# M6500 Series 100G/200G Muxponder/Transponder NE Configuration Manual

# Contents

# Preface

**Overview**

| Chapter Number | Description |
|---|---|
| Preface | This chapter introduces contents, version information and explanation of special symbols. |
| Chapter 1 Preparation Before Configuration | This chapter describes the preparation work required before configuring network elements. |
| Chapter 2 Create A Network | This chapter introduces how to build a network environment. |
| Chapter 3 DCN Configuration | This chapter introduces the configuration method of DCN in band. |
| Chapter 4 NE & Board Configuration | This chapter introduces NE and board configuration instructions, configuration steps and explanation. |
| Chapter 5 Service Configuration | This chapter introduces the service configuration scheme of network element under different service types and different environments. |
| Chapter 6 Overhead Configuration | This chapter introduces the traditional overhead configuration scheme of OTN. |
| Chapter 7 SNC Protection Configuration | This chapter introduces the SNC protection configuration and the protection conditions etc. |
| Chapter 8 Alarm Management | This chapter introduces the current alarm and history alarm of NE and NMS system. |
| Chapter 9 Performance Management | This chapter introduces the current and history performance statistics of optical power, OCh, FEC, OTUk/ODUk, SDH regeneration segment and Ethernet. |
| Abbreviation | |

**Product Version**

| Product Number | Version Number |
|---|---|
| M6500 Series NMS | R6.4.23_v13530 |

**Content Introduction**

This manual mainly introduces the general operation of the network management platform, including installation and startup of the NMS system, login, exit, password change, security management, system management of network element, alarm management, log management, performance management, routine maintenance of the NMS system, common problems and so on.

**Explanation of Special Symbols**

The following symbols may appear in this manual, which respectively represent the following meanings:

| Symbol | Description |
|---|---|
| Danger | Special attention should be paid to the content. If the operation is improper, it may cause serious injury to the person. |
| Attention | It reminds the matters for attention. Improper operation may cause loss of data or damage to the device. |
| Hint | It represents the operation or information that requires special attention to ensure the success of the operation or the normal work of the device. |
| Knack | A skill or a knack which helps to solve a problem and save time. |
| Explain | The necessary supplement and explanation for the description of the text. |
| Note | Notes contain helpful suggestions or references to material not covered in the manual. |

Note

- It is not allowed to make modification if the input box or the drop-down box is grayed out.
- The add, delete, modify and refresh buttons are all on the toolbar.
- One and only one data in the table must be selected first while doing the modification operation.
- At least one data in the table must be selected while doing the deletion operation.

# 1. Preparation Before Configuration

## 1.1. Configuration Process

When configuring M6500 devices on M Series NMS system, some rules and orders must be followed.

If the whole project and its configuration are initially created, please refer to process in 1-1 to complete the operation. If the project has been created, only the configuration of one NE or single card needs to be changed, please perform the operation according to relevant content of chapters in Figure 1-1.

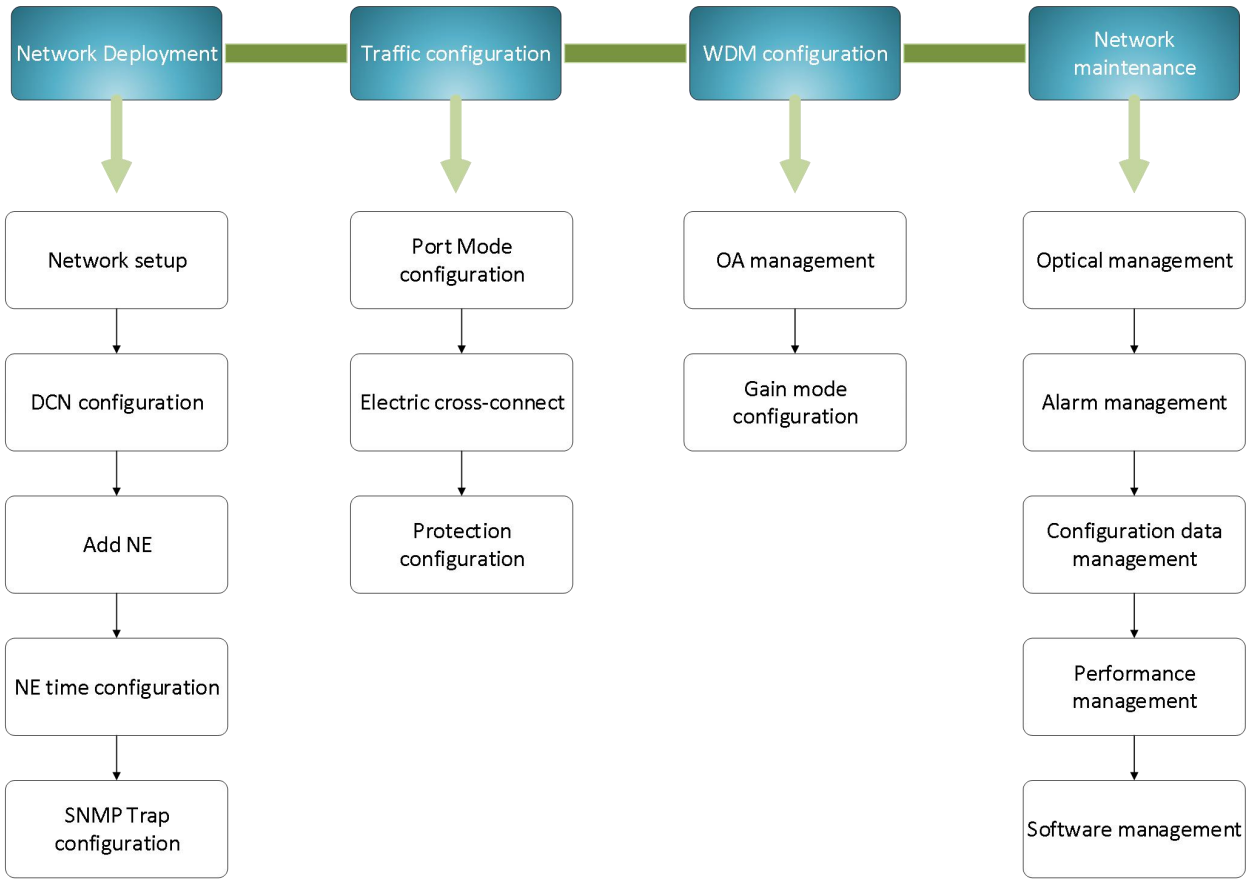



Figure 1-1 M6500 Service Configuration Process

M Series NMS system mainly contains operations such as parameter configuration of single card service, protection, in-band management as well as alarm query and performance query etc.

**Hint**

**It is recommended that the configurations of M Series NMS equipment be completed according to the sequence of operation in the flowchart.**

## 1.2. Connect NMS System & NE

For different network devices, there are multiple connection ways to connect M Series NMS network management computer and M6500 network elements. Normally the M Series NMS Server and M6500 network Element are both connected to a HUB by direct connection network cable. But the M Series NMS Server can also

be directly connected to M6500 network element's management port through twisted pair cable or direct connection network cable.

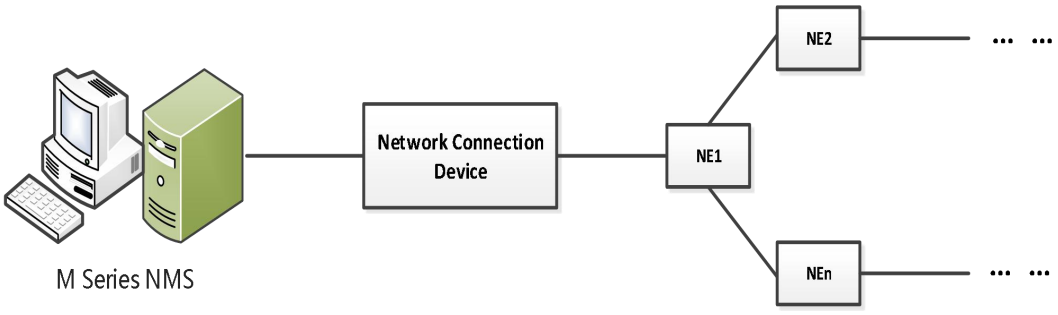



Figure 1-2 Connection Schematic Diagram of Network Management System and Network Elements

**Prerequisite**

The deployment of network cables between the NMS system and NE has been completed.

