GMP (Generic Mapping Procedure) .
- 40GE services are mapped to ODUflex or OPU 3 through GFP-F .
- 40GE services are mapped to OPU 3 through GMP .
- 10GE services are mapped to OPU 2 or ODUflex through GFP-F.
- 10GE services are mapped to OPU 2 e through the Bit-synchronous Mapping Procedure (BMP) .
- STM- 64 services are mapped to OPU 2 through AMP (Asynchronous Mapping Procedure) or BMP .
- 16G FC services are mapped to ODUflex through BMP.
- 10G FC services are mapped to OPU 2 e through GFP-F.
- 8G FC services are mapped to OPU 2 through GMP .

Tributary slot type

OTUk supports multiplexing functions, for example, OPU2 in OTU2 channel supports division into OPU tributary time slots, multiple

OPU tributary timeslot multiplexing transmission.

"1G25" refers to a 1.25G tributary slot. The rate of each OPU2 tributary slot is approximately 1.25 Gbit/s. The OTU1/OTU2/OTU4

respectively support 2/8/80 tributary slots. For instance, a GE service occupies one 1.25G tributary slot. The 18M2C2 supports the 1.25G tributary slot mode.

Maintenance signal

The OTN network specifies the maintenance signal function for diagnosis. The device automatically inserts the maintenance signal when sending a fault. The device also supports manual configuration to insert the maintenance signal to diagnose whether the service has a fault or to check the link status when a fault occurs.

Common maintenance signal types and the message conditions after the maintenance signal is inserted are described as follows.

- OTUk_AIS: OTUk AIS (Alarm Indication Signal), OTN frame is filled with PN-11 code. After the path sink detects the AIS signal, it can be inferred that a fault has occurred upstream and the service is unavailable.
- ODUk_AIS: ODUk AIS, ODUk signal is all " 1 ", and STAT overhead information is " 111 ".
- ODUk_OCI: ODUk OCI (Open Connection Indication), ODUk signal (default) repeats the " 01100110 " format. When the STAT overhead information is " 110 ", it is fixed to indicate the OCI signal. After the trail sink detects the OCI signal, it can be inferred that the upstream signal is not connected to the trail source.
- ODUk_LCK: ODUk LCK (Locked Defect), ODUk signal (default) repeats the " 01010101 " format. When the STAT overhead information is " 101 ", it is fixed to indicate the LCK signal. The LCK signal is used to indicate that the upstream connection is "locked" and no signal is passing.

OTN signal processing

- From the client side:
  - The services accessed by the client are mapped to the client-side ODUk, which is cross-connected with the line-side ODUk. The line-side ODUk is multiplexed into OTU4 and converted into optical signals for transmission through the line-side interface.
- From the line side:
  - The line-side interface converts the service into an electrical signal and completes the demultiplexing process from OTU4 to ODUk, and then cross-connects with the ODUk on the client side or line side.
  - In the case where the ODUk on the client side is cross-connected with the line side, the ODUk on the client side

transmits services from the client side interface through a mapping relationship.

- In the case of cross-connection between the line-side ODUk, the line-side ODUk is transmitted through the other line-side ODUk and does not need to be landed through the equipment.

Note

This function is usually used to troubleshoot the situation where a loop is formed by self-crossing.

4.1.3. OTN Overhead

Applicable to SM, PM, TCM three-level overhead functions

The SM, PM, and TCM layers of the device provide the following overhead functions respectively. Their principles and processing methods are the same, but the functions are implemented in their respective layers.

- The monitoring functions include SAPI (Source Access Point Identifier), DAPI (Destination Access Point Identifier), and user-defined monitoring (Operator specific).
- SAPI, DAPI, and user-defined monitoring functions TTI (Trail Trace Identifier). TTI supports configuration and viewing in the form of hexadecimal numbers or text.
  - TTI is a string of 64 bytes, which is transmitted four times in one OTUk multiframe (64 bytes each time, with each byte in one base frame).
  - The TTI header of SAPI and DAPI is fixed to 0x00 (00 in hexadecimal display and space in text display), and is subsequently divided into two parts for configuration: the first part is 3 bytes, namely IS (International Segment); the second part is 12 bytes, namely NS (National Segment).
  - The TTI for user-defined monitoring (Operator specific) is 1 part, totaling 32 bytes.
  - NS , IS and user-defined monitoring bytes: if a byte is missing, it is supplemented with 0x00 (in hexadecimal display) or a space (in text display); however, in text configuration, the input space corresponds to the hexadecimal number 0x20 .
- BIP-8 (Bit Interleaved Parity - 8) monitoring function parameters. BIP-8 is calculated as follows.
  - The frame signal is divided into blocks of 8 bits .
  - The blocks are arranged in a rectangular shape.

- Compute the sum of 1s and 0s in each column .
- If the sum is odd, the corresponding BIP- 8 bit is filled with 1 .
- If the sum is even, the corresponding BIP- 8 bit is filled with 0 .

- BEI (Backward Error Indication) monitoring function parameters. A BEI overhead information indicates one of the following functions.
  - Indicates the number of BIP- 8 errors.
  - An incoming alignment error (IAE) occurs.
  - BIP- 8 is error-free and no BIAE (Backward Incoming Alignment Error) occurs.
- Subsequent response function for TIM (Trace Identification Mismatch) alarm. The value of "Actual TTI" needs to be the same as the value of "Receivable TTI". If the SAPI, DAPI and/or user-defined overhead fields are configured for monitoring, a TIM alarm of the corresponding level will begenerated when the corresponding TTI overhead fields are detected to be different. After a TIM alarm isgenerated, the processing method is as follows according to the enabling/disabling of the TIM subsequent response function.
  - Enable TIM subsequent response: insert the corresponding layer of AIS and send the corresponding layer of BDI (Backward Defect Indication) back to the peer end.
  - Disable TIM subsequent response: No subsequent processing is performed.

Note

- The high-order ODUk interfaces on the line side and the client side, as well as the Client-ODUk interface corresponding to the non-OTN service on the client side, support the configuration of PM related functions.
- The low-order ODUk interface on the line side and the client side transparently transmits PM information.

Applicable to PM and TCM two-level overhead functions

The PM and TCM layers of the equipment provide the following costs and functions respectively. Their principles and processing methods are the same, but the functions are implemented in their respective layers.

- Non-intrusive monitoring function: configure whether to monitor the PM or TCM overhead, that is, when configuring ODUk SNCP (Subnetwork Connection Protection) of SNC/N monitoring mode, configure the monitored overhead to be PM or TCM.

- When enabled: monitor the PM or TCM overhead. This monitoring is non-intrusive, that is, it will not affect the service signal. After the problem is detected, subsequent functions such as alarmgeneration and protection switching can be realized.
- When prohibited: No monitoring is performed and the signal is transparently transmitted.

Applicable only to PM level overhead functions

- Display the received STAT (Status) overhead: PM STAT has 3 bits in total and is used to indicate the PM signal type. Its values are as follows.
  - 001 : Normal channel signal.
  - 101 : ODUk-LCK maintenance signal.
  - 110 : ODUk-OCI maintenance signal.
  - 111 : ODUk-AIS maintenance signal.
  - remaining four values are reserved.

Applicable only to TCM-level overhead functions

- Configure TCM source and sink modes and functions: The two ends of the series connection act as the source (TCM inbound direction) and sink (TCM outbound direction) to each other. When it is necessary to process the overhead at the TCM source or monitor at the sink, the mode and function need to be configured. Transparent transmission: The source does not generate TCM overhead; the sink transparently transmits TCM overhead.
  - Operation: The source end generates TCM overhead; the sink end monitors the TCM overhead. When a fault is detected, it reports BDI to the source end and inserts AIS at the same time.
  - Monitoring: Applicable only to the sink end. The sink end monitors the TCM overhead and reports the BDI to the source end when a fault is detected.
  - Enable: The source and sink support enabling the TCM function separately. After enabling, the processing is performed according to the respective modes of the source and sink.
  - Disable: The source and sink support disabling the TCM function separately. After disabling, the source and sink are processed according to their respective transparent transmission modes.

- Display the received STAT (Status) overhead: TCM STAT has 3 bits in total, which are used to indicate the TCM signal type, whether the TC-CMEP (Tandem Connection-Connection Monitoring End Point) exists at the source end, and whether there is IAE at the source end. Its values are as follows.
  - 000 : Passive series connection.
  - 001 : Normal series connection signal and no IAE at the source end.
  - 010 : Series connection signal, IAE at the source. When IAE occurs at the source of the series connection, the sink knows the fault through the STAT overhead of " 010 ", and can stop calculating the error bits at the sink.
  - 101 : ODUk-LCK maintenance signal.
  - 110 : ODUk-OCI maintenance signal.
  - 111 : ODUk-AIS maintenance signal.
  - The other two values are reserved.
- Subsequent response function for LTC (Loss of Tandem Connection) alarm. When the STAT monitoring function is enabled and the STAT value is " 000 ", it indicates that the tandem connection is unavailable and the ODUk_TCMi_LTC alarm is generated. After the ODUk_TCMi_LTC alarm is generated, the processing method is as follows according to the enabling/disabling of the LTC subsequent response function.
  - Enable LTC subsequent response: insert AIS and send ODUk TCMi BDI back to the other end.
  - Prohibit LTC Subsequent Response: No subsequent processing.

GCC Overhead

The OTUk overhead provides 2 bytes of GCC0 (general Communications Channel) overhead, which is used as the communication channel for network management and other information between OTUk overhead termination points.

The ODUk overhead provides GCC1 and GCC2 overhead channels , each of which occupies 2 bytes.

The GCC2 channel is used for communication between two network elements that process the ODUk frame structure (for example, 3R regeneration nodes).

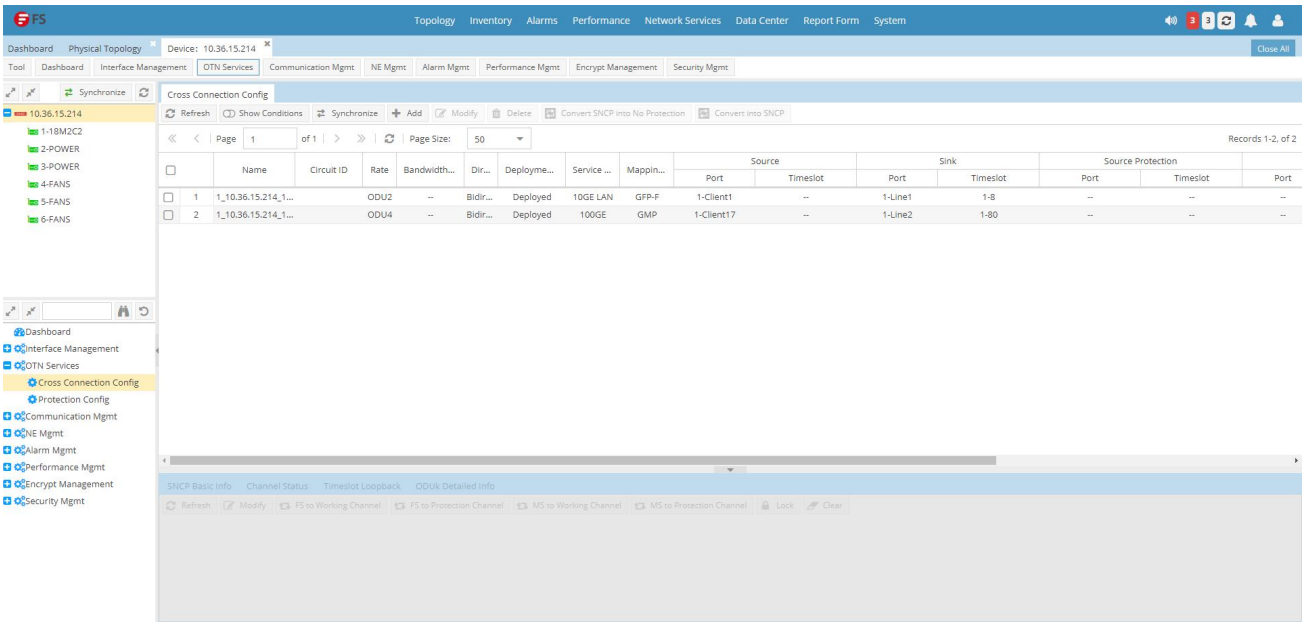
4.2. Configuring OTN Services

4.2.1. Configuring ODUk Services

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [OTN Service/Cross-link Configuration]. The interface is as shown below.

Step 2 Click <Add> and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.



Parameter	Value	Note
Name	0 ～ 50 Characters	Configure the cross-name.
Circuit Number	0 ～ 100 Characters	Configure cross-connect circuit number information. This information is only saved in the network management system and will not be sent to the device.
Founder	0 ～ 100 Characters	Configure the cross connection creator information. This information is only saved in the network management system and will not be sent to the device.

Rate	• ODU0 • ODU1 • ODU2 • ODUflex • ODU2e • ODU3 • ODU4	Configure the crossover rate. The default is ODU0 .
SNCP Protecting location	• No protection • Source Protection • Sink protection • Source and sink dual protection	Configuring SNCP Protection function. • No protection: No SNCP Protection function. • Source protection: 2 source ports, 1 Sink ports form SNCP Protection function. • Sink protection: 2 sink ports and 1 source port form the SNCP protection function. • Source and sink dual protection: 2 source ports, 2 Each sink port forms the SNCP protection function. The default is no protection.
Cross direction	• Unidirectional • Bidirectional	Configure the crossover direction. • Bidirectional cross-connection support conversion to SNCP cross. • The source of a bidirectional crossover cannot be used as the source of other bidirectional crossovers, but can be used as the source of other unidirectional crossovers. The sink of a bidirectional crossover cannot be used as the sink of other common crossovers, but can be used as the sink of SNCP. Cross lodging. • The source of a unidirectional cross can be used as the source of other crosses, but the sink of a unidirectional cross cannot be used as the sink of other crosses . The default is bidirectional.
Source Port	-	Click < ▪▪▪ > Select the port of the source end .
Sink Port	-	Click < ▪▪▪ > Select the sink port .

Source port service type	• STM- 64 • 10GE LAN • OTU2(e) • OTU2E • FC800 • FC1200 • FC1600 • FC3200 • OTU4 • 40GE • 100GE	Configure the service type. Depending on the current business model, only relevant business types can be selected .
Sink port service type	• STM- 64 • 10GE LAN • OTU2(e) • OTU2E • FC800 • FC1200 • FC1600 • FC3200 • OTU4 • 40GE • 100GE	Configure the mapping mode. Depending on the selected service type, only relevant mapping modes can be selected .
Source port mapping mode	• AMP • BMP • GFP- F • GMP • ODU- >OTU	Configure the mapping mode. Depending on the selected service type, only relevant mapping modes can be selected .
Sink port mapping mode	• AMP • BMP • GFP- F • GMP • ODU- >OTU	Configure the mapping mode. Depending on the selected service type, only relevant mapping modes can be selected .
Source time slot	-	Click < ▪▪▪ > Configure the port timeslot occupied by the source end .
Sink Time Slot	-	Click < ▪▪▪ > Configure the port timeslot occupied by the sink .

Protecting source ports	-	Click < ▪▪▪ > Select the port of the source end . Applicable to SNCP Source protection and source-destination dual protection.
Protecting the sink port	-	Click < ▪▪▪ > Select the sink port . Applicable to SNCP Destination protection and source-destination dual protection.
Protection source time slot	-	Click <▪▪▪ > Configure the port timeslot occupied by the source end of the protection channel . Applicable to SNCP Source protection and source-destination dual protection.
Guard Sink Slot	-	Click <▪▪▪ > Configure the port timeslot occupied by the host end of the protection channel . Applicable to SNCP Destination protection and source-destination dual protection.

Note

Depending on the selected board and device, interface parameters only support the values that are actually supported by the configuration.

Related operations

Operation	Function Entry	Note
View port information	OTN on the top of the interface. Business records , click the " ODUk Details" tab at the bottom of the interface	View information related to cross-connect ODUk, including port name, service type, mapping method, ODUk name, and time slot number.
Quick View and Configuration of SNCP Protection Groups	OTN on the top of the interface. Business records , click the " SNCP Basic Information" tab at the bottom of the interface	• View SNCP Protection group information. • Click the record and click <Modify> to configure SNCP Protection group, parameters are shown in Table 3 - 7. • Click < Forced Switch to Protection > , < Forced Switch to Work > , < Manual Switch to Protection > , < Manual Switch to Work > , <Lock> , or <Clear> to configure the switching operation .
Quick Status Check of Channels	OTN on the top of the interface. Business records , click the "Channel Status" tab at the bottom of the interface	Check the status information of the protection group channel. The parameters are shown in Table 3 - 8.
Quick Configuration of Timeslot Loopback	OTN on the top of the interface. Business Records , click the "Time Slot Loopback" tab at the bottom of the interface	Click the record and click <Modify> to configure the loopback function. The parameters are as shown in Table 3 - 6 .

Table 3 - 6 -Slot loopback configuration parameters

Parameter	Value	Note
Port Number	-	Display the port number.
Loopback mode	• No loopback • Inner Ring • Outer Ring • Bidirectional loopback	Configure the loopback function of the cross-connect source timeslot. • No loopback: Disable the loopback function. • Inner loop: loops back to the other end's time slot. • External loop: loops back to the interface. • Bidirectional loopback: Performs inner loopback and outer loopback simultaneously. The default is no loopback.
Holding time (minutes)	• 0 • 1 to 65535 , measured in minutes	Configure the loopback time of the cross-connect source timeslot. • 0 : After executing loopback, you need to manually disable loopback. • 1 to 65535 : After waiting for this time, loopback is automatically disabled . The default is 0 .

4.2.2. Configuring SNCP Function

For the created OTN services, you can configure or cancel the SNCP protection function.

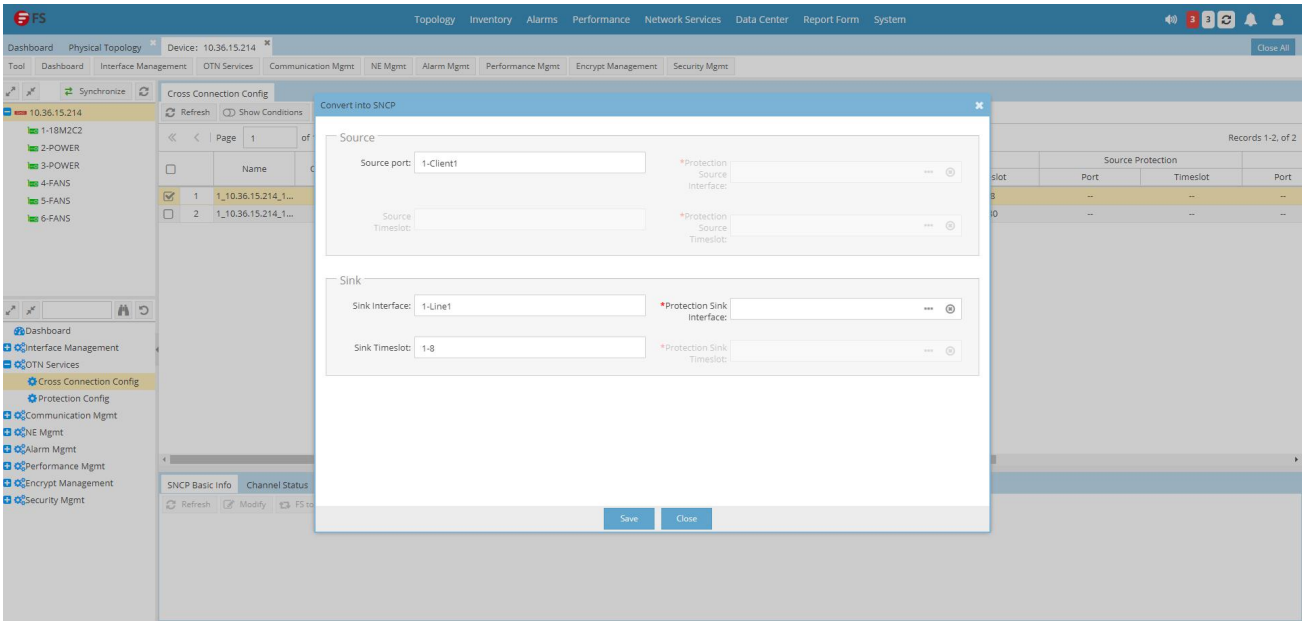
- For OTN services that are not configured with SNCP, you can configure SNCP protection functions by creating SNCP protection cross-connections and establishing protection groups.
- For OTN services that have been configured with SNCP, you can configure and delete the SNCP protection cross-connection and the protection group to cancel the SNCP protection function.

Configure ODUk SNCP Protection Function

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [OTN Service/Cross-link Configuration].

Step 2 Click the ODUk service record that is not configured with SNCP at the top of the interface, and click <Convert to SNCP>. The interface is shown in the figure below and the parameters are shown in the table below.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.



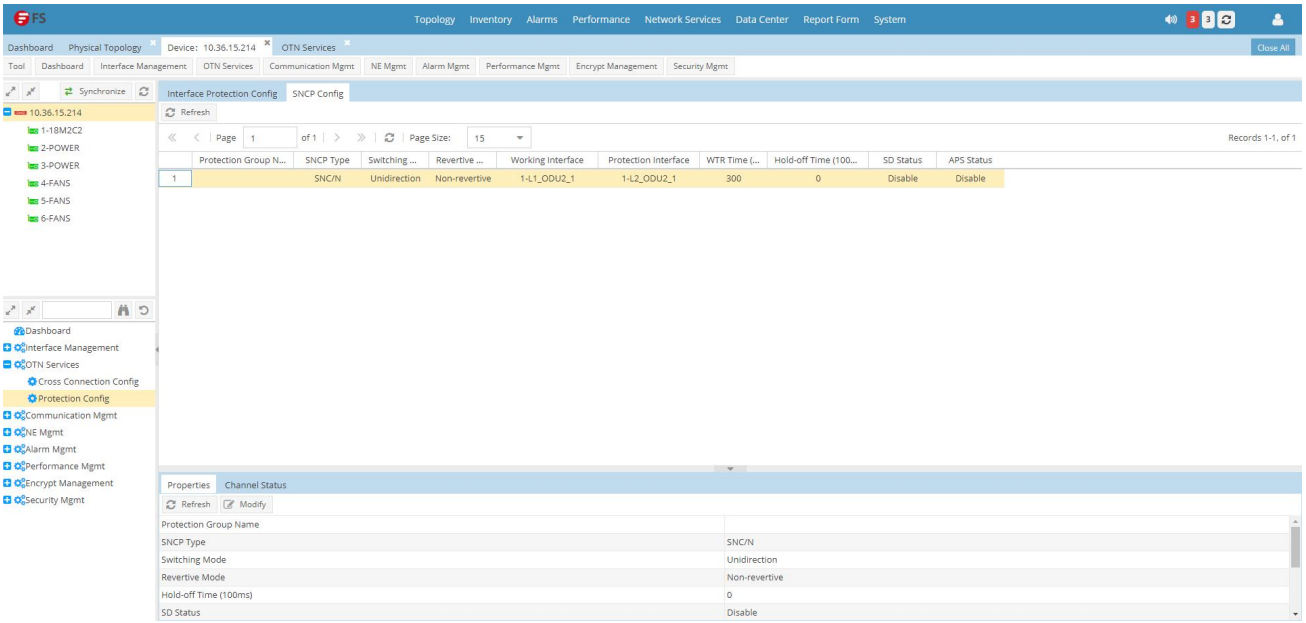
Parameter	Value	Note
Source Port	-	Display ODUk Port of the service source.
Protecting source ports	-	Click < ▪▪▪ > Select the protection port of the source end .
Source time slot	-	Display source port ODUk Business time slot.
Protection source time slot	-	Click < ▪▪▪ > Select the time slot of the protection port at the source end .
Sink Port	-	Display ODUk Service sink port.
Protecting the sink port	-	Click < ▪▪▪ > Select the protection port of the sink .
Sink Time Slot	-	Display sink port ODUk Business time slot.
Guard Sink Slot	-	Click < ▪▪▪ > Select the time slot of the protection port of the sink .
Source Protection	-	SNCP with the same sink timeslot Protection group.
Sink protection	-	SNCP with the same source timeslot Protection group.
Source and sink dual protection	-	Create four SNCP protection groups with identical working/protection source timeslots and identical working/protection destination timeslots. This dual protection is also known as an 8-character cross-connection.

Modify SNCP Protection Groups

When configuring the SNCP protection function, the system creates SNCP protection groups using default parameters, which can be subsequently modified to align with network planning.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [OTN Service/Protection Configuration].

Step 2 Click the SNCP Protection Configuration tab at the top of the interface, click the SNCP protection group record, and the relevant information is displayed at the bottom of the interface, as shown in the following figure.



Step 3 Click the "Properties" tab at the bottom of the interface and click <Modify>. The parameters are shown in the following table.

Parameter	Value	Note
Protection group name	1 ～ 200 Characters	Configure the SNCP protection group name. The default is empty, indicating no configuration name.
SNCP type	• SNC/I • SNC/N • SNC/S	Configure the monitoring type of SNCP protection. The default is SNC/I.
Switching mode	• Unidirectional • Bidirectional	Configure the protection switching working mode. The default is unidirectional.
Return method	• Return • Non-return	Configure the protection switching return mode. The default is non-return mode.
WTR (seconds)	0 ~ 720	Configure the return wait time in seconds. This parameter is only supported when the return mode is "Return". The default is 300.
HoldOff time (100 ms)	0 ～ 100	Configure the protection switching delay time in 100 milliseconds. The default value is 0, which means immediate switching.

SD Enable	• Enable • Prohibit	Configure the SD (Signal Degrade) function to trigger the protection switching function. The default is disabled.
APS Enable	• Enable • Prohibit	Configuring APS Protocol function. The default is disabled.
Operational Status	• Clear • Locking • Forced switching to protection • Forced switch to work • Manual switching to protection • Manual switching to work	Display the protection group operation status.
Working port	-	Display the working channel port of the protection group.
Protect Port	-	Display the protection channel ports of the protection group.
Current working port	-	Display the port where the OTN service is currently located.

Step 4 Click the "Channel Status" tab at the bottom of the interface to view the status information of the protection group channel. The parameters are shown in the following table.

Table 3 - 8 Configuration parameters

Parameter	Value	Note
Channel	• Working channel • Protection channel	Display the channel type.
Source Port	-	Display the source port.
Source time slot	-	Display the source time slot.
Source ODUk	-	Display the source ODUk .
Sink Port	-	Display the sink port.
Sink Time Slot	-	Display the sink time slot.
Sink ODUk	-	Display the sink ODUk .

Channel Status	• Clear • Locking • Protection channel signal failure • Forced switching to protection • Forced switch to work • Signal failure • SF Switching • SD Switching • Manual switch to protection • Manual switch to work • Waiting for reply • Practice switching • Request return • Do Not Return	Display channel status information.
Working status	• Work • Wait	Display the working status of the channel. • Work: Business is transmitted in this channel. • Waiting: The service is not transmitted in this channel.

Configure SNCP protection group switching operations

SNCP protection groups support configuration of manual switching and other operations to meet network planning or test protection switching functions.

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [OTN Service/Protection Configuration].

Step 2 Click the SNCP Protection Configuration tab at the top of the interface, right-click the SNCP protection group record, and click [Forced Switch to Working], [Forced Switch to Protection], [Manual Switch to Working], [Manual Switch to Protection], [Lock], or [Clear].

Disable SNCP protection function

After conversion to unprotected service, the cross-connection of the working channel is restored to normal cross-connection, and the service loses the SNCP protection function.

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [OTN Service/Cross-link Configuration].

Step 2 Click the OTN service record that has been configured with SNCP at the top of the interface, and click <Change to No Protection from SNCP> to display a pop-up prompt.

Step 3 Click Yes to deliver the configuration.

4.2.3. Configuring OCh 1+1 Protection and Client-side Port Protection

The device supports unidirectional OCh 1 + 1 protection and client-side interface 1 + 1 protection.

- One-way OCh 1 + 1 protection: Protection switching does not use the APS protocol. OCh 1 + 1 protection is supported between Line 1 and Line 2 interfaces on the line side .
- After configuring OCh protection, when establishing cross-connection, you only need to establish cross-connection between the client-side ODUk and the line-side ODUk of the working channel, and the device will automatically establish the corresponding cross-connection of the protection channel.
- Client-side interface 1 + 1 protection: Protection switching does not use the APS protocol. The client-side interface supports OCh 1 + 1 protection when accessing OTU 2 and OTU4 services .

Notice

- When deleting a protection group, if the working channel has failed, the loss of protection function may cause business interruption. Please use it with caution according to the actual situation.
- After executing the external command of forced switching or manual switching, the device cannot automatically perform protection switching. Please clear the external command in time according to the situation.
- Because protection switching operations have priorities, only the currently applicable operations can be configured.
- Before creating a protection group, the protection interface must not have a cross-connection configured.