**Steps**

Here we take the connection mode of "cable+HUB" direct-connect network as an example to introduce the steps to connect the NMS system and the network elements:

- Turn on the network management computer and take a network cable to connect one end to the network card interface of the host computer, and connect the other end to the Ethernet port of HUB.
- Take another network cable and connect one end to the Ethernet port of HUB and connect the other end to MGMT1/MGM2 of NMU board for M Series NMS equipment.
- Check on the network management computer to see if the network cable is connected to a device network card; if not, connect the network cable to another network card of the network management computer.

# 1.3. Start Network Management Service

**Prerequisite**

Ensure that the M Series NMS system has been installed on the network management host.

## 1.3.1. Start Server Program

Double click on "NMS Server" 

on the network management computer, the"NMS"server window pops up. Then double click on"Start NMS Server", as shown in Figure 1-3:

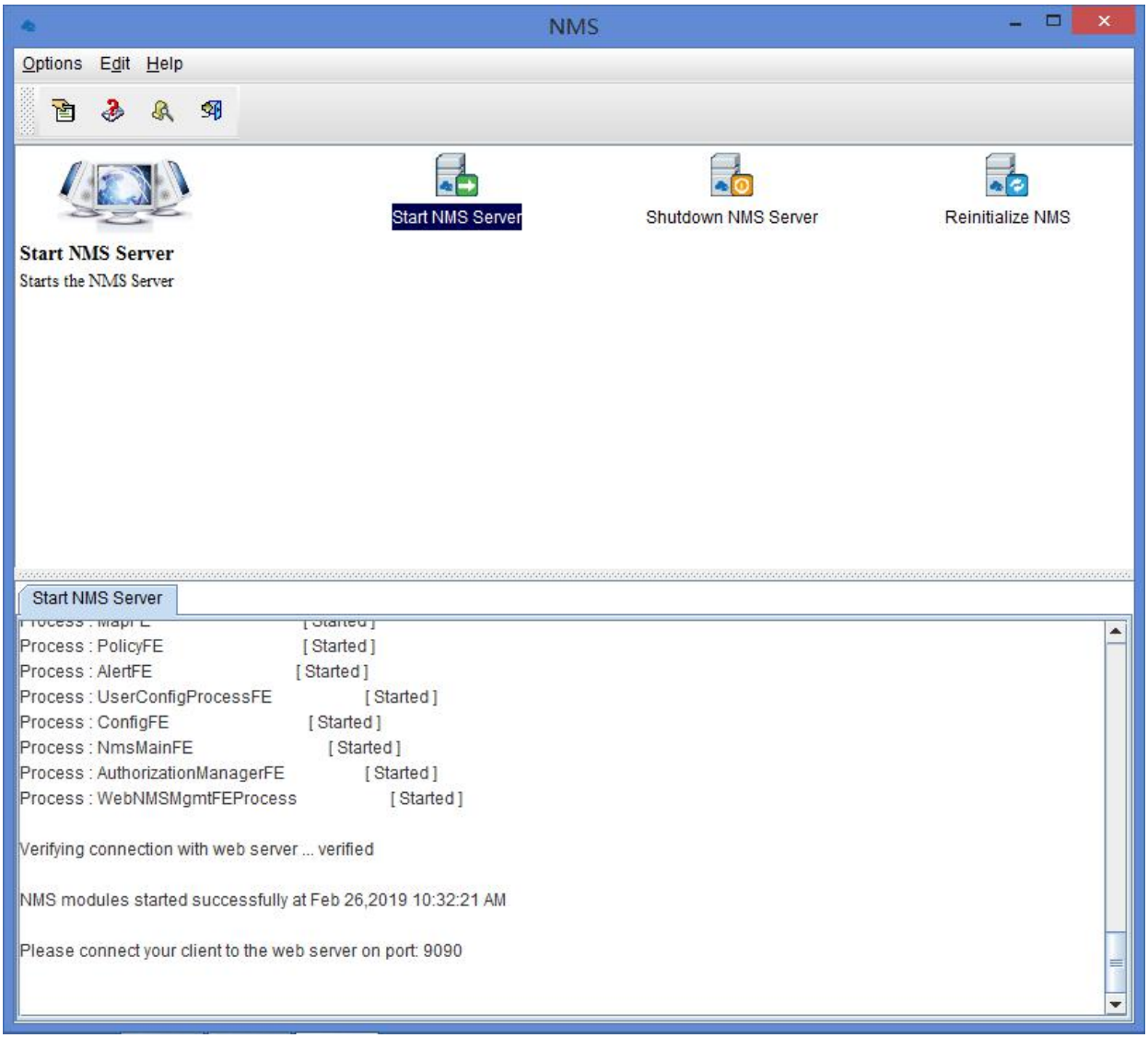



Figure 1-3 Start NMS Server

# 2. Create Network

Create network topology, that is, create corresponding network model of actual project according to the configuration of actual engineering (such as networking, single site configuration etc.), so as to realize the monitoring of devices.

Before creating a network topology, operators need to know the relevant engineering configuration files, including:

- Information such as the NE type and single card configuration of each site.
- Network topology of engineering.
- Service scheduling and protection scheme.

If an operator only needs to add a network element to an existing project, he only needs to know the location and topological connection of the network element in the actual network.

It will introduce the creation steps of the network topology according to the configuration process in the following passage. Moreover, it will focus on the parameter configuration related to M6500in each step, and only the sections of the reference book will be provided for the common configuration steps for each device. M Series NMS related software was pre-installed when the network management host was manufactured. When the network management host was turned on, the network topology could be created according to the configuration process. This chapter includes the following content:

- Create Network Flow
- Login NMS Interface
- Create Nodes
- Add NE
- Establish Network Element connection
- Management of Network Elements
- Check Configuration Data
- Save Configuration Data

## 2.1. Network Creation Process

The topology of subnet, network element and fiber cable can be created in M Series NMS. Network element data can be configured.The single board parameters can be checked or modified, and further the subnet, network element or fiber cable can be managed by M Series NMS.

To create network, you can take the following process as reference:

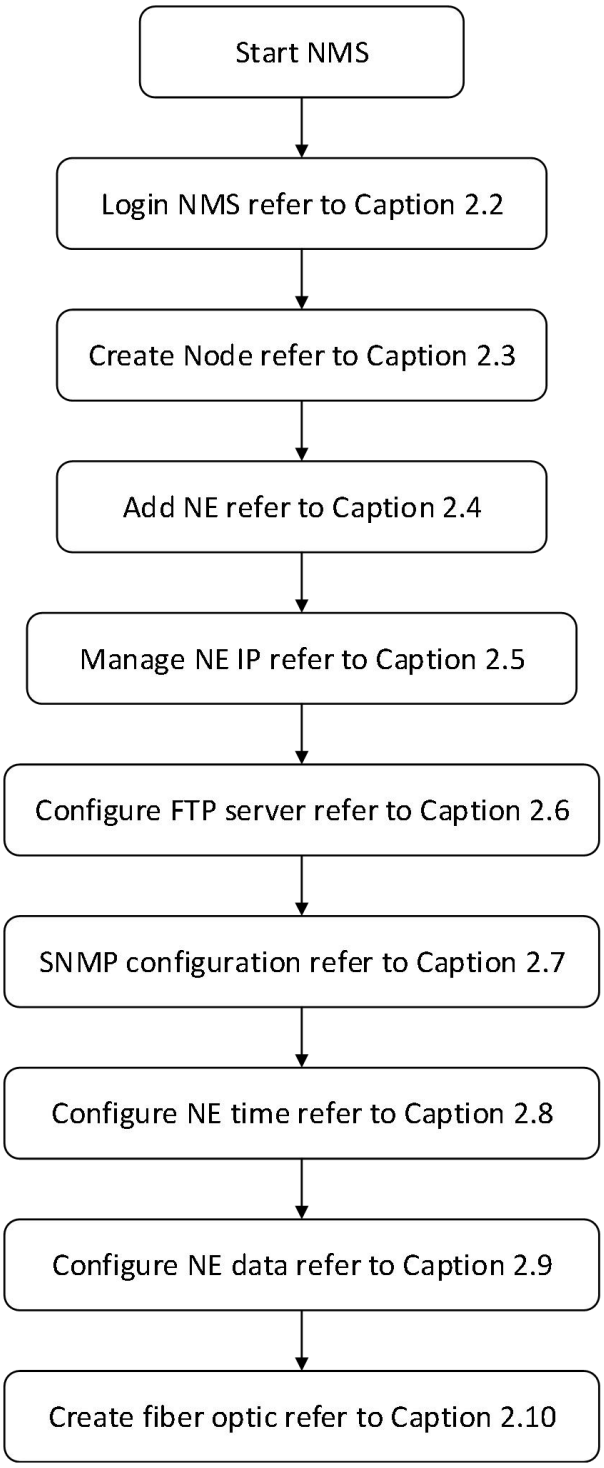



Figure2-1 Flow Chart of Create Network Topology

## 2.2. Login NMS Interface

**Prerequisite**

The installation of NMS system is completed, and NMS server has been started.

***Steps***

Open Google Chrome and type in the address bar the following network address:

1. Network management host: localhost:9090
2. Remote network management server: xxx.xxx.xxx.xxx:9090.

Enter your user name and password to login. Default user name:root  Default password:public

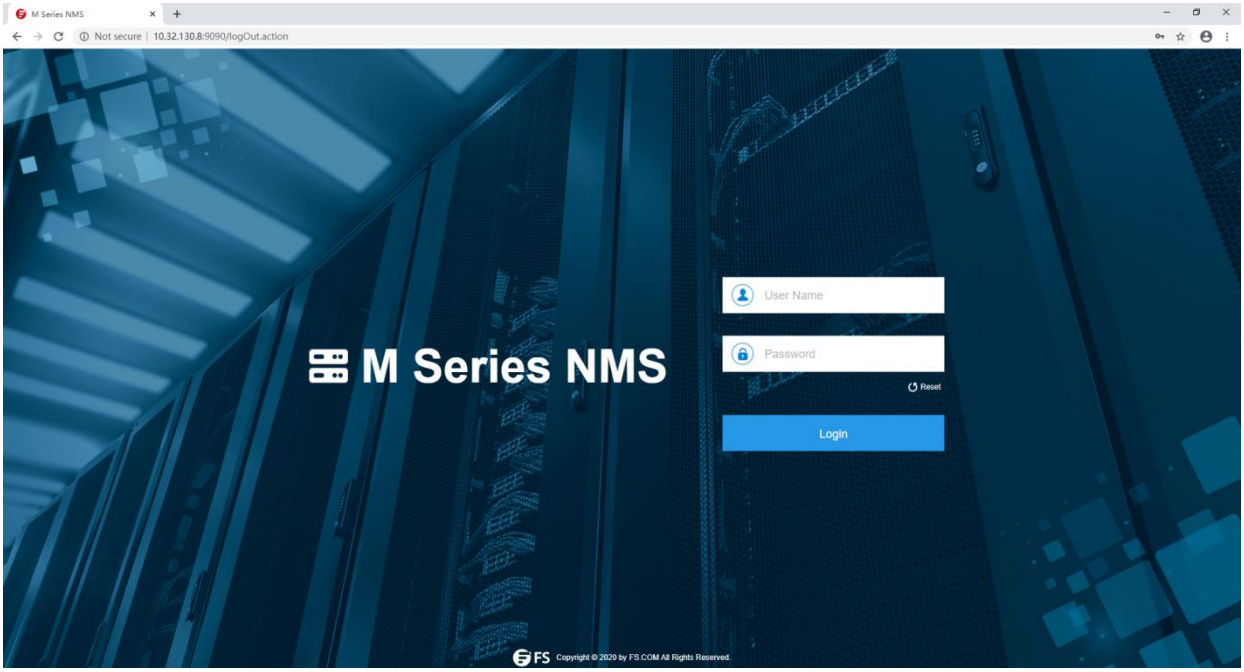



Figure2-2 Login NMS System

## 2.3. Create Groups

***Steps to add a group:***

1. Click on"*Global View*", and select"*Group Configuration*"on the right;
2. Enter the node name and description information in the"*Add Group*"module. The description information can be blank.
3. Click on"*Apply*" to save the new group information.

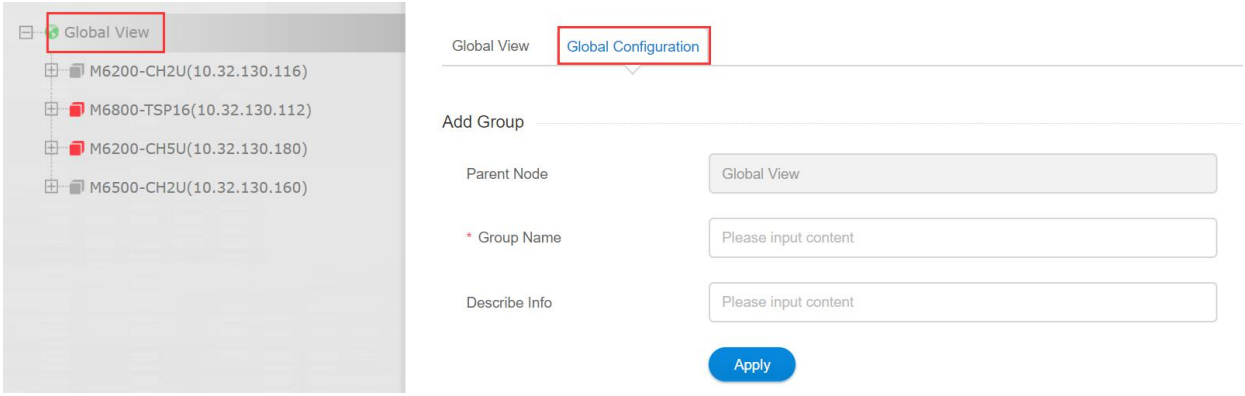



Figure2-3 Add a Group

***Steps to add a child group:***

1. Click on the created group;
2. Click on"*Group Configuration*"on the right to continue adding a child group;
3. Enter the name of the child group in the"*Add Group*"module;
4. Click on"*Apply*"to add a child group.

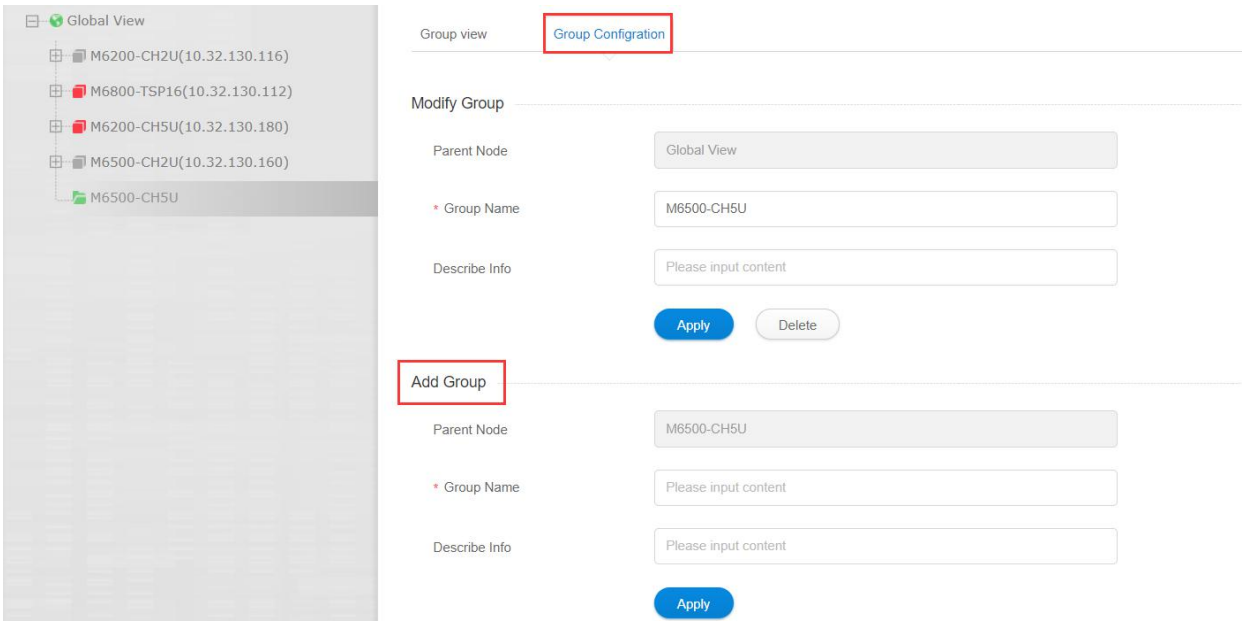



Figure2-4 Add a Child Group

# 2.4. Add NE

## 2.4.1. Add NE

***Steps:***

1. Click on the group which has been added, and select "*Group Configuration*"on the right;
2. Input the NE name, NE IP address, subnet mask, Trap host name, Trap host IP address in the"*Add NE*"module;
3. Click on"*Apply*" to save the configuration.

**Note** *: The trap host IP address is the network management server IP address.*

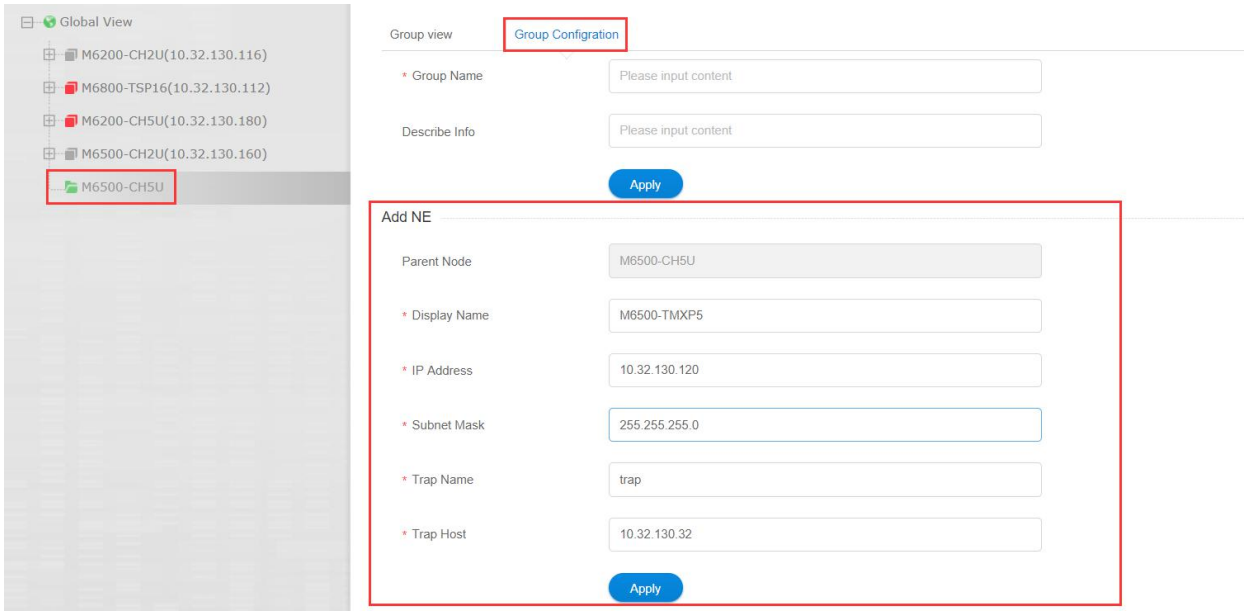



Figure2-5 Add NE

### 2.4.2. Modify NE

***Steps:***

1. Click on the NE which has been added and select"*Group Configuration*"on the right;
2. Modify the"*Modify Group*"module .

**Note** : Only the display name of the network element can be modified here.

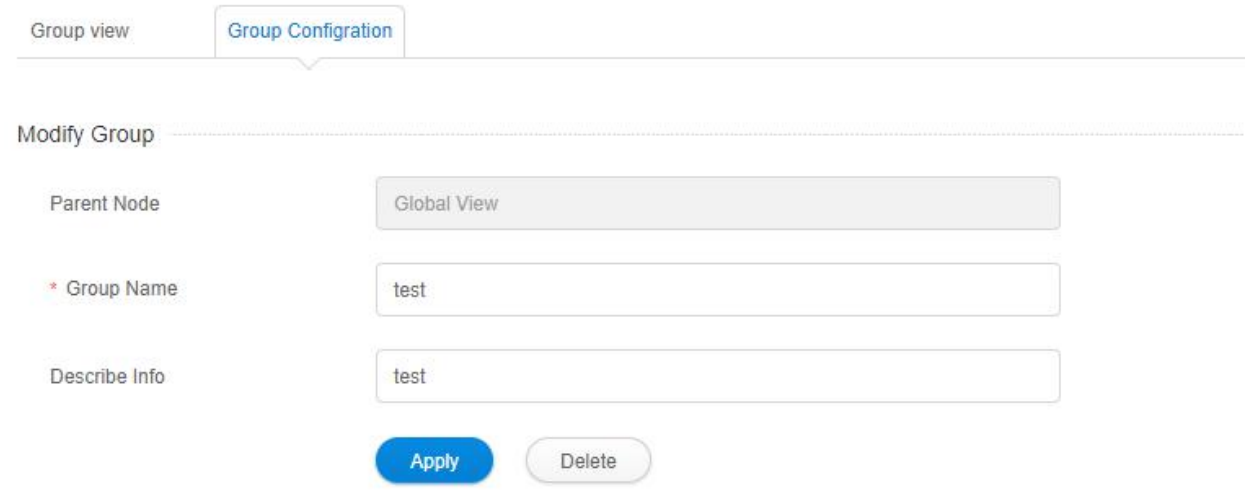



Figure2-6 Modify NE

### 2.4.3. Delete NE

***Steps:***

1. Click on the NE which has been added;and select"*Group Configuration*"on the right;
2. Click on"*Delete*"in the"*Modify Group*"module.