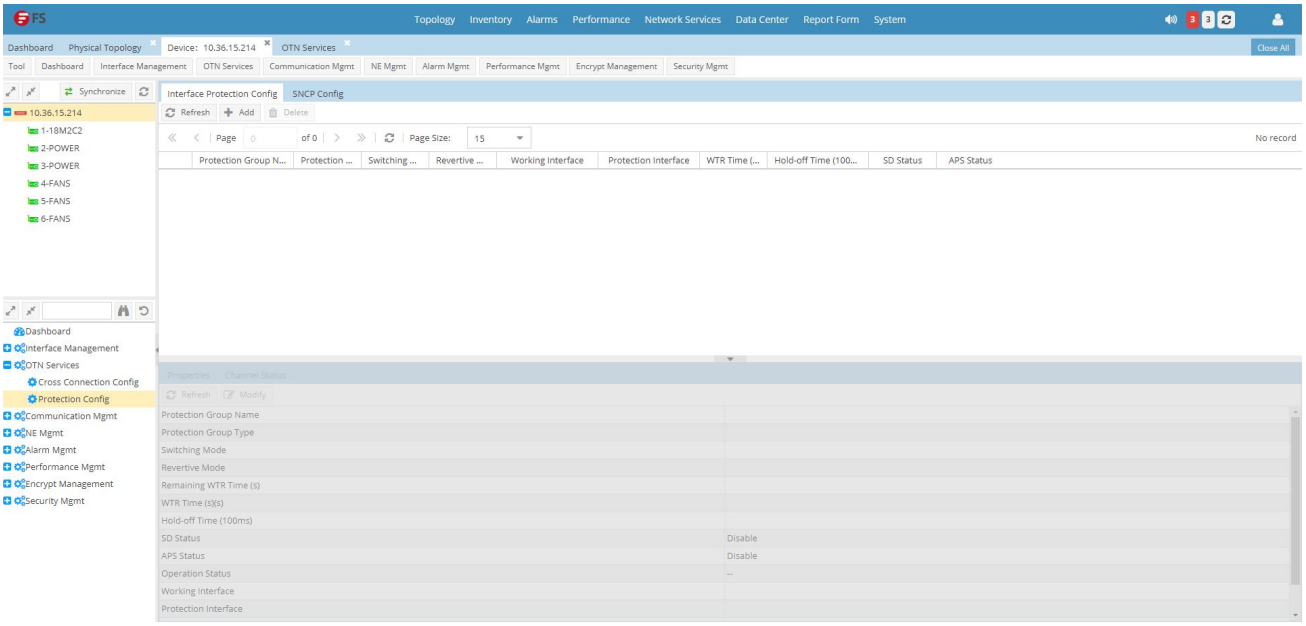
Create a Protection Group

1 + 1 protection and client-side port protection is completed , providing protection functions.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [OTN Service/Protection Configuration]. The interface is shown in the figure below.

Step 2 Click the Port Protection Configuration tab, click <Add>, and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.



Parameter	Value	Note
Protection group name	1 ～ 200 Characters	Configure the protection group name.
Protection group type	Channel 1 + 1	Display the protection group type, which is fixed as "Channel 1 + 1 ".
Working port	-	Configure the working channel port of the selected protection group.
Protect Port	-	Configure the protection channel port of the selected protection group.
Switching mode	Unidirectional	Display the switching mode, which is fixed as unidirectional.
Return method	• Non-return • Return	Configure the return mode of the protection group. The default is non-return mode.
WTR Time (Second)	0 ~ 720	Configure the return wait time in seconds. This parameter is only supported when the return mode is "Return" . The default is 300 .

HoldOff time (100 ms)	0 ～ 100	Configure Hold Off Timer Timer, measured in 100 milliseconds . The default is 0 .
APS Enable	Prohibit	APS is enabled for the protection group. Protocol, fixed to prohibited.

Configure protection groups

Configuring a protection group mainly includes viewing, modifying, and deleting a protection group.

Notice

When deleting a protection group, if the working channel has failed, the loss of protection function may cause business interruption. Please use it with caution according to the actual situation.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [OTN Service/Protection Configuration].

Step 2 Click the Port Protection Configuration tab. At the top of the configuration interface on the right, click the protection group record. Select a tab at the bottom of the interface to view the record.

- Click the Properties tab to view the protection group information. The parameters are shown in Table 3 - 9. Click <Modify> to modify the protection group parameters. After the modification is complete, click <Save> to deliver the configuration.
- Click the Channel Status tab to view the status of the working channel and protection channel. The parameters are listed in Table 3 - 10 .

Step 3 (Optional) Click a protection group record and click <Delete>. A confirmation prompt pops up and click <Yes> to delete the protection group.

Table 3-9 Protection group attributes

Parameter	Value	Note
Protection group name	1 ～ 200 Characters	Configure the protection group name.
Protection group type	Channel 1 + 1	Display the protection group type, which is fixed as "Channel 1 + 1 ".
Switching mode	unidirectional	Display the switching mode, which is fixed as unidirectional.
Return method	• Non-return • Return	Configure the return mode of the protection group. The default is non-return mode.

WTR Time (seconds)	0 ~ 720	Configure the return wait time in seconds. This parameter is only supported when the return mode is "Return" . The default is 300 .
WTR Time Left (Second)	1 ~ 720	Display WTR time left. WTR before returning. Status ends. This parameter displays the remaining time before the WTR status ends.
HoldOff Time (100 ms)	0 ～ 100	Configuring Hold Off Timer Timer, unit is 100 millisecond. The default is 0 .
SD Enable	• Enable • Prohibit	Configure SD (Signal Degrade (signal quality decreases) triggers the protection switching function. The default is disabled.
APS Enable	Prohibit	APS is enabled for the protection group. Protocol, fixed to prohibited.
Operational Status	• Clear • Locking • Forced switching to protection • Forced switch to work • Manual switching to protection • Manual switching to work	Display the protection group operation status.
Working port	-	Configure the working channel port of the selected protection group.
Protect Port	-	Configure the protection channel port of the selected protection group.
Current working port	-	Display the port where the service is currently located.

Table 3 - 10 Channel Status

Parameter	Value	Note
Channel	• Working channel • Protection channel	Display the channel type.
port	-	Display the interface information of a channel.

Channel Status	• Clear • Locking • Protection channel signal failure • Forced switching to protection • Forced switch to work • Signal failure • SF Switching • SD Switching • Manual switch to protection • Manual switch to work • Waiting for reply • Practice switching • Request return • Do Not Return	Display channel status information.
Working status	• Work • Wait	Display the working status of the channel. • Work: The service is transmitted in this channel . • Wait: The service is not transmitted in this channel.

Configuring Switchover Operations

Notice

After executing the external command of forced switching or manual switching, the device cannot automatically perform protection switching. Please clear the external command in time according to the situation.

The protection group supports configuration of manual switching and other operations to meet network planning or test protection switching functions.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [OTN Service/Protection Configuration].

Step 2 Click the Port Protection Configuration tab at the top of the interface, right-click the protection group record, and click Forced Switch to Protection, Forced Switch to Working, Manual Switch to Protection, Manual Switch to Working, Lock, or Clear.

4.3. Configuration Overhead

The OTN network provides a rich set of overhead bytes to ensure and monitor network operation. Based on the characteristics of layered monitoring, the OTN electrical layer overhead is used to monitor the SM layer of OTUk, the PM layer and TCM layer of ODUk, and the OPUk overhead.

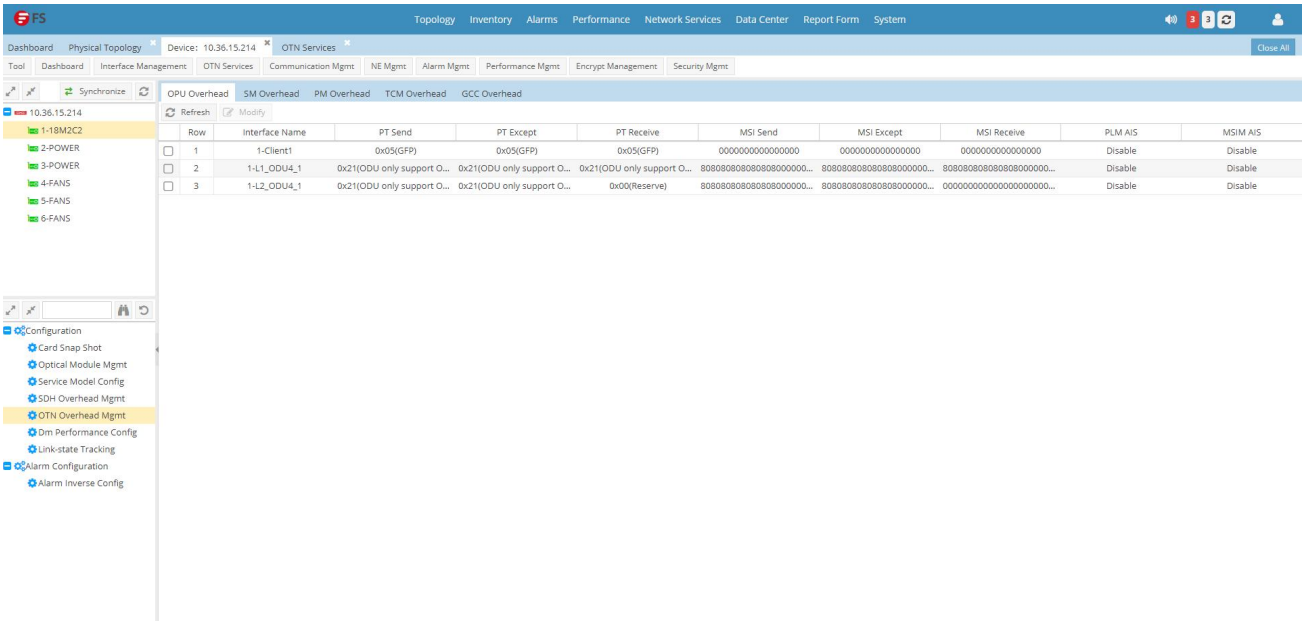
The OTN overhead function mainly configures the content, monitoring function, and monitoring threshold of the overhead bytes. It is suitable forGEnerating alarms and triggering protection switching when service quality degrades or is interrupted.

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [Configuration/OTN Overhead Management]. The interface is shown in the figure below.

Step 2 In the configuration interface on the right, the port records that support OTN overhead configuration are displayed by tab classification. Click to select a port record, and click <Modify> to open the configuration panel for configuration.

- Click the OPU Overhead tab to display the overhead records of the configured OTN service ports. The configuration parameters are shown in Table 3 - 11 .
- Click the SM Overhead tab to display the line-side port overhead record. The configuration parameters are shown in Table 3 - 12 .
- Click the PM Overhead tab to display the overhead records of the configured OTN service ports. The configuration parameters are shown in Table 3 - 14 .
- Click the TCM Overhead tab to display the overhead records of the configured OTN service ports. The configuration parameters are shown in Table 3 - 15 .
- Click the GCC Overhead tab to display the overhead records related to the line-side ports and ODUk ports configured with OTN services. The configuration parameters are shown in Table 3 - 16 .
- Click the GCC Channel Timeslot tab to view the GCC overhead records configured on the GCC Overhead tab.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.



Configure OPU Overhead

The main configuration functions of OPU overhead are as follows.

- first frame of the OPU's PSI (Payload Structure Identifier) multiframe structure , that is, PSI[0], and is used to indicate the payload type or composition structure of the OPUk signal.
- If PT is 0x20 or 0x21 , MSI (Multiplex Structure Identifier) is also supported. MSI is used to indicate the multiplex structure .
- PLM (Payload Mismatch) insert ODUk_AIS function: The values of "receivable PT" and "actual PT" should be the same. If they are different, the OPUk_PLM alarm will be reported. When reporting the alarm, if the PLM insert ODUk_AIS function is enabled, AIS will be inserted at the same time.
- MSIM (Multiplex Structure Identifier Mismatch) insert ODUk_AIS function: The values of "MSI to be received" and "MSI actually received" should be the same. If they are different, an OPUk_MSIM alarm will be reported. When reporting an alarm, if the MSIM insert ODUk_AIS function is enabled, AIS will be inserted at the same time.

Table 3-11 OPU Overhead Parameters

Parameter	Value	Note
Port Name	-	Display OPUk port.
Send PT	2 Hexadecimal number	Configure the PT to be sent Number, format is 16 Base.
PT receivable	2 Hexadecimal number	Configure the PT that should be received Number.
Received PT	2 Hexadecimal number	Display the actual received PT Number.
Send MSI	16 Hexadecimal number	The MSI that is sent .

MSI receivable	16 Hexadecimal number	the MSI that is sent .
MSI received	16 Hexadecimal number	Display the actual received MSI .
Insert ODUk_AIS in PLM	• Enable • Prohibit	Configure the ODUk_AIS function to be down-plugged when a PLM alarm is generated. The default is disabled.
Insert ODUk_AIS in MSIM	• Enable • Prohibit	Configure the ODUk_AIS function to be inserted when MSIM alarm is generated. This parameter is valid when "Receivable PT" is configured as "20" or "21". The default is disabled.

Configure SM Overhead

The main configuration contents of SM (Section Monitoring) overhead are as follows.

- SAPI, DAPI, and user-defined monitoring (Operator specific) monitoring functions.
- SAPI, DAPI, TTI of user-defined monitoring functions.
- BIP- 8 monitoring function parameters.
- BEI monitoring function parameters.
- Subsequent response function for TIM alarms.

Table 3-12 SM Overhead Parameters

Parameter	Value	Note
Port Name	-	Display OTUk port.
SAPI Detection	• Enable • Prohibit	Configuring SAPI Monitoring function. Disabled by default.
DAPI Detection	• Enable • Prohibit	Configuring DAPI Monitoring function. Disabled by default.
User-defined detection	• Enable • Prohibit	Configure user-defined monitoring function. Disabled by default.
TTI should be issued	-	Click < ▪▪▪ > Configuration SAPI , DAPI , USER (Operator specific , user-defined monitoring) sends TTI content.
TTI receivable	-	Click < ▪▪▪ > Configuration SAPI , DAPI , USER Should receive TTI content .
Received TTI	-	Click < ▪▪▪ > View SAPI , DAPI , USER Actual received TTI content .

FEC mode for OTUk	• GFEC • SD- FEC Mode1 • SD- FEC Mode2 • SD- FEC Mode3 • OFEC	Configuring FEC The optical module actually used may only support some modes .
BIP8 Error code threshold	• 1.0E - 3 • 1.0E - 4 • 1.0E - 5	Configure the threshold for BIP-8 overhead excursion in the SM (Section Monitoring). When the BIP-8 error rate exceeds this threshold, it signifies that the SM has detected a degradation in quality, triggering the OTUk_SM_BIP8_EXC error excursion alarm. A smaller threshold value indicates a stricter quality requirement. The default value is 1.0E-3.
BIP8 Error degradation threshold	• 1.0E - 6 • 1.0E - 7 • 1.0E - 8 • 1.0E - 9	Configure the degradation threshold for BIP-8 overhead in the SM. When the BIP-8 error rate exceeds this threshold, it indicates that the SM has detected quality degradation, and an error threshold crossing alarm, OTUk_SM_BIP8_DEG, is reported. A smaller value indicates a higher quality requirement. The default value is 1.0E-6.
BEI Error code threshold	• 1.0E - 3 • 1.0E - 4 • 1.0E - 5	Configure the excursion threshold for the SM overhead BEI. When the BEI error rate exceeds this threshold, it indicates that the SM has detected a quality degradation, prompting the reporting of the OTUk_SM_BEI_EXC error excursion alarm. A smaller threshold value implies a higher quality requirement. The default value is 1.0E-3.
BEI Error degradation threshold	• 1.0E - 6 • 1.0E - 7 • 1.0E - 8 • 1.0E - 9	Configure the degradation threshold for the SM overhead BEI. When the BEI error rate exceeds this threshold, it signifies that the SM has detected a quality deterioration, triggering the reporting of the OTUk_SM_BEI_DEG error threshold crossing alarm. A smaller threshold value indicates a stricter quality requirement. The default setting is 1.0E-6.
TIM Subsequent response enable	• Enable • Prohibit	Configure reporting of OTUk_SM_TIM Response function after alarm. The default setting is disabled.