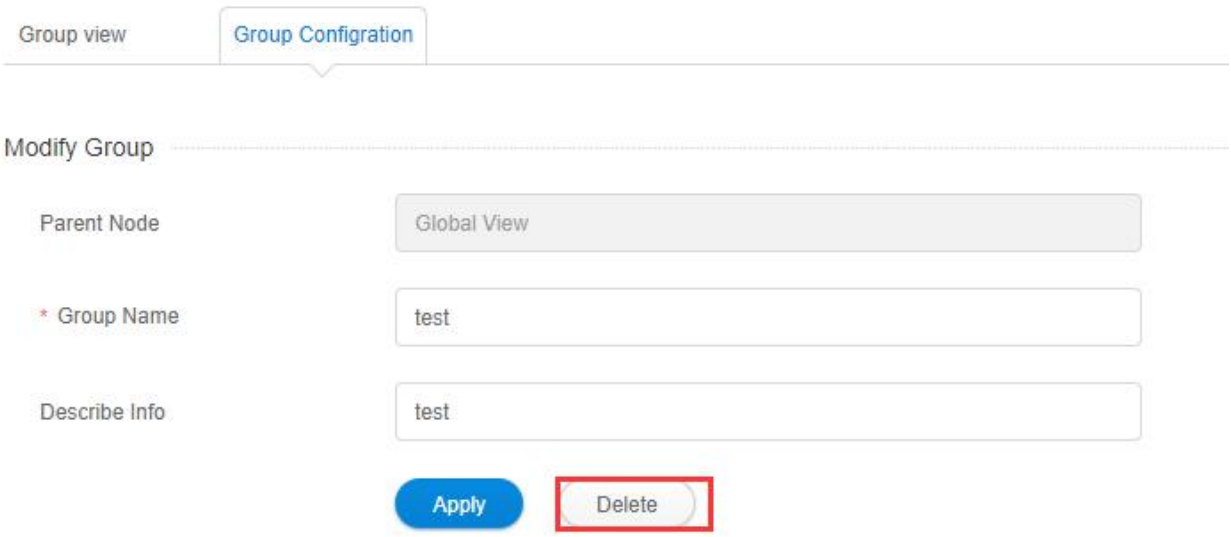



Figure2-7 Delete NE

### 2.4.4. Add a Line-card

***Steps:***

1. Select an empty slot on the added network element;
2. Click on the empty slot; and select"*Card Mode Configuration*"module;

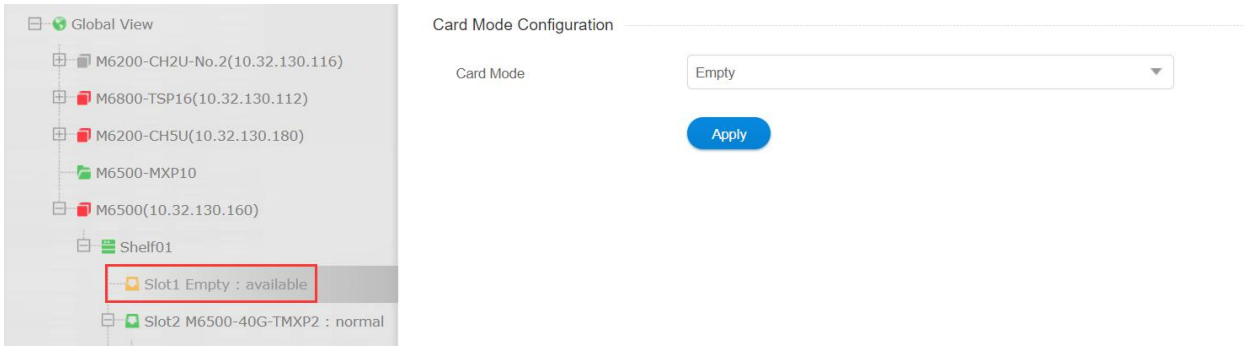



Figure2-8 Add a line-card

3. Select the card mode in the list;

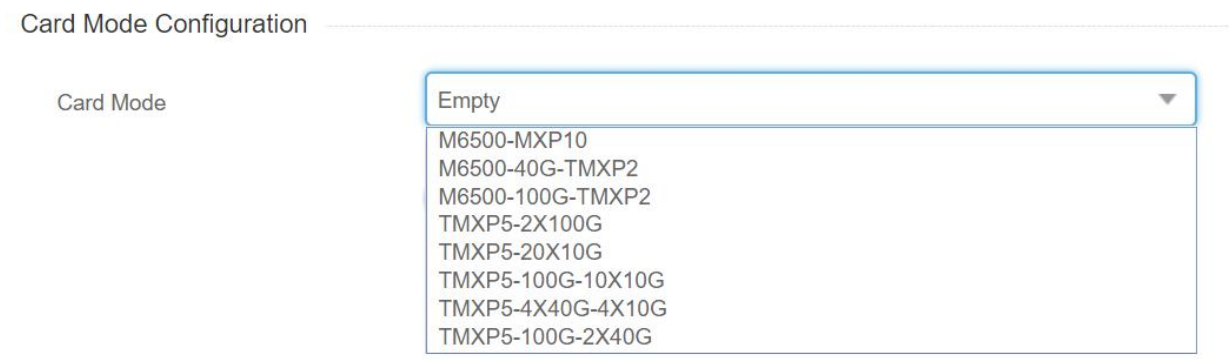



Figure2-9 Select a Card Mode

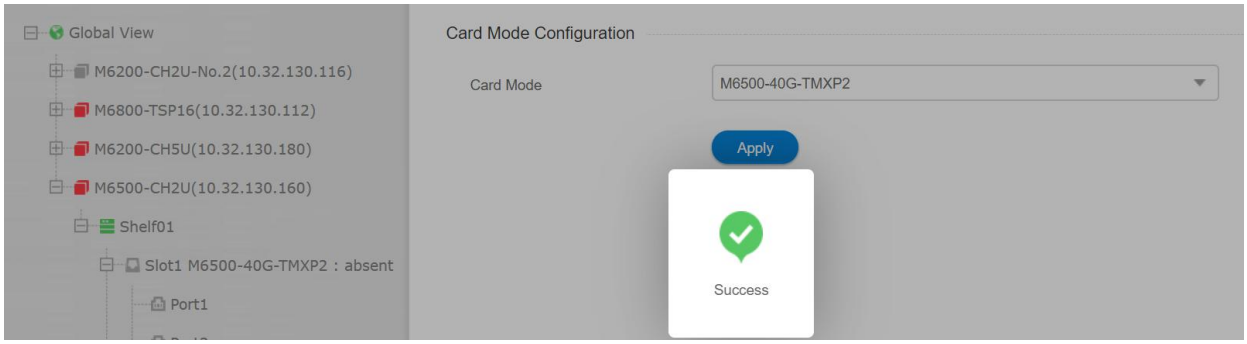
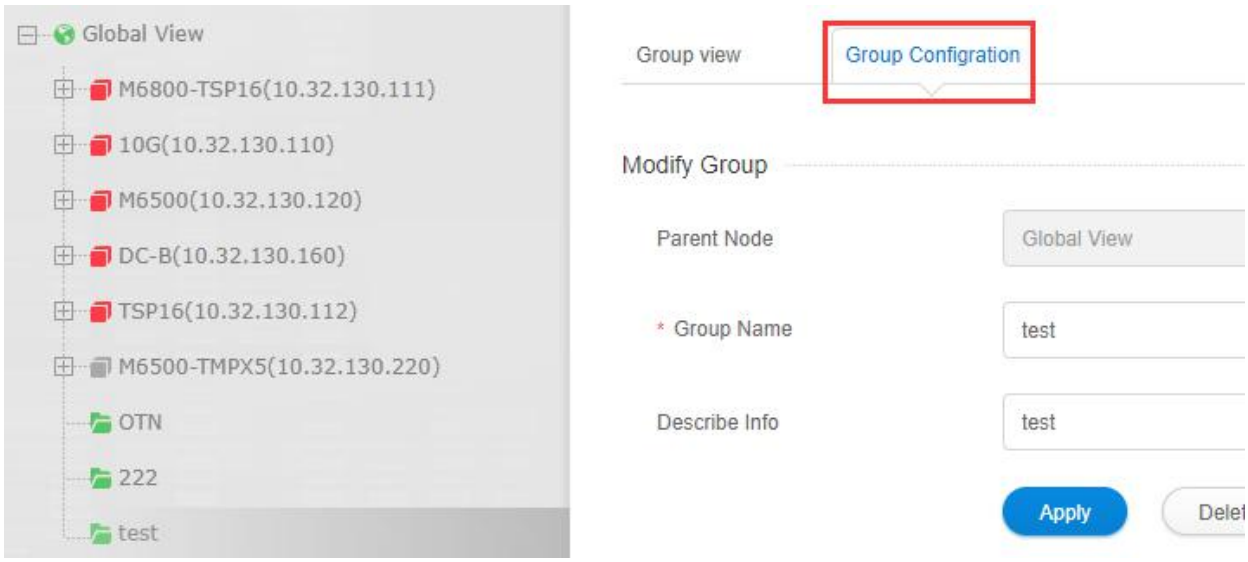