Note

- The default value of the OTN overhead related to the service is displayed only after the OTN service is configured. If the OTN service is not configured, the default value of the OTN overhead related to the service is displayed as an invalid value.

- TTI configuration interface of SM, PM, and TCM is shown in Figure 3-1 and Figure 3-2 , and the TTI default value is shown in Table 3-13 .

Figure 3-1 TTI Configuration Interface Example - Hexadecimal

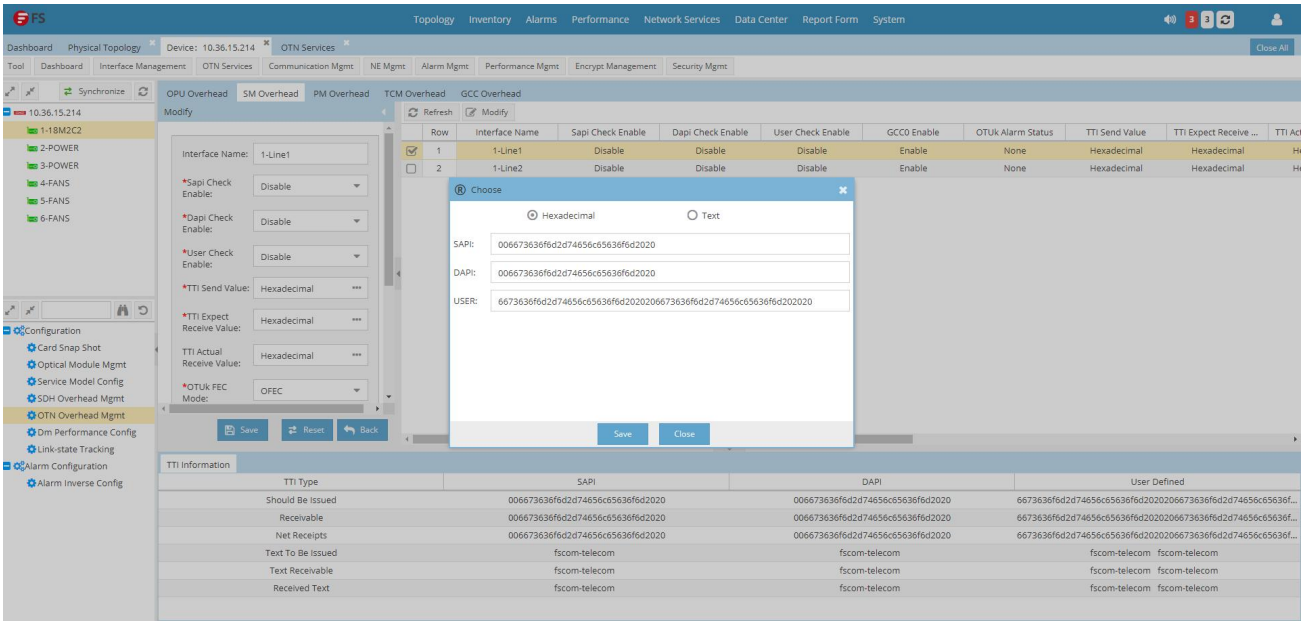


Figure 3-2 TTI Configuration Interface Example - Text

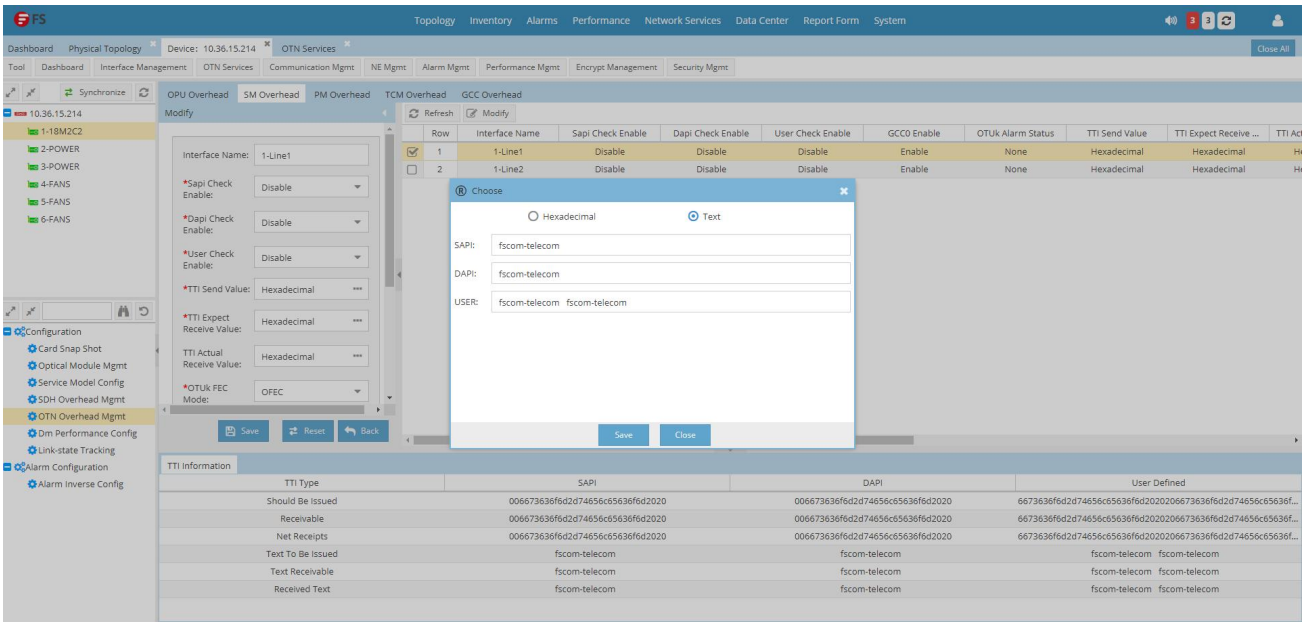


Table 3-13 Default conditions for transmitting TTI and receiving TTI

Overhead and Mode	Default Value	
SAPI , DAPI	fscom-telecom	fscom-telecom
16 Base	006673636f6d2d74656c65636f6d2020	006673636f6d2d74656c65636f6d2020

Text	fscom-telecom	fscom-telecom
User-defined monitoring (Operator specific ）		
16 Base	6673636f6d2d74656c65636f6d2020206673636f6d2d74656c65636f6d202020	
Text	[space] fscom-telecom [space][space][space] fscom-telecom [space][space]	

Note

- The first byte of SAPI, DAPI, and user-defined monitoring overhead is obtained by CRC check.
- If the hexadecimal number is outside the ASCII range, special characters may appear when displayed in text mode.

Configuring PM Cost

The main configuration contents of PM (Path Monitoring) overhead are as follows.

- SAPI, DAPI, and user-defined monitoring (Operator specific) monitoring functions.
- SAPI, DAPI, TTI of user-defined monitoring functions.
- BIP- 8 monitoring function parameters.
- BEI monitoring function parameters.
- Subsequent response function for TIM alarms.
- Non-intrusive monitoring capabilities.
- Display received STAT overhead.

Table 3 - 14 PM Overhead Parameters

Parameter	Value	Note
Port Name	-	Display ODUk port.
SAPI Detection	• Enable • Prohibit	Configuring SAPI Monitoring function. Disabled by default.
DAPI Detection	• Enable • Prohibit	Configuring DAPI Monitoring function. Disabled by default.
User-defined detection	• Enable • Prohibit	Configure user-defined monitoring function. Disabled by default.
TTI should be issued	-	Click < ▪▪▪ > Configuration SAPI , DAPI , USER （ Operator specific , user-defined monitoring) sends TTI content.

TTI receivable	-	Click < ▪▪▪ > Configuration SAPI , DAPI , USER The TTI content that should be received .
Received TTI	-	Click < ▪▪▪ > View SAPI , DAPI , USER The actual received TTI content .
BIP8 Error code threshold	• 1.0E - 3 • 1.0E - 4 • 1.0E - 5	Configure the excursion threshold for the TCMi overhead BIP-8. When the BIP-8 error rate exceeds this threshold, it indicates that the TCMi has detected a quality degradation, prompting the reporting of the ODUk_TCMi_BIP8_EXC error excursion alarm. A smaller threshold value signifies a higher quality requirement. The default value is 1.0E-3.
BIP8 Error degradation threshold	• 1.0E - 6 • 1.0E - 7 • 1.0E - 8 • 1.0E - 9	Configure the degradation threshold for the TCMi overhead BIP-8. When the BIP-8 error rate surpasses this threshold, it signifies that the TCMi has detected a quality deterioration, triggering the reporting of the ODUk_TCMi_BIP8_DEG error threshold crossing alarm. A smaller threshold value indicates a stricter quality requirement. The default setting is 1.0E-6.
BEI Error code threshold	• 1.0E - 3 • 1.0E - 4 • 1.0E - 5	Configuring PM Expenses BEI The crossing threshold. BEI When the bit error rate exceeds the threshold, it indicates PM When the quality is degraded, the error code limit alarm ODUk_PM_BEI_EXC is reported . The smaller the value, the higher the quality requirement . The default is 1.0E - 3 .
BEI Error degradation threshold	• 1.0E - 6 • 1.0E - 7 • 1.0E - 8 • 1.0E - 9	Configure the excursion threshold for the TCMi overhead BEI. When the BEI error rate exceeds this threshold, it indicates that the TCMi has detected a quality degradation, prompting the reporting of the ODUk_TCMi_BEI_EXC error excursion alarm. A smaller threshold value signifies a higher quality requirement. The default value is 1.0E-3.
TIM Subsequent response enable	• Enable • Prohibit	Configuration reporting ODUk_PM_TIM Subsequent response function of the alarm . The default is disabled.
Non-intrusive monitoring	• Enable • Prohibit	Configure the non-intrusive monitoring function. The default is disabled.

STAT byte	• Reserve • Signal normal (001) • The signal is LCK Status (101) • The signal is OCI Status (110) • The signal is AIS Status (111) • Passive TC status (000) • Signal exists IAE (010)	Display the actual received STAT Expenses.

Note

- The TTI configuration interface of PM is shown in Figure 3-1 and Figure 3-2 , and the TTI default value is shown in Table 3-13 .
- The high-order ODUk interfaces on the line side and the client side, as well as the Client-ODUk interface corresponding to the non-OTN service on the client side, support the configuration of PM related functions.
- The low-order ODUk interface on the line side and the client side transparently transmits PM information.

Configuring TCM Overhead

The main configuration contents of TCM (Tandem Connection Monitoring) overhead are as follows.

- The modes and functions of the source and sink ends.
- SAPI, DAPI, and user-defined monitoring (Operator specific) monitoring functions.
- SAPI, DAPI, TTI of user-defined monitoring functions.
- BIP- 8 monitoring function parameters.
- BEI monitoring function parameters.
- Subsequent response function for TIM alarms.
- Subsequent response function for LTC alarm.
- Non-intrusive monitoring capabilities.
- Display received STAT overhead.

Table 3-15 TCM Overhead Parameters

Parameter	Value	Note
Port Name	-	Display TCMi OD port.

TCM level	TCM 1 to TCM 6	Display TCMi level.
Sink Enable	• Enable • Prohibit	Configure the sink function of TCMi. After enabling, monitor the TCMi overhead according to the sink mode. The default is to prohibit.
Sink Mode	• Transparent transmission • Run • Monitor	Configure the TCMi sink mode. The default is transparent transmission.
Source Enable	• Enable • Prohibit	Configuring TCMi When enabled , TCMi overhead is processed according to the source mode. The default is disabled.
Source mode	• Transparent transmission • Run	Configuring TCMi Source mode. The default is transparent transmission.
SAPI Detection	• Enable • Prohibit	Configuring SAPI Monitoring function. Disabled by default.
DAPI Detection	• Enable • Prohibit	Configuring DAPI Monitoring function. Disabled by default.
User-defined detection	• Enable • Prohibit	Configure user-defined monitoring function. Disabled by default.
TTI should be issued	-	Click < ▪▪▪ > Configure SAPI , DAPI , USER (Operator specific , user-defined monitoring) sends TTI content.
TTI receivable	-	Click < ▪▪▪ > Configuration SAPI , DAPI , USER Should receive TTI content.
Received TTI	-	Click < ▪▪▪ > View SAPI , DAPI , USER Actual received TTI content.
BIP8 Error code threshold	• 1.0E - 3 • 1.0E - 4 • 1.0E - 5	Configuring TCMi Overhead BIP- 8 The crossing threshold. BIP- 8 When the bit error rate exceeds the threshold, it indicates TCMi If the quality is degraded, the error code limit alarm ODUk_TCMi_BIP8 _EXC is reported . The smaller the value, the higher the quality requirement. The default is 1.0E-3 .
BIP8 Error degradation threshold	• 1.0E - 6 • 1.0E - 7 • 1.0E - 8 • 1.0E - 9	Configuring TCMi Overhead BIP- 8 degradation threshold. BIP- 8 When the bit error rate exceeds the threshold, it indicates TCMi When quality degradation is detected, the error code exceeding limit alarm ODUk_TCMi_BIP8 _DEG is reported . The smaller the value, the higher the quality requirement. The default is 1.0E-6 .

BEI Error code threshold	• 1.0E - 3 • 1.0E - 4 • 1.0E - 5	Configuring TCMi Expenses BEI The crossing threshold. BEI When the bit error rate exceeds the threshold, it indicates TCMi If the quality is degraded, the error code limit alarm ODUk_TCMi_BEI_EXC is reported . The smaller the value, the higher the quality requirement. The default is 1.0E - 3 .
BEI Error degradation threshold	• 1.0E - 6 • 1.0E - 7 • 1.0E - 8 • 1.0E - 9	Configuring TCMi Expenses BEI degradation threshold. BEI When the bit error rate exceeds the threshold, it indicates TCMi When quality degradation is detected, the error code limit alarm ODUk_TCMi_BEI_DEG is reported . The smaller the value, the higher the quality requirement. The default is 1.0E - 6 .
TIM Subsequent response enable	• Enable • Prohibit	Configuration reporting ODUk_TCMi_TIM Subsequent response function of the alarm . The default is disabled.
LTC Subsequent response enable	• Enable • Prohibit	Configure and report ODUk_TCMi_LTC Subsequent response function of the alarm . The default is disabled.
STAT byte	-	Display the actual received STAT Expenses.
Non-intrusive monitoring	• Enable • Prohibit	Configure the non-intrusive monitoring function. Disabled by default.

Note

The TTI configuration interface of TCM is shown in Figure 3-1 and Figure 3-2 , and the TTI default value is shown in Table 3-13 .

Configuring GCC Overhead

The GCC overhead supports configuring the port to either disable the GCC functionality or enable it and select the GCC channel to be used.

Table 3-16 GCC overhead parameters

Parameter	Value	Note
Port Name	-	Display Port.
Network management information transmission channel	• Prohibit • GCC0 • GCC1 • GCC2	Configure the transmission channel for network management information, specifically which GCC overhead byte to use for transmission. The default setting is GCC0.

4.4. Configuration Examples

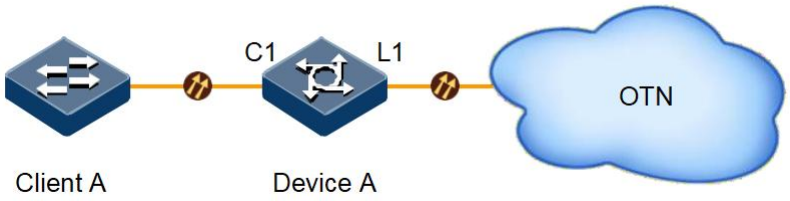
4.4.1. Example of Configuring OTN Services

Network Requirements

According to the network planning, the C1 interface on the client side of the equipment accesses the 10GE Ethernet service, which is cross-connected to the L1 interface on the line side , occupying the 1st to 8th time slots of the L1 interface . The L1 on the line side is multiplexed and accessed to the OTN network. The network connection is shown in Figure 3-3 .

The client-side service mode of the device needs to be configured as Mapper, which is applicable to client-side access to multiple 10GE and other 10 G Any services.

Figure 3 - 3 Network connection



Configuration steps - client-side business mode

Step 1 In the resource tree on the main interface of Device A, click to select the 18M2C2 board. In the function list, click [Configuration/Service Mode Configuration].

Step 2 The single board service configuration mode is displayed in the configuration interface on the right, and the configuration parameters are shown in the following table.

Step 3 After the configuration is complete, click <Apply>.

Parameter	Value
Board Mode	MAPPER mode

Configuration Steps - Cross Connection

Step 1 In the resource tree on the main interface of Device A, click to select the root node of the network element. In the function list, click [OTN Service/Cross-link Configuration].

Step 2 Click <Add> and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value
Name	1
Rate	ODU 2
Direction	Bidirectional
Source Port	1 -Client 1
Sink Port	1 -Line 1
Source port service type	10GE LAN
Source port mapping mode	GFP- F
Sink port service type	OTU4
Sink port mapping mode	ODU- >OTU
Sink Time Slot	1 - 8

Check the results

- In the resource tree on the main interface of Device A, click to select the NE root node. In the function list, click [OTN Service/Cross-connection Configuration] to check whether the cross-connection information is consistent with the plan.
- Client A's services can be transmitted normally.
- Unplug the optical fiber on the client side, and the other end detects the OPU_CSF alarm.
- Unplug the optical fiber on the line side, and the client-side interface outputs a Local Fault alarm.

4.4.2. Example of configuring OCh 1+1 protection

Network Requirements

As shown in Figure 3-4 , to improve the transmission reliability between Device A and Device B, OCh 1 + 1 protection is configured on the two devices. This network uses the dual-transmit selective reception function of OCh 1 + 1 protection to protect the upstream OTU4 service, upstream OCh channel, upstream interface, and physical link.

- The protection function requirement parameters are shown in Table 3-17. The relevant parameters not mentioned in the table use the default values.

- After configuring the protection group, you need to force switching to the protection channel in advance due to reasons such as line cutover and maintenance.

Figure 3 - 4 OCh 1 + 1 protection network diagram

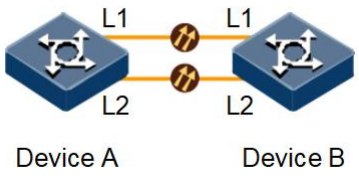


Table 3-17 OCh 1 + 1 protection networking parameters

Parameter	Device A	Device B	Note
Working channel port	Line 1		The network connection consists of 2 Line1 port connections and 2 Line2 port connections.
Protect channel ports	Line 2		
Switching mode	Unidirectional		Unidirectional switching does not require handling the APS protocol, allowing for faster switching.
Return method	Non-return		The transmission quality and loss of the two lines are similar, so no return is required.
APS Enable	Prohibit		APS does not need to be enabled for unidirectional protection switching protocol.

Configuration Steps - OCh 1+1 Protection Group

The protection group configuration steps and parameters of Device A and Device B are the same. Parameters not involved in the configuration steps use the default values.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [OTN Service/Protection Configuration].

Step 2 Click the Port Protection Configuration tab, click <Add>, and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value
Protection group name	OCh 1 + 1 Group 1
Protection group type	Channel 1 + 1
Working port	1 -Line 1
Protect Port	1 -Line 2
Switching mode	Unidirectional

Return method	Non-return
APS Enable	Prohibit

Configuration steps - forced switching

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [OTN Service/Protection Configuration].

Step 2 Click the Port Protection Configuration tab, right-click the protection group record, and click Force Switch to Protection.

Check the results

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [OTN Service/Protection Configuration].

Step 2 Click the protection group record at the top of the configuration interface. Check the Values in the "Properties" tab at the bottom of the interface. They should be consistent with the configured values. Check the "Switch Status" parameter. It should be "Normal".

Step 3 Click the Channel Status tab at the bottom of the interface and check the Channel Status parameters of the working channel and the protection channel. The value should be Normal, the Working Status of the working channel should be Working, and the Working Status of the protection channel should be Waiting.

4.4.3. Example of Configuring OTN Service Overhead

Network Requirements

For OTN services, PM overhead is configured to monitor whether the line-side service transmission is normal.

- Monitor the PM overhead SAPI of ODU 2 on the line side : After enabling SAPI monitoring and configuring the SAPI value, if the SAPIs are different, the device reports a TIM alarm.
- networking and prerequisite configuration , see " 3.4.2 Example for Configuring OCh 1 + 1 Protection".

Note

- If there is no relay device between service paths, either SM overhead or PM overhead can be monitored.

- If there is a relay device between service paths, the relay device will terminate the SM overhead, so the PM overhead should be monitored.

Configuration steps

The configuration steps and parameters for both ends of the service are the same. This article takes Device A as an example.

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [Configuration/OTN Overhead Management] .

Step 2 In the configuration interface on the right, click the PM Overhead tab to display the overhead records of the configured OTN service ports.

Step 3 Click to select the port record, click <Modify> to open the configuration panel for configuration. The configuration-related parameters are shown in the following table.

Step 4 After the configuration is complete, click <Save> to deliver the configuration.

Table 3 - 18 Configuration parameters

Parameter	Values of the working channel interface	Parameters of the protection channel interface
Port Name	1 -L 1 _ODU 2 _ 1	1 -L 2 _ODU 2 _ 1
SAPI Detection	Enable	Enable
TTI should be issued	fscom-telecom (click <▪▪▪ > Configure SAPI in text form)	fscom-telecom (click <▪▪▪ > Configure SAPI in text form)
TTI receivable	fscom-telecom (click <▪▪▪ > Configure SAPI in text form)	fscom-telecom (click <▪▪▪ > Configure SAPI in text form)

Check the results

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [Configuration/OTN Overhead Management].

Step 2 In the configuration interface on the right, click the "PM Expenses" tab, click Interface Record at the top of the interface, and check that the "Text to be sent" and "Text received" information of SAPI at the bottom of the interface are the same as the configured "TTI to be sent".

4.4.4. Example of Configuring SNCP Protection

Network Requirements

According to the network planning, the device has been configured in Mapper mode and connected to 10GE services. Now it is necessary to configure service cross-connection and line-side ODUk SNCP 1 + 1 protection. The network connection is shown in Figure 3 - 5. The planned parameters are shown in Table 3 - 19. Other parameters use the default parameters.

Figure 3-5 Network connection

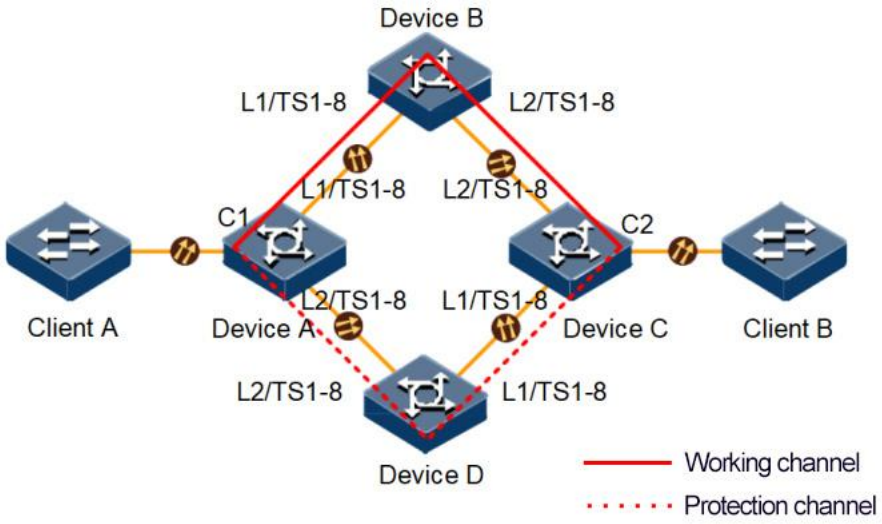


Table 3-19 Planning parameters

Device	Protected Channel	Working channel	Protection channel	Through Cross
Device A	C 1	L 1 No. 1 to 8 Time slot	L 2 No. 1 to 8 Time slot	-
Device B	-	-	-	L 1 No. 1 to 8 The time slots are cross-connected to L 2 No. 1 to 8 Time slot
Device C	C 2	L 2 No. 1 to 8 Time slot	L 1 No. 1 to 8 Time slot	-
Device D	-	-	-	L 2 No. 1 to 8 The time slots are cross-connected to L 1 No. 1 to 8 Time slot

Configuration steps - Configuring Device A service cross-connection and ODUk SNCP 1+1 protection

Step 1 In the resource tree on the main interface of Device A, click to select the NE root node. In the function list, click [OTN Service/Cross-link Configuration].

Step 2 Click <Add> and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value
Name	C 1
Rate	ODU 2
SNCP Protecting location	Sink protection
Cross direction	Bidirectional
Source Port	1 -Client 1
Sink Port	1 -Line 1
Source port service type	10GE LAN
Sink port service type	OTU4
Source port mapping mode	GFP- F
Sink port mapping mode	ODU- >OTU
Sink Time Slot	1 - 8
Protecting the sink port	1 -Line 2
Guard Sink Slot	1 - 8

Configuration steps - Configuring Device B to pass-through crossover

Step 1 In the resource tree on the main interface of Device B, click to select the NE root node. In the function list, click [OTN Service/Cross-link Configuration].

Step 2 Click <Add> and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Table 3 - 20 Configuration parameters

Parameter	Value
Name	1
Rate	ODU 2
SNCP Location	No protection
Direction	Bidirectional
Source Port	1 -Line 1
Sink Port	1 -Line 2

Source port service type	OTU4
Sink port service type	OTU4
Source port mapping mode	ODU- >OTU
Sink port mapping mode	ODU- >OTU
Source time slot	1 - 8
Sink Time Slot	1 - 8

Configuration steps - Configuring Device C service cross-connection and ODUk SNCP 1+1 protection

Step 1 In the resource tree on the main interface of Device C, click to select the NE root node. In the function list, click [OTN Service/Cross-link Configuration].

Step 2 Click <Add> and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value
Name	C 2
Rate	ODU 2
SNCP Protecting location	Sink protection
Cross direction	Bidirectional
Source Port	1 -Client 2
Sink Port	1 -Line 2
Source port service type	10GE LAN
Sink port service type	OTU4
Source port mapping mode	GFP- F
Sink port mapping mode	ODU- >OTU
Sink Time Slot	1 - 8
Protecting the sink port	1 -Line 1
Guard Sink Slot	1 - 8

Configuration steps - Configuring Device D to pass-through crossover

Step 1 In the resource tree on the main interface of Device D, click to select the NE root node. In the function list, click [OTN Service/Cross-link Configuration].

Step 2 Click <Add> and the parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Table 3 - 21 Configuration parameters

Parameter	Value
Name	1
Rate	ODU 2
SNCP Location	No protection
Direction	Bidirectional
Source Port	1 -Line 2
Sink Port	1 -Line 1
Source port service type	OTU4
Sink port service type	OTU4
Source port mapping mode	ODU- >OTU
Sink port mapping mode	ODU- >OTU
Source time slot	1 - 8
Sink Time Slot	1 - 8

Check the results

Step 1 In the resource tree on the main interface of each NE, click to select the NE root node. In the function list, click [OTN Service/Cross-connection Configuration] to check whether the cross-connection is consistent with the plan.

Step 2 Click the cross-connection record, click the Channel Status tab on the interface, and check the Channel Status of the working channel and protection channel. The status should be normal.

Step 3 Check that the services of Client A and Client B can be transmitted normally.

5. Alarm Management

This chapter introduces how to configure alarm management related functions.

- Overview
- Configure Alarm Synchronization
- Configure Alarm Shielding

- Configure Alarm Reversal

5.1. Overview

5.1.1. Alarm Management Function

Alarms are mainly used to record equipment fault information to facilitate equipment troubleshooting. Alarm management is mainly to manage the alarm function of the equipment, reduce meaningless alarm information, and ensure that the equipment alarm is more effective. The alarm management functions are described as follows.

Basic alarm functions

- Alarm synchronization: Synchronize all alarm records of the device.
- Alarm query: Query and view the current alarm.
- Alarm Delete: Manually delete the alarm information on the device.

Automatic alarm reporting

Configure whether to report device alarms to the network management system through traps. That is, when an alarm is generated, an SNMP trap message carrying alarm information is automatically sent. Alarms that are not automatically reported are only recorded on the device.

Alarm shielding

Configure whether to shield device alarms. Shielded alarms will not be recorded on the device or reported to the network management system.

- When alarm shielding is enabled, the device discards the specified alarms without subsequent processing, and the alarms are not recorded on the device.
- Alarm shielding configuration supports configuration by alarm type.

Alarm reversal

Configure the interface alarm inversion function to reverse the alarms of unused interfaces. Alarm inversion can reduce invalid

alarms and support the generation of alarms to prompt that the interface is connected. The device supports three alarm inversion modes, and you can configure whether to enable the inversion function for the interface.

- Non-reversal mode: Device alarms are reported normally.
- Manual recovery mode: When the alarm reversal mode is configured as manual recovery mode, regardless of the current alarm status of the interface, the reported alarm status of the interface is immediately changed to the opposite of the actual alarm status. That is, when there is an actual alarm, the corresponding recovery alarm is reported, and when there is no actual alarm, the alarm is reported.
- Automatic recovery mode: When the alarm reversal mode is set to automatic recovery mode, once the reversal alarm of the interface is restored, the interface automatically enters the alarm non-reversal mode and reports alarms normally. That is, the alarm reversal function is canceled as long as the alarm reversal recovery is completed once.

Note

If the interface currently has no reversible alarm, the configuration can be successful but will not actually take effect; if the interface currently has a reversible alarm, the setting is successful, the corresponding recovery alarm is reported and the reversal mode is entered, that is, the reported alarm status is immediately changed to the opposite of the actual alarm status.

5.1.2. Alarm level

Alarm levels are classified according to the severity of the alarm. Different alarm types are divided into five levels according to their severity. The severity levels are as follows from high to low:

Alarm level	Color	Note
Emergency Alert (Critical)	Red:	The highest level will cause business system interruption.
Major warnings (Major)	Orange:	The business system was not interrupted, but its performance was severely degraded, affecting user business operations.
Minor Alarm (Minor)	Yellow:	The system generates an alarm message but does not affect the operation of the business system.
Prompt warning (Warn)	Teal:	The business system is operating normally, but general usage issues have occurred.
Unknown alarm (Unknown)	Light Gray :	Unrecognizable warning message.