Figure2-10 Add a line-card successfully

## 2.4.5. Delete a Line-card

**Prerequisite**

**The line-card to be deleted has no single-board crossover or cross-board crossover services, otherwise it cannot be deleted.**




***Steps:***

1. Click on the line-card and select"*Delete Card*"module on the right;
2. Click on"*Delete*".

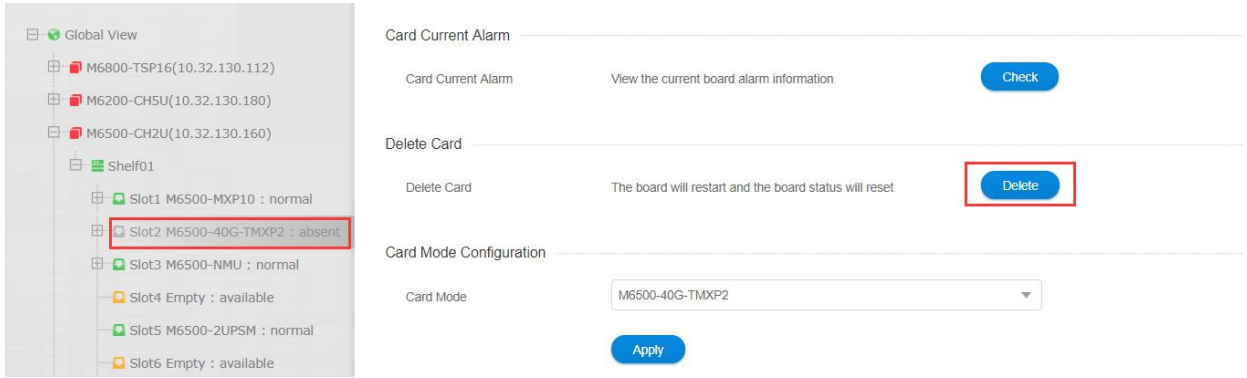



Figure2-11 Delete a line-card

**Attention**

1. **Users can only add line-card in the slots in available state.**
2. **Users can only delete line-card whose slot status is absent.**

# 2.5. NE IP Address Management

There are three types of NE IP address:

| Name | Description | Note |
|---|---|---|
| Node IP address | In-band management IP address | Suitable for DCN transmission |
| IP1/IP2 address | Out-band management IP address | Can be modified by the client |
| Local NMS IP address | default IP address, 192.168.126.2 | |

Use of DCN: The NMS system of the transmission products will manage thousands of network elements in most cases. Using this technology, all network elements can be managed by one or several access network elements.

## 2.5.1. Node IP Configuration

***Steps:***

1. Click on the NE which has been added;
2. Click on"*MGMT IP Configuration*"on the right;


Figure2-12 Manage IP Configuration

3. Input the node IP address in the"*Add NE*"module,
4. Click on"*Apply*"to save the configuration.

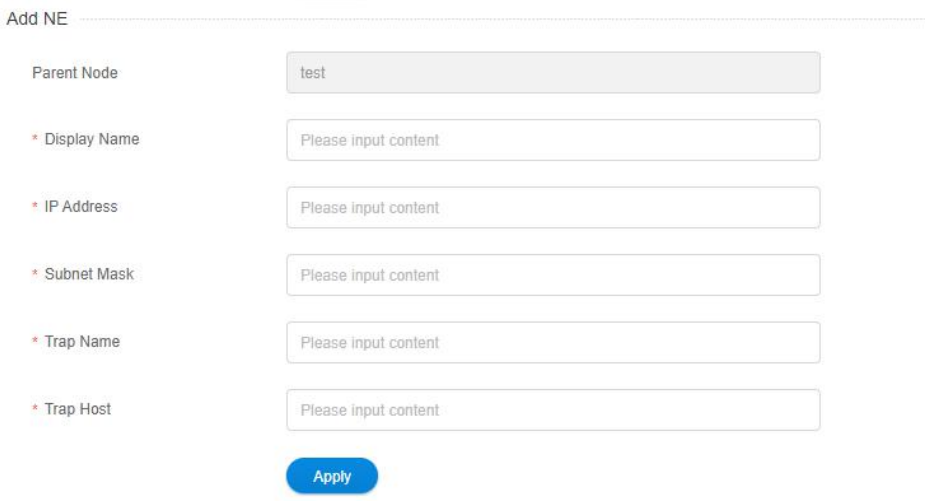


Figure2-13 Manage IP Configuration

## 2.5.2. NMS IP1 Configuration

***Steps:***

1. Click on the NE which has been added;
2. Click on"*MGMT IP Configuration*"on the right.
3. Input NMS IP1 address in the NMS IP1 (MGMT_Port1, 3, 4) box
4. Click on"*Apply*"to save the configuration.

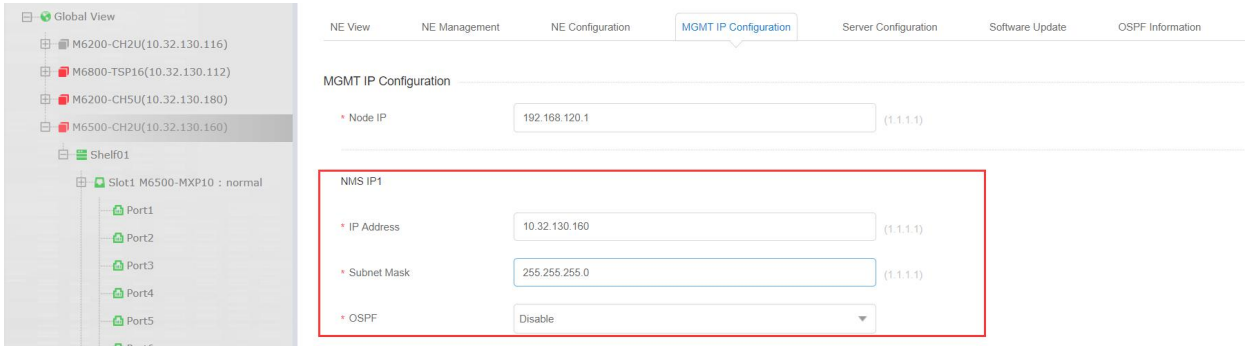



Figure2-14 NMS IP1 Configuration

## 2.5.3. NMS IP2 Configuration

***Steps:***

1. Click on the NE which has been added;
2. Click on"*MGMT IP Configuration*"on the right.
3. Input NMS IP2 address in the NMS IP1 (MGMT_Port2) box
4. Click on"*Apply*" to save the configuration.