5.2. Configuring Alarm Synchronization

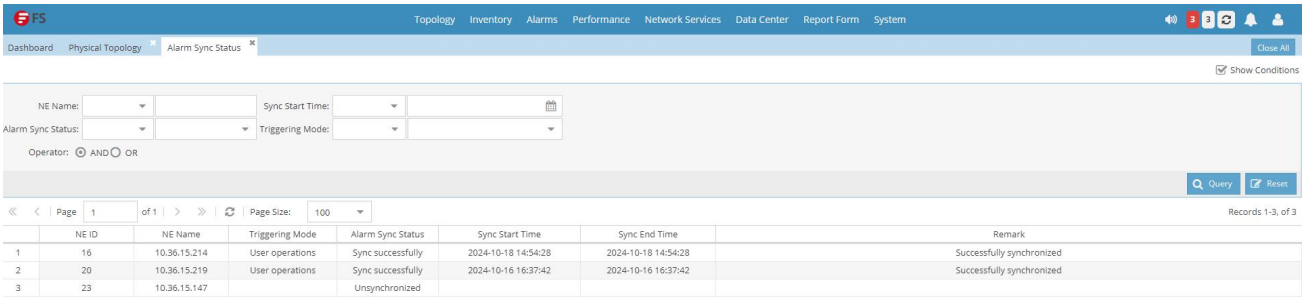
Configuring alarm synchronization is to synchronize the current alarm data of the device with the network management system so that the alarm information is consistent with the device.

Step 1 Click [Topology/Topology View] in the top navigation.

Step 2 In the topology diagram, right-click the NE and click [Alarm Synchronization] to manually synchronize alarms. A small icon is displayed above the NE icon, indicating that synchronization is being performed.

Step 3 Then wait disappears, synchronization is complete.

Step 4 (Optional) Click [Alarm/Alarm Synchronization Status Monitoring] in the top navigation to view the alarm synchronization status, as shown in the following figure.



5.3. Configuring Alarm Shielding

Notice

- If the alarm is configured to be shielded, the device will not record the shielded alarm, and the network management system will not receive the alarm. As a result, the device failure may not be discovered. Please use it with caution according to the actual situation.
- By default, no alarm is masked.
- APS automatic protection switching related alarms do not support configuration of alarm shielding.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Alarm Management/Alarm Type Shielding]. The configuration interface on the right displays the alarm shielding configuration according to the alarm type.

Step 2 Select the alarm type that needs the alarm shielding function. If the parameter "Is it effective for all boards" is "Yes", it means that all boards of the device are configured to shield this alarm type at the same time.

Step 3 After the configuration is complete, click <Apply> to deliver the configuration.

5.4. Configuring Alarm Reversal

Notice

- Before configuring the interface alarm reversal function, make sure that the "Alarm Reversal Mode" parameter in the [Alarm Management/Alarm Attribute Configuration] interface of the NE is set to "Automatic Recovery Mode" or "Manual Recovery Mode". Otherwise, the interface configuration reversal function will not take effect.
- If you configure alarm reversal, please note that the actual situation is the opposite of the alarm status. Please use it with caution according to the actual situation.

Configuring the device alarm inversion mode

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [Alarm Management/Alarm Attribute Configuration]. The configuration parameters are shown in the following table.

Step 2 After the configuration is complete, click <Apply> to deliver the configuration.

Parameter	Value	Note
Alarm reversal mode	• Automatic recovery mode • Manual recovery mode • Non-inverting mode	Configure the alarm inversion mode. The device supports configuration of the inversion mode, and the device interface supports individual configuration of whether the inversion is enabled. The default is automatic recovery mode.

Configuring the alarm inversion function on an interface

Step 1 In the resource tree on the main interface, click to select a board. In the function list, click [Alarm Configuration/Alarm Reverse Configuration].

Step 2 Click the port record and click <Modify>. The parameters are shown in the following table.

Step 3 After the configuration is complete, click <Save> to deliver the configuration.

Parameter	Value	Note
Alarm reversal	• Reversal • No Reversal	Configure the alarm inversion function. The default is no inversion.

6. Maintenance Management

This chapter introduces the maintenance functions of the device.

- Overview
- Management Boards
- Backup and Upgrade
- Configuration Examples

6.1. Overview

6.1.1. Backup and Upgrade

Backup and upgrade is to back up and upgrade the system files of the device.

System files

System files refer to the files required during the operation of the device (such as system software, configuration files, etc.). Such files are generally stored in the memory of the device. In order to facilitate users to effectively manage the memory, the device uses file system

These files are managed in a traditional way. The specific functions mainly include backup, upgrade and deletion of system files.

The configuration file is the configuration item file that needs to be loaded when the device is started this time or next time. After the device is powered on, it reads the configuration file from the memory to initialize the device. Therefore, the configuration in the configuration file is called the initial configuration.

If there is no configuration file in the memory, the device will be initialized with default parameters. Corresponding to the initial configuration, the configuration that is in effect during the operation of the device is called the current configuration.

The user can modify the current configuration of the device. In order to make the current configuration the starting configuration when the device is powered on next time, it is necessary to save the current configuration to the memory to form a configuration file. The management operations of the configuration file include backup, upgrade or delete.

Backup

Backup means copying the system files stored in the device memory to the server memory for storage, so that the backup files can be restored when the device fails to ensure normal operation of the device. When the device fails as follows, the old system files need to be restored:

- System files are lost or damaged due to equipment failure.
- The device malfunctioned due to a system upgrade failure.

It is recommended that users regularly back up device system files to the server's storage.

Upgrade

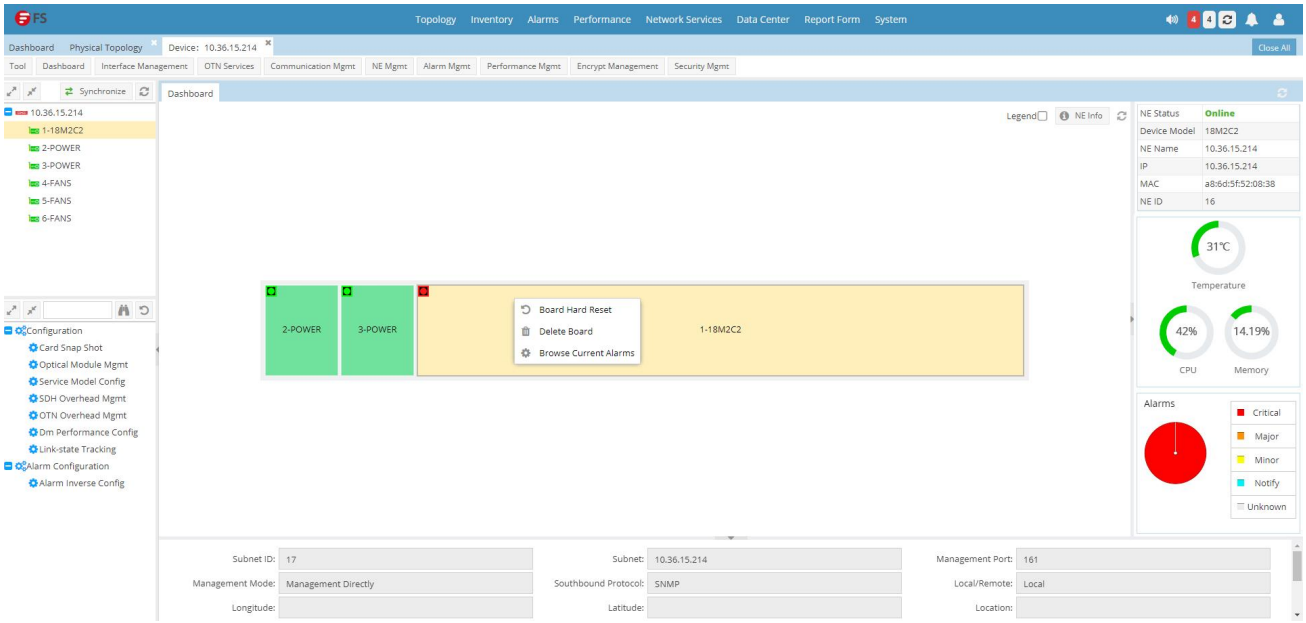
When you need to add new features to the device, optimize the original functions, or solve the bugs in the current software version, you can upgrade the system software of the device. The specific function is mainly to upgrade the system software, or quickly configure the same device of the same model by upgrading the configuration file.

6.2. Management Boards

The device board supports reset, restart and delete functions.

Notice

- Resetting a board will cause service interruption and is usually only used for maintenance or testing. Please use it with caution according to actual conditions.
- Deleting a board will also delete the board alarm and other related historical data in the network management system, and the data cannot be restored. It is usually only used for maintenance or testing. Please use it with caution according to the actual situation.
- After deleting the board, perform the network element synchronization function on the network element and support adding the board to the network management system again.
- In the overview interface, right-click the board node and click [Board Reset] to configure the board reset and restart, as shown in the following figure.
- In the overview interface, right-click the board node and click Delete Board to configure the information related to the deleted board.



6.3. Backup and Upgrade

Notice

Before upgrading, please confirm the current software version and contact technical support personnel for upgrading .

The board of the device supports FTP backup (ie upload) and upgrade (ie download), mainly for backing up and upgrading

software and configuration files.

Note

- Usually, you need to back up before upgrading to provide relevant files for rollback to avoid the inability to quickly restore service due to upgrade failure.
- Please make sure that the name of the configuration file used for the upgrade contains the keyword "startup".
- Since the FTP protocol is required for communication, it is necessary to confirm that the device and the FTP server can communicate normally. The FTP protocol communication port is 21 .
- generally, the upgrade sequence is Bootrom, FPGA, and system software. When upgrading multiple files on a board, set the "Update Operation" of the last file to "Restart after completion" and set the "Update Operation" of the previous files to "Start". This configuration allows the board to download all upgrade files first and then restart, reducing service interruption time.

Step 1 In the resource tree on the main interface, click to select the NE root node. In the function list, click [NE Management/Upload/Download]. The parameters are shown in the following table.

Step 2 After the configuration is complete, click <Apply> to perform the backup or upgrade.

Table 5-1 Backup and upgrade parameters

Parameter	Value	Note
Update Control	• Upload • download	Select the Upgrade or Backup function. • Download: Execute the upgrade function. • Upload: Executes the backup function.
FTP IP address	Dotted decimal IP address	Configure FTP Server IP address.
Username	-	Configure FTP username.
Password	-	Configure FTP password
File Type	• System Software • Configuration Files • FPGA • FPGA 2 • System log files	Select system files to upgrade or back up. Users usually only need to select system software or configuration files. System log files only support backup.

Slot	-	Select the slot where the board is located.
File name	-	The file name downloaded from the FTP server during configuration upgrade and the file name uploaded to the FTP server during backup.
Update Type	Update Now	Configure the execution time of backup or upgrade. Immediate update is a one-time operation, which performs a backup or upgrade immediately after the configuration is delivered.
Update Status	• Prepare • Loading	Displays the current operation status of the backup or upgrade.
Update Operation	• Prepare • Start • Restart after completion	Configure the backup or upgrade operation. • Prepared: indicates that no configuration has been performed. • Start: Send to the device and perform corresponding operations. The operation results will take effect at the next startup. • Restart after completion: Send the data to the device to perform the operation . After the operation is completed, restart the device.
Last updated	-	Display the time when the last backup or upgrade operation was performed.
Update result description	• Success • Fail	Display the backup or upgrade execution results.

6.4. Configuration Examples

6.4.1. System Software Backup and Upgrade Configuration Example

Network Requirements

As shown in Figure 5-1 , the device and FTP server work together to complete the backup and upgrade of system software. Before upgrading, you need to back up the current version of the device's system software. The relevant required parameters for backup and upgrade are shown in Table 5-2 .

Figure 5-1 Backup and upgrade diagram

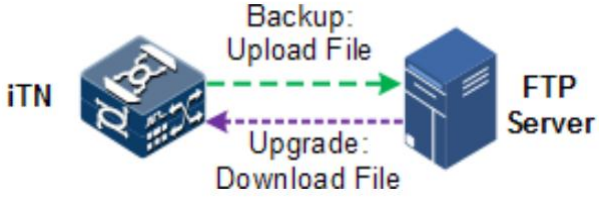


Table 5-2 Backup and upgrade related requirement parameters

Parameter	Value	Note
FTP Server IP address	192 . 168 . 0 . 100	Remove IP Address, FTP The port used by the protocol should be 21 .
FTP username	User 1	-
FTP password	User 1	-
Slot	1	Performs an operation on a single board in slot 1.
File Type	System startup software	Device system software.
Backup file name	Backup 1	Upload to FTP The file name to be saved when logging in to the server .
Upgrade file name	Update 1	The name of the file downloaded from the FTP server.
Execution time	Execute immediately	-
Restart after upgrade	yes	After the upgrade, you need to restart the device to work with the upgraded system software.

Configuration steps

Step 1 Back up system software.

1. In the resource tree on the main interface, click to select the NE root node. In the function list, click [NE Management/Upload/Download]. The parameters are shown in the following table.
2. After the configuration is complete, click <OK> to perform the backup or upgrade.

Table 5-3 Backup and upgrade parameters

Parameter	Value
Update Control	Upload
FTP IP address	192 . 168 . 0 . 100
username	User 1
password	User 1
File Type	System Software
Slot	18M2C2
File name	Backup 1
Update Type	Update Now
Update Operation	Start up

Step 2 Upgrade system software.

1. In the resource tree on the main interface, click to select the NE root node. In the function list, click [NE Management/Upload/Download]. The parameters are shown in the following table.
2. After the configuration is complete, click <OK> to perform the backup or upgrade.

Table 5-4 Backup and upgrade parameters

Parameter	Value
Update Control	download
FTP IP address	192 . 168 . 0 . 100
Username	User 1
Password	User 1
File Type	System Software
Slot	18M2C2
File name	Update 1
Update Type	Update Now
Update Operation	Restart after completion

Check the results

When backing up and upgrading, click <Refresh> in the configuration interface and check the "Update Result Description" parameter, which should be displayed as successful.

7. Appendix

This chapter introduces the alarm list and performance indicator list supported by the device, as well as the abbreviations and terms used in this document.

- Alarm List
- Terminology
- Abbreviations

7.1. Alarm List

Table 6-1 Alarm List

English name
chassis lost
find new chassis
cold start
warm start
authentication failure
upgrade/backup failure
upgrade/backup success
temp. above the upper threshold
temp. below the lower threshold
temp. normal
power module pulled out
power module plugged in
power module output fault
power module output normal
voltage above the upper threshold
voltage below the lower threshold
fan module pulled out
fan module plugged in
fan fault
fan normal
System clock source switch
System clock source lost
System clock source recovery
System clock source SD
System clock source SD recovered
general alarm led On
general alarm led Off
System Clock Abnormal
System Clock Normal
Input voltage above the upper threshold

Input voltage below the lower threshold
Input voltage above the upper threshold
Input voltage above the upper threshold
Input voltage below the lower threshold
Input voltage exceed the Threshod, recovered
Output voltage above the upper threshold
Output voltage below the lower threshold
Output voltage exceed the Threshod, recovered
Save configuration success
Save configuration failure
Optical module pulled out
Optical module pulled in
Optical module laser transmit fault
Optical module laser transmit normal
Optical module R_LOS
Optical module R_LOS, recovered
port link down
port link up
remote port link down
remote port link up
port looped
port no looped
Optical module temp. above the upper threshold
Optical module temp. below the lower threshold
Optical module temp. exceed the threshold, recovered
Optical module voltage above the upper threshold
Optical module voltage below the lower threshold
Optical module voltage exceed the threshold, recovered
Optical module current above the upper threshold
Optical module current below the lower threshold
Optical module current exceed the threshold, recovered

Optical module transmit power above the upper threshold
Optical module transmit power below the lower threshold
Optical module transmit power exceed the threshold, recovered
Optical module receive power above the upper threshold
Optical module receive power below the lower threshold
Optical module receive power exceed the threshold, recovered
Optical module temp. above the upper threshold warning
Optical module temp. below the lower threshold warning
Optical module temp. exceed the threshold warning, recovered
Optical module voltage above the upper threshold warning
Optical module voltage below the lower threshold warning
Optical module voltage exceed the threshold warning, recovered
Optical module current above the upper threshold warning
Optical module current below the lower threshold warning
Optical module current exceed the threshold warning, recovered
Optical module transmit power above the upper threshold warning
Optical module transmit power below the lower threshold warning
Optical module transmit power exceed the threshold warning, recovered
Optical module receive power above the upper threshold warning
Optical module receive power below the lower threshold warning
Optical module receive power exceed the threshold warning, recovered
Optical module laser backlight power crossed
Optical module laser backlight power normal
Optical module laser lifetime expired
Optical module laser lifetime recovered
port LOL

port LOL recovered
port LOS
port LOS recovered
port protection switch
port protection switch recovered
fiber port R_LOS
fiber port R_LOS recovered
fiber port LOF
fiber port LOF recovered
fiber port BER> 1 E- 3
fiber port BER> 1 E- 3 recovered
fiber port BER> 1E - 6
fiber port BER> 1E - 6 recovered
fiber port receive power below the lower threshold warning
fiber port receive power exceed the threshold warning, recovered
ETH CRC error
ETH CRC correct
ETH CRC error stat. above the threshold
ETH CRC error stat. normal
ETH Local Fault
ETH Local Fault,Recovered
ETH Remote Fault
ETH Remote Fault,Recovered
LSP Up
LSP Down
GFP frame error rate exceed the threshold
GFP frame error rate exceed the threshold, recovered
SDH channel protection switch
SDH path protection switch recovered
R_LOF
R_LOF recovered

R_OOF
R_OOF recovered
RS_TIM
RS_TIM recovered
RS_EXC
RS_EXC recovered
RS_DEG
RS_DEG recovered
RS_ES exceed the threshold
RS_ES normal
RS_SES exceed the threshold
RS_SES normal
RS_UAS
RS_UAS recovered
voltage above threshold recovery
voltage below threshold recovery
temp. above threshold recovery
temp. below threshold recovery
Power input current exceed the threshold Alarm
Power input current exceed the threshold Alarm, recovered
OAM discovered
OAM remote device lost
extend OAM upgrade/backup
Errored Symbol Period Event
Errored Frame Period Event
Errored Frame Event
Errored Frame Seconds Summary Event
Link Fault
Link Fault Recovered
Dying Gasp
Dying Gasp Recovery

Critical Event
Critical Event Recovery
Optical module Not Ready
Optical module ready
Optical module authentication check failed
Optical module authentication check succeed
Optical module wavelength above the upper threshold
Optical module wavelength below the lower threshold
Optical module wavelength exceeds the threshold, recovered
Optical module wavelength above the upper threshold warning
Optical module wavelength below the lower threshold warning
Optical module wavelength exceeds the threshold warning, recovered
Optical module password check failure
Optical module password check succeed
AIS Alarm
AIS Alarm Recovered
Locking LCK Alarm
Locking LCK Alarm Recovered
Client Loss of Signal
Client Forward Defect
Client Reverse Defect
Client Defect Clear
Optical module Temperature Alarm Normal
Optical module Temperature Warning Normal
in_power. above the high threshold
in_power. below the low threshold
in_power.recovered
pump_cold. above the highest threshold
pump_cold.recovered

pump_temp. above the highest threshold
pump_temp.recovered
pump_power. above the highest threshold
pump_power.recovered
OTU Loss of Frame
OTU Loss of Frame recovered
OTU Loss of Multiframe
OTU Loss of Multiframe recovered
OTU Alarm Indication Signal
OTU Alarm Indication Signal recovered
OTU Trail trace Identifier Mismatch
OTU Trail trace Identifier Mismatch recovered
OTU Server Signal Fail
OTU Server Signal Fail recovered
OTU_SM Backward Defect Indication
OTU_SM Backward Defect Indication Recovered
Error threshold crossing Before Forward Error Correction
Error threshold crossing Before Forward Error Correction recovered
Error threshold crossing After Forward Error Correction
Error threshold crossing After Forward Error Correction recovered
ODU_PM Locked defect
ODU_PM Locked defect recovered
ODU_PM Open Connection Indication
ODU_PM Open Connection Indication recovered
ODU_PM Alarm Indication Signal
ODU_PM Alarm Indication Signal recovered
ODU_PM Trail trace Identifier Mismatch
ODU_PM Trail trace Identifier Mismatch recovered
ODU_PM Server Signal Fail
ODU_PM Server Signal Fail recovered

ODU_PM Backward Defect Indication
ODU_PM Backward Defect Indication recovered
ODU_TCM Locked defect
ODU_TCM Locked defect recovered
ODU_TCM Open Connection Indication
ODU_TCM Open Connection Indication recovered
ODU_TCM Alarm Indication Signal
ODU_TCM Alarm Indication Signal recovered
ODU_TCM Trail trace Identifier Mismatch
ODU_TCM Trail trace Identifier Mismatch recovered
ODU_TCM Server Signal Fail
ODU_TCM Server Signal Fail recovered
ODU_TCM Backward Defect Indication
ODU_TCM Backward Defect Indication recovered
OPU Payload Mismatch
OPU Payload Mismatch recovered
OTU SM_IAE Alarm
OTU SM_IAE Alarm Recovery
OTU SM_BIAE Alarm
OTU SM_BIAE Alarm Recovery
OTU TCM Input Location Error
OTU TCM Input Location Error Recovery
ODU_TCM_BIAE Alarm
ODU_TCM_BIAE Alarm Recovery
ODU_TCM_LTC Alarm
ODU_TCM_LTC Alarm Recovery
ODU_LOFLOM Alarm
ODU_LOFLOM Alarm Recovery
OPU Loss of Frame(LOOMFI)
OPU Loss of Frame(LOOMFI),Recovered
Card Not Polling Alarm

Card Not Polling Alarm Normal
OTU_SM_BIP8 _OVER Alarm
OTU_SM_BIP8 _OVER Alarm Recovered
OTU_SM_BIP8 _DEG Alarm
OTU_SM_BIP8 _DEG Alarm Recovered
OTU_SM_BEI_OVER Alarm
OTU_SM_BEI_OVER Alarm Recoverd
OTU_SM_BEI_DEG Alarm
OTU_SM_BEI_DEG Alarm Recoverd
OTU_OOM Alarm
OTU_OOM Alarm Recovered
ODU_BIP8 _OVER Alarm
ODU_PM_BIP8 _OVER_OK
ODU_BIP8 _DEG Alarm
ODU_PM_BIP8 _DEG_OK
ODU_BEI_DEG Alarm
ODU_PM_BEI_DEG_OK
ODU_BEI_OVER Alarm
ODU_PM_BEI_OVEROK
ODU_TCM_BIP8 _OVER Alarm
ODU_TCM_BIP8 _OVER Alarm Recovered
ODU_TCM_BIP8 _DEG Alarm
ODU_TCM_BIP8 _DEG Alarm Recovered
ODU_TCM_BEI_OVER Alarm
ODU_TCM_BEI_OVER Alarm Recovered
OPU_MSIM Alarm
OPU_MSIM Alarm Recovered
OPU_CSF Alarm
OPU_CSF Alarm Recovered
HA_SWITCH
HA Backup Failed

HA Backup Failed Normal
HA Software Heartbeat Disappears
HA Software Heartbeat Disappears Normal
HA Electrical Management Heartbeat Disappears
HA Electrical Management Heartbeat Disappears Normal
HA Slave Fault
HA Slave Fault Normal
SYS_CLOCK_SW_OK
OTU_OOF Alarm
OTU_OOF Alarm Recovered
ODU_LCK Alarm
ODU_LCK Alarm Recovered
ODU_OCI Alarm
ODU_OCI Alarm Recovered
FOP_PM_OK
FOP_PM
APS
APS_OK
ODU_AIS Alarm
ODU_AIS Alarm Recovered
ODU_TCM_BEI_DEG Alarm
ODU_TCM_BEI_DEG Alarm Recovery
Card Power Off Alarm
Card Power On
Card Register Succeed
Card Restore Succeed
Card Reverse Config Query Failed Alarm
Card Reverse Config Query Succeed
RS twenty four Hours ES Over
RS twenty four Hours ES Over Recovered

RS twenty four Hours SES Over
RS twenty four Hours SES Over Recovered
PPP Interface LinkDown
PPP Interface LinkUp
Grouping Protection Protocol Mismatch Alarm
Grouping Protection Protocol Mismatch Alarm,Recovered
Grouping Protection Switch
Grouping Protection Switch Recovered
APS Switch to Protect Event
APS Switch to Work Event
APS Lock Event
APS Force Switch to Protect Event
APS MS to Work Event
APS MS to Protect Event
APS Signal Fault Switch to Work Event
APS Signal Fault Switch to Protect Event
APS SD Switch to Work Event
APS SD Switch to Protect Event
APS_WTR Event
APS_DNR Event
OTU_SM_BIP8 _ 15 M_ES_OVER
OTU_SM_BIP8_15 M_ES_OVER_OK
OTU_SM_BIP8 _ 15 M_SES_OVER
OTU_SM_BIP8_15 M_SES_OVER_OK
OTU_SM_BIP8 _ 15 M_UAS_OVER
OTU_SM_BIP8_15 M_UAS_OVER_OK
OTU_SM_BEI_ 15M_SES_OVER
OTU_SM_BEI_ 15 M_SES_OVER_OK
OTU_SM_BEI_ 15 M_UAS_OVER

OTU_SM_BEI_ 15 M_UAS_OVER_OK
OTU_SM_BIP8 _ 24 H_ES_OVER
OTU_SM_BIP8_24 H_ES_OVER_OK
OTU_SM_BIP8 _ 24 H_SES_OVER
OTU_SM_BIP8_24 H_SES_OVER_OK
OTU_SM_BIP8 _ 24 H_SES_OVER
OTU_SM_BIP8_24 H_UAS_OVER_OK
OTU_SM_BEI_ 24H_ES_OVER
OTU_SM_BEI_ 24H_ES_OVER_OK
OTU_SM_BEI_ 24H_SES_OVER
OTU_SM_BEI_ 24H_SES_OVER_OK
OTU_SM_BEI_ 24H_UAS_OVER
OTU_SM_BEI_ 24 H_UAS_OVER_OK
ODU_PM_BIP8 _ 15 M_ES_OVER
ODU_PM_BIP8_15 M_ES_OVER_OK
ODU_PM_BIP8 _ 15 M_SES_OVER
ODU_PM_BIP8_15 M_SES_OVER_OK
ODU_PM_BIP8 _ 15 M_UAS_OVER
ODU_PM_BIP8_15 M_UAS_OVER_OK
ODU_PM_BEI_ 15M_ES_OVER
ODU_PM_BEI_ 15 M_ES_OVER_OK
ODU_PM_BEI_ 15M_SES_OVER
ODU_PM_BEI_ 15 M_SES_OVER_OK
ODU_PM_BEI_ 15M_UAS_OVER
ODU_PM_BEI_ 15 M_UAS_OVER_OK
ODU_PM_BIP8 _ 24 H_ES_OVER
ODU_PM_BIP8_24 H_ES_OVER_OK
ODU_PM_BIP8 _ 24 H_SES_OVER
ODU_PM_BIP8_24 H_SES_OVER_OK

ODU_PM_BEI_ 24H_ES_OVER
ODU_PM_BEI_ 24H_ES_OVER_OK
ODU_PM_BEI_ 24H_SES_OVER
ODU_PM_BEI_ 24H_SES_OVER_OK
ODU_PM_BEI_ 24H_UAS_OVER
ODU_PM_BEI_ 24H_UAS_OVER_OK
ODU_TCM_BIP8 _ 15 M_ES_OVER
ODU_TCM_BIP8_15 M_ES_OVER_OK
ODU_TCM_BIP8 _ 15 M_SES_OVER
ODU_TCM_BIP8_15 M_SES_OVER_OK
ODU_TCM_BIP8 _ 15 M_UAS_OVER
ODU_TCM_BIP8_15 M_UAS_OVER_OK
ODU_TCM_BEI_ 15M_ES_OVER
ODU_TCM_BEI_ 15M_ES_OVER_OK
ODU_TCM_BEI_ 15M_SES_OVER
ODU_TCM_BEI_ 15M_SES_OVER_OK
ODU_TCM_BEI_ 15M_UAS_OVER
ODU_TCM_BEI_ 15M_UAS_OVER_OK
ODU_TCM_BIP8 _ 24 H_ES_OVER
ODU_TCM_BIP8_24 H_ES_OVER_OK
ODU_TCM_BIP8 _ 24 H_SES_OVER
ODU_TCM_BIP8_24 H_SES_OVER_OK
ODU_TCM_BIP8 _ 24 H_UAS_OVER
ODU_TCM_BIP8_24 H_UAS_OVER_OK
ODU_TCM_BEI_ 24H_ES_OVER
ODU_TCM_BEI_ 24H_ES_OVER_OK
ODU_TCM_BEI_ 24H_SES_OVER
ODU_TCM_BEI_ 24H_SES_OVER_OK
ODU_TCM_BEI_ 24H_UAS_OVER

ODU_TCM_BEI_ 24 H_UAS_OVER_OK
OTU_SM_BEI_ 15M_ES_OVER
OTU_SM_BEI_ 15 M_ES_OVER_OK
ODU_PM_BIP8 _ 24 H_UAS_OVER
ODU_PM_BIP8_24 H_UAS_OVER_OK
Loopback Of Ethernet Error Device Detected
Device Voltage Higher Recovery
Device Voltage Higher
Device Voltage Lower Recovery
Device Voltage Lower
Remote Device Disapper
Remote Device Discover
Ethernet GFP Client Prior Defect Indication Alarm
Ethernet GFP Client Prior Defect Indication Recovery Alarm
Ethernet GFP Client Reverse Defects Indication Alarm
Ethernet GFP Client Reverse Defects Indication Recovery Alarm
Ethernet GFP Client Signal Los Alarm
Ethernet GFP Client Signal Los Recovery Alarm
Message With L Bit Received
Message With L Bit Received Alarm Recovery
Message With R Bit Received
Message With R Bit Received Alarm Recovery
FC Business Illegal Transfer Character Alarm
FC Business Illegal Transfer Character Alarm Restore
FC Business Code Violation Alarm
FC Business Code Violation Alarm Restore
FC Business LOS Sync Alarm
FC Business LOS Sync Alarm Restore
FC Business Link Fault Alarm
FC Business Link Fault Alarm Restore

FC Business GFP CSF Alarm
FC Business GFP CSF Alarm Restore
FC Business Remote Fault Alarm
FC Business Remote Fault Alarm Restore
PTN Practise Protection Switch Failure Alalrm
SFP laser lifetime expired
SFP laser lifetime expired restore
Pump Monitor Failure Alarm
Pump Monitor Failure Alarm Restore

7.2. Terminology

Numeric	
1 : 1 Protection	1 : 1 Protection means that during normal transmission, the transmitting end sends the main service on the main channel and sends the additional service (low-level service) on the backup channel, and the receiving end receives the main service from the main channel and the additional service from the backup channel. When the main channel is damaged, in order to ensure the transmission of the main service, the transmitting end sends the main service to the backup channel, and the receiving end switches to receiving the main service from the backup channel. At this time, the transmission of the additional service is terminated and the transmission of the main service is restored. This switching method is called double-end switching (both the receiving / transmitting ends are switched), the switching rate is slow, but the channel utilization rate is high. Since the transmission of the additional service must be terminated when the main channel is damaged, the additional service is also called unprotected service.
802.1Q in 802.1Q	QinQ (also known as Stacked VLAN QinQ (or Double VLAN) technology is an extension of 802.1Q and is defined by IEEE in the 802.1ad standard . Basic QinQ is a simple Layer 2 VPN . Tunnel technology, which encapsulates the outer VLAN Tag for the user's private network message at the operator's access end , so that the message carries two layers of VLAN Tags Pass through the operator's backbone network (public network). In the public network, the message is transmitted only according to the outer VLAN Tag (that is, the public network VLAN Tag) , and the user's private network VLAN Tags It is then transmitted as the data part of the message .
A	
Access Layer	The access layer refers to the part facing user connection or access, which is responsible for connecting end-user devices to the communication service provider network and has the characteristics of low cost and high port density. Access layer equipment is characterized by low cost and high functionality.