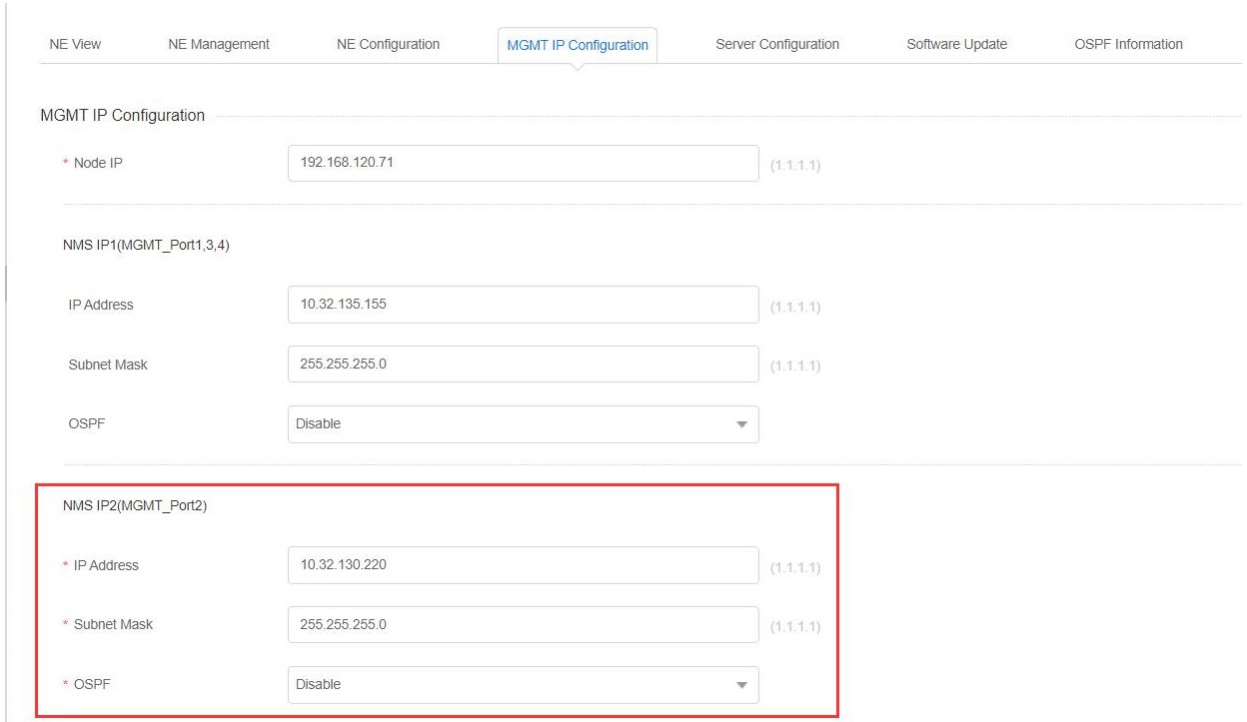


Figure2-15 NMS IP2 Configuration

### 2.5.4. Local NMS IP (LCT IP) Configuration

The default local NMS IP address is 192.168.126.1; The default Subnet Mask is 255.255.255.252.

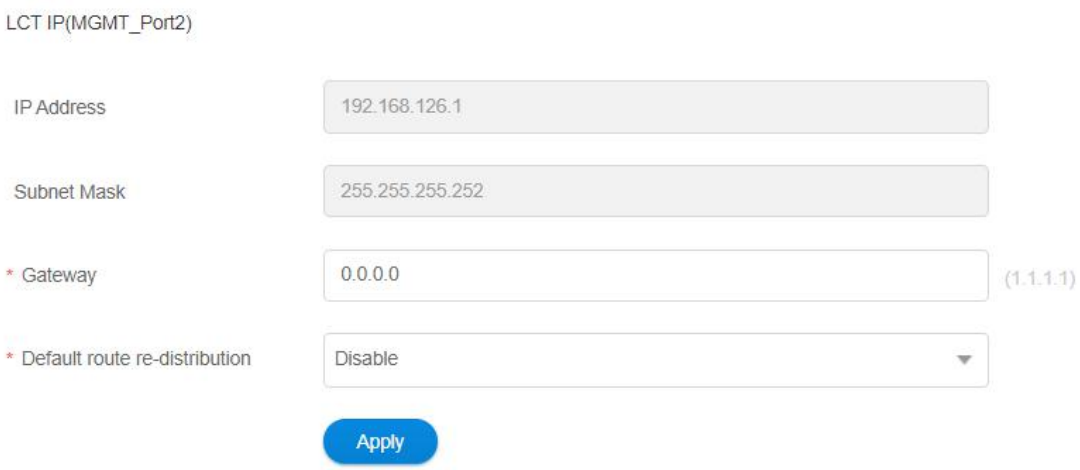



Figure2-16 Local NMS IP Configuration

### 2.5.5. Gateway Configuration

***Steps:***

1. Click on the NE which has been added;
2. Click on"*MGMT IP Configuration*"on the right;
3. Select "*Gateway*"box, input gateway IP address;
4. Click on"*Apply*"to save the configuration.

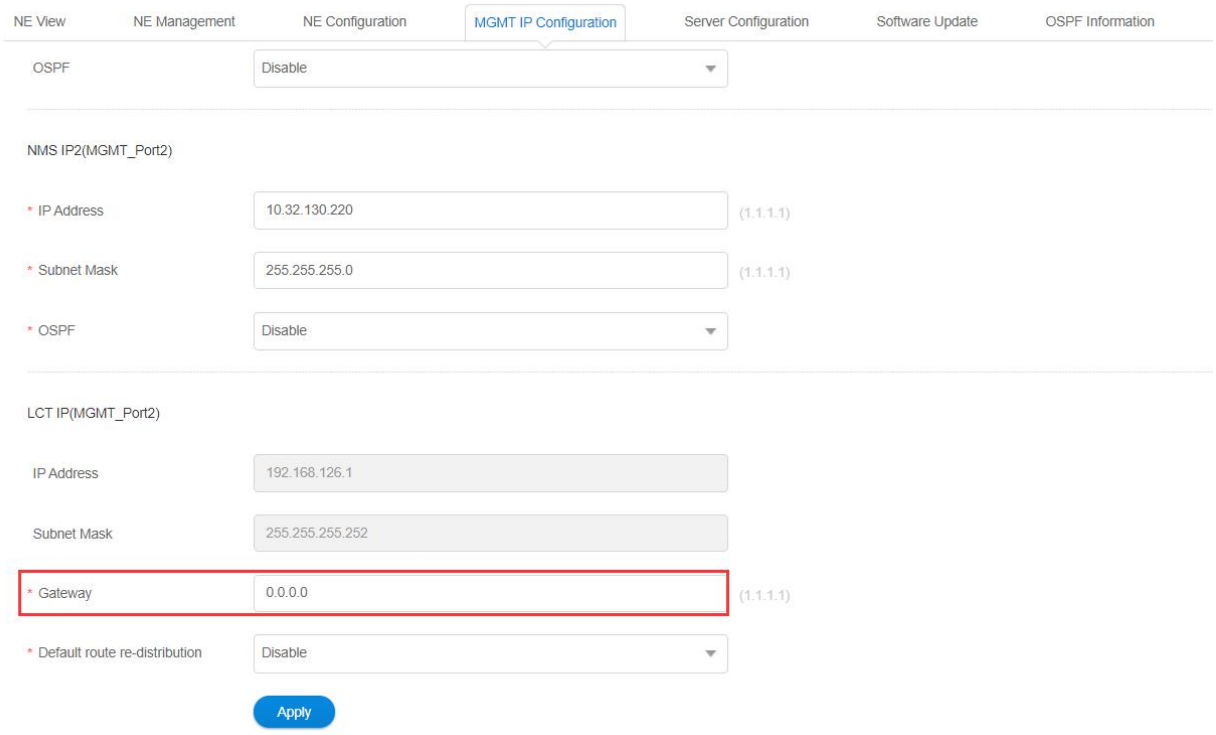



Figure2-17 Gateway Configuration

# 2.6. Configure FTP Server

In the following cases, you must configure the FTP server address:

- NE Software Upgrade
- NE Configuration Upload & Download
- NE Log Upload
- NMU/LC Card BSP Upgrade
- Performance Management

**Note**

During the use of the FTP server, one and only one server address can be configured. For different FTP servers, different FTP server addresses can be configured.

***Steps:***

1. Click on the NE which has been added;
2. Click on"*Server Configuration*"on the right;
3. Select"*FTP Server Configuration*"module;
4. Input the FTP server address;
5. Click on"*Apply*"to save the configuration.