Alarm	Information reported by a device or network management system when a fault is detected .
Alarm Auto- Report	The device records the alarms that meet the reporting rules and reports them to the network management system. You can configure The device does not need to report alarms to the network management system.
Alarm Filter	The network management system will not receive alarms from devices that meet the filtering rules .
Alarm Inverse	For ports that have not been opened for service, alarm inversion is used to avoidGEnerating related alarm information and avoid alarm interference. By configuring the alarm inversion function, the alarm status of the port is opposite to the actual status, that is, when there is an alarm, no alarm is reported, and when there is no alarm, an alarm is reported.
Automatic Protection Switched	Automatic protection switching technology can detect faults and hidden dangers in a timely manner through real-time monitoring of transmission line changes and automatic analysis of alarm information. When a serious fault occurs, it can quickly switch the working channel to the backup channel and restore communications in a very short time, completing a rapid response and recovery mechanism for faults .
B	
Back Borad	A backplane is an electronic circuit board that includes wiring and sockets into which other electronic devices on other circuit boards or circuit cards can be plugged. In computer systems, a backplane is synonymous with or a subtype of a motherboard.
Board	An electronic module consists of a chip and other electronic components mounted on a flat and rigid substrate, on which a conducting circuit is arranged to connect the components.
C	
Collision Domain	In Ethernet, if a CSMA/CD If two computers on the network communicate at the same time, a conflict will occur . A network is a collision domain. If the segments in an Ethernet network are connected with repeaters, they are still a collision domain because collisions cannot be avoided.
Control Word	Length 4 Byte TDM The service data encapsulation message header is used for circuit emulation services. Its main functions include indicating message sequence number, indicating link failure, indicating that the encapsulated message length is too short, indicating the encapsulated message type and other information.
Current Alarm	The current alarm is defined according to the operational status of the alarm. All alarm events that have not been cleared or filtered become the current alarm.
Customer	Clients use the services provided by the equipment, and client information can be integrated with network elements and alarms. The client information is only stored in the network management system.
E	
Encapsulation	Encapsulation is a technology used by layered protocols. The message from the upper layer protocol is mapped into the data part of the bottom layer protocol. The outer layer of the data is encapsulated by the bottom layer protocol overhead to form the bottom layer

	protocol message structure . Protocol IP Message , mapped into 802.1Q The data part of the protocol , the outer layer consists of 802.1Q The frame header is encapsulated to form a VLAN frame structure.
Ethernet	The most widely used LAN, with speeds of 10 Mbit/s , 100 Mbit/s , and 1000 Mbit/s and 10 Gbit/s Etc., using CSMA/CD Access control method .
Ethernet in the First Mile	Follow IEEE 802 . 3 ah EFM of the agreement It is a link-level Ethernet OAM technology that provides link connectivity detection, link fault monitoring, and remote fault notification functions for the link between two directly connected devices. EFM is mainly used for Ethernet links at the edge of the network where users access.
F	
First Mile	The first mile is from the end-user device to the communications service provider's switch. Connections between rooms.
Force-Switch	Forced switching means that when the main channel is normal, no matter whether the backup channel is normal or not, All services can be forcibly switched to the backup channel.
Forwarding Equivalence Class	MPLS is a classified forwarding technology that requires packets with the same characteristics to be classified into one category, called forwarding equivalence class (FEC) . Packets of the same forwarding equivalence class will receive exactly the same forwarding treatment in the MPLS network. Forwarding equivalence classes are divided according to packet characteristics, such as the same IP address, the same forwarding path, the same service level , etc.
Frame	Data is transmitted on the network in small units called frames. A frame consists of several parts, and different parts perform different functions .
Full-duplex	Both parties on the communication link can send and receive data simultaneously .
H	
Half-Duplex	Half-duplex refers to two-way electronic communication that can only be carried out in the same direction at the same time. Communication where one party is receiving information while the other party is sending information is half-duplex.
History Alarm	Historical alarms are all alarms that have been cleared or filtered .
Hop	The simplest routing metric is the cost of each link. 1. This function can calculate the rated number of times a message is forwarded .
I	
IETF	The abbreviation of Internet Engineering Task Force, established at the end of 1985 , is the most authoritative technical standardization organization for the global Internet . Its main task is to be responsible for the research and development and formulation of Internet-related technical specifications. Currently, the vast majority of international Internet technical standards come from IETF .
In-band Network Management	In-band network management is the communication of network management information between the network management system and devices through the business network .

L	
Label	A set of symbols defined to facilitate identification of certain specially defined data blocks or program segments in a program . In the IEEE 802.11 standard, a label is a short identifier of fixed length and local significance only, which is used to uniquely identify the forwarding equivalence class (FEC) to which a packet belongs.
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.
Link Aggregation Group	A group of links that appear to be one link from the aggregated user. Improve link reliability or ensure even load balancing of traffic.
Local Area Network	A local area network is a network that connects multiple data communication devices in a small area. communication network to achieve resource sharing and data communication within the local area network.
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.
M	
MA	Also known as a service instance, it is a MD Part of an MD It can be divided into one or more service instances. One service instance corresponds to one business and can be mapped to a group of VLANs. The VLANs mapped to different service instances cannot cross.
Manual-Switch	Regardless of whether the backup channel is normal, the manual switching command can be issued successfully, switching the service from the main channel to the backup channel for transmission. However, the manual switching can only take effect when the backup channel is normal.
Mapping	A virtual data correspondence
MD	A network running CFM functions, which determines the scope of the network for OAM management . The maintenance domain has level attributes and is divided into 8 Level (0 to 7) . The larger the number , the higher the maintenance domain level and the larger the range of the corresponding maintenance domain. The protocol packets of the low-level MD are discarded after entering the high-level MD , and the protocol packets of the high-level MD can pass through the low-level MD . Within the same VLAN range , different maintenance domains can be adjacent, nested, and intersecting .
MEP	The edge node of a service instance. A MEP can send and process CFM messages. The service instance to which the MEP belongs and the MD determine the VLAN and level of the messages that the MEP sends and receives.
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.

MP	MEP and MIP is collectively referred to as MP .
Multi-mode Fiber	Multimode optical fiber is an optical fiber that can transmit multiple modes of light in the same optical fiber.
N	
Network Element	Network devices are managed as network elements in the system .
Network Management System	A computer program that manages network devices .
Node	Ageneral term for subnets, network elements, and symbols in a network management system .
O	
Offline	Due to the interruption of management channel or the device being offline, it is out of control of the network management system. The device cannot be managed after it is disconnected from the network.
Optical Power	The work done by light per unit time. The units of optical power are milliwatt (mW) and decibel milliwatt (dBm). mW is a linear unit and dBm is a logarithmic unit. The relationship between the two is shown in the following formula. P(dBm) = 10 Log(P(mW)/ 1 mW)
Out-of-band Network Management	Out-of-band network management is the communication of network management information between the network management system and the equipment through another network management network independent of the business network.
P	
Packet Switching	The data transmitted by the user is divided into multiple data segments. The data segments are encapsulated with control information such as the destination address to form packets. The packets are transmitted to the destination in the network in a store-and-forward manner. This process is called packet switching.
Polling	Polling can periodically detect whether a device is offline .
Protection Switching	Protection switching is a characteristic of the transmission entity, which can transfer data on a failed device or failed link to another device or link. This characteristic is bidirectional. In the ring network, M protection channels are established for N working channels , and 1 <= M <= N. When a working channel to be protected appears between network nodes in the ring network , the short path or long path of one of the M protection channels between the network nodes is determined to protect the working channel to be protected through the use of the protection channel stored locally and the signaling transmission of the protocol.
Q	
QoS	A network security mechanism is a technology used to solve network delay and congestion problems . When the network is overloaded or congested, QoS It can ensure that important services are not delayed or discarded, while ensuring efficient operation of the network.
R	
Resource	The management objects in the network management system include equipment, chassis,

	boards, ports , etc.
S	
Single Mode Fiber	light in the same optical fiber .
SNMP	By IETF To solve the Internet SNMP is a set of network management protocols proposed to solve the problem of network device management in TCP/IP networks. SNMP enables a network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configuration, receiving network event alarms, etc. It is currently the most widely used network management protocol in TCP/IP networks.
Subnet	A subnet is a logical division of the network topology in the system, which helps to clearly display the topology of network elements in the system. Topological nodes such as networks, network elements, symbols, links, etc.
Symbol	Symbols are schematic topological nodes that cannot be managed, but can better display the structure in the network.
Synchronization	The network management system can update the device resources or alarm information in the database through synchronization. information to keep the network management system consistent with the equipment.
T	
TDM	A technology for transmitting multiple digitized data, voice, and video signals simultaneously over the same communications medium by interleaving bit pulses in different channels or time slots.
Timeslot	Divide time into periodic frames, and each frame is divided into several time slots. A time slot is a communication channel assigned to a user .
Topology	The graphical network structure in the network management system intuitively displays the networking status, sub- Alarms and online status of networks or network elements .
Trap	The device sends alarm information to the network management system through SNMP The message is reported to the network management system .
Trap Inhibit	The device only reports the root alarm, and the suppressed derivative alarms are not reported to the network management system .
U	
Universal Asynchronous Receiver/Transmitter	UART It is a universal asynchronous receive / transmit serial bus that works at the data link layer and is used to control the communication between computers and serial devices. It includes RS 232 , RS 422 and RS 485 Interface standards and bus standards. The UART 's sending logic converts data from parallel to serial, and the receiving logic converts data from serial to parallel. At a sufficiently high system clock rate , the UART cangenerate all standard baud rates, control data transmission and reception , and interrupt control when an exception occurs .

User	The collection of management domains and operation permissions of network management system client users, users and their user groups determines the system functions that users can use .
V	
Virtual Local Area Network	It is a protocol proposed to solve the broadcast problem and security of Ethernet. It is a Layer 2 isolation technology that divides the devices in the local area network into segments logically rather than physically, thereby realizing multiple virtual workgroups that do not affect each other .

7.3. Abbreviations

A	
AC	Alternating Current
AIS	Alarm Indication Signal
ALS	Automatic Laser Shutdown
APS	Automatic Protection Switching
ATM	Asynchronous Transfer Mode
C	
CBS	Committed Burst Size
CC	Continuity Check
CCM	Continuity Check Message
CE	Customer Edge
CFM	Connectivity Fault Management
CIR	Committed Information Rate
CRC	Cyclic Redundancy Check
D	
DCN	Data Communication Network
DHCP	Dynamic Host Configuration Protocol
DoS	Deny of Service
E	
EBS	Excess Burst Size
EFM	Ethernet in the First Mile
EIR	Excess Information Rate
E- Line	Ethernet- Line
EPL	Ethernet Private Line
EVPL	Ethernet Virtual Private Line
FDDI	Fiber Distributed Data Interface
F	
FE	Fast Ethernet
FEC	Forwarding Error Correction
FM	Fault Management
FR	Frame Relay

FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
H	
HTTP	Hyper Text Transfer Protocol
I	
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU- T	International Telecommunications Union-Telecommunication Standardization Sector
L	
L2VPN	Layer 2 Virtual Private Network
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LB	Loop Back
LBM	LoopBack Message
LBR	LoopBack Reply
LC	Little Connector
LER	Label Edge Router
LLDP	Link Layer Discovery Protocol
LLDPDU	ink Layer Discovery Protocol Data Unit
LSP	Label Switched Path
LSR	Lable Switching Router
LT	Link Trace
LTM	LinkTrace Message
LTR	LinkTrace Reply
M	
MA	Maintenance Association
MAC	Medium Access Control
MD	Maintenance Domain
MEG	Maintenance Entity Group
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MP	Maintenance Point
MPLS	Multi Protocol Label Switching

MPLS-TP	Multi-Protocol Label Switching in Transport Networks
MTU	Maximum Transmission Unit
N	
NAPT	Network Address Port Translation
NAT	Network Address Translator
NNI	Network to Network Interface
O	
OAM	Operation Administration and Maintenance
OAMPDU	OAM Protocol Data Units
OTN	Optical Transport Network
P	
PC	Personal Computer
PDU	Protocol Data Unit
PE	Provider Edge
PHB	Per-Hop Behaviour
PHP	Penultimate Hop Popping
PPP	Point to Point Protocol
PTN	Packet Transport Network
PW	Pseudo Wire
PWE 3	Pseudo Wire Emulation Edge-to-Edge
Q	
QoS	Quality of Service
RIP	Routing Information Protocol
R	
RMEP	Remote Maintenance association End Point
S	
SC	Square Connector
SD	Signal Detect
SF	Signal Fail
SFP	Small Form-factor Pluggable
SFP+	Enhanced Small Form Factor Pluggable
SNCP	Sub-Network Connection Protection
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SSH	Secure Shell
SSHv2	Secure Shell version 2

STP	Spanning Tree Protocol
T	
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TDP	Transmitter and Dispersion Penalty
TLV	Type
TPID	Tag Protocol Identifier
TTL	Time to Live
UDP	User Datagram Protocol
U	
UNI	User Network Interface
V	
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
W	
WRR	Weight Round Robin
WTR	Wait To Restore