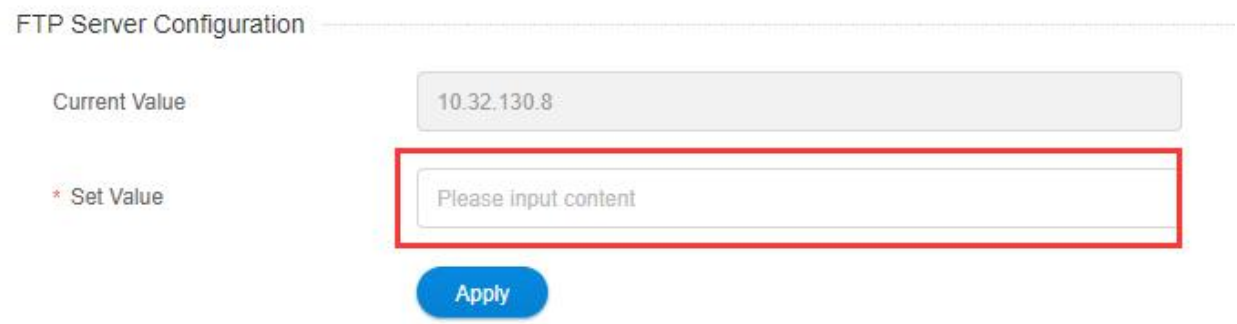



Figure2-18 FTP Server Configuration

## 2.7. SNMP Trap Configuration

***Steps:***

1. Click on the NE which has been added;
2. Click on"*Server Configuration*"on the menu bar;
3. Select"*SNMP Trap Configuration*"module ;

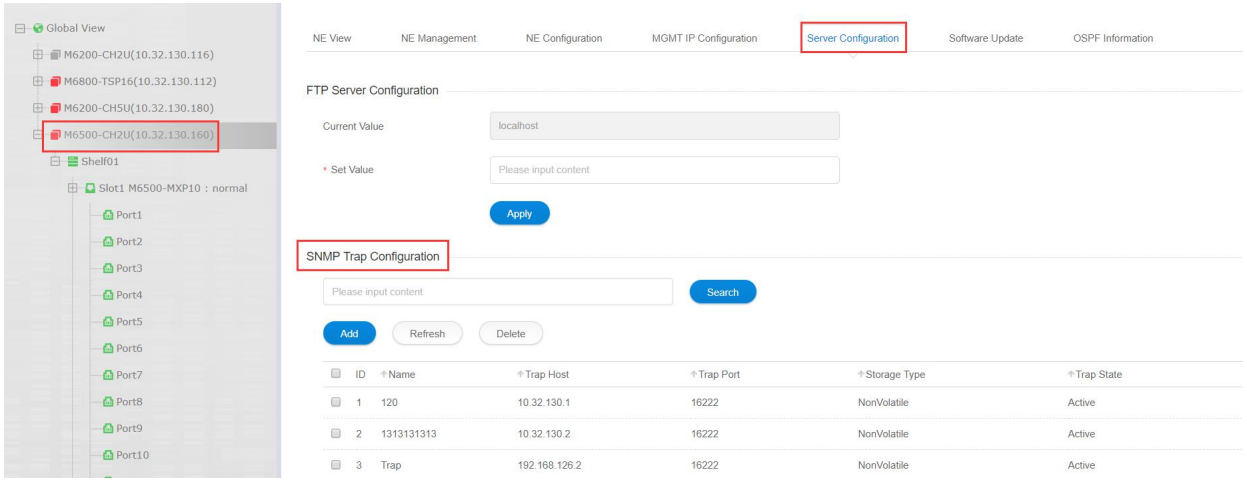



Figure2-19 SNMP Trap Configuration

4. Click on"*Add*"button to add SNMP Trap information. The default Trap Port is 16222. It is not recommended to modify it.
5. Click on"*Apply*"to save the configuration.

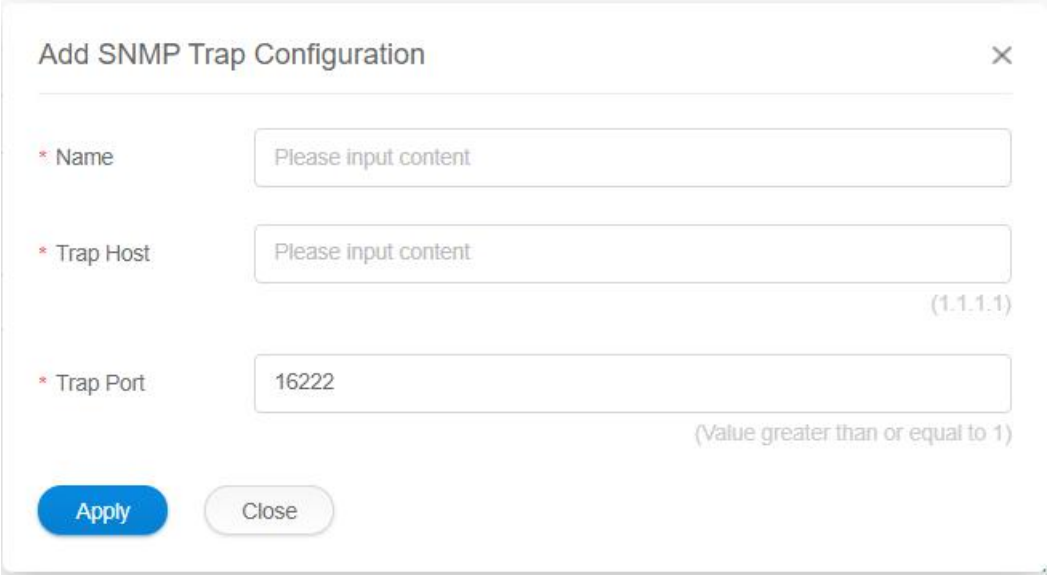



Figure2-20 Add Trap Address

**Attention**

**The newly-added Trap name or Trap IP cannot be same as that of the trap which has been added, or the add operation will fail.**

# 2.8. Configure NE Time

## 2.8.1. Configure NTP Server

Click on the NE which has been added→Click on"*Server Configuration*"on the right→Select"*NTP Configuration*"module to make relevant configuration.

***Steps:***

1. Click on the NE which has been added;
2. Click on"*Server Configuration*"on the menu bar;
3. Select"*NTP Configuration*"module to enter the configuration interface;

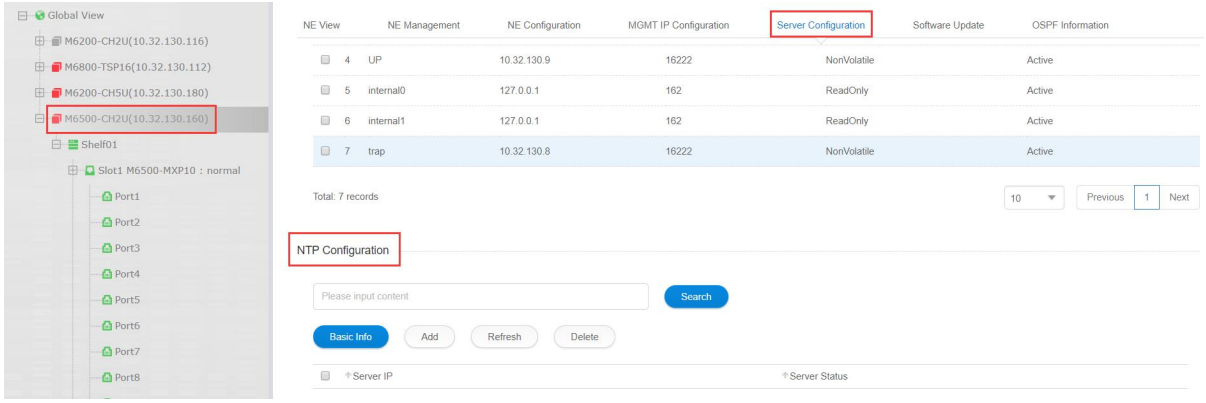



Figure2-21 NTP Configuration

4. Click on"*Add*"button and input the of NTP server IP,

5. Click on"*Apply*"to save the configuration.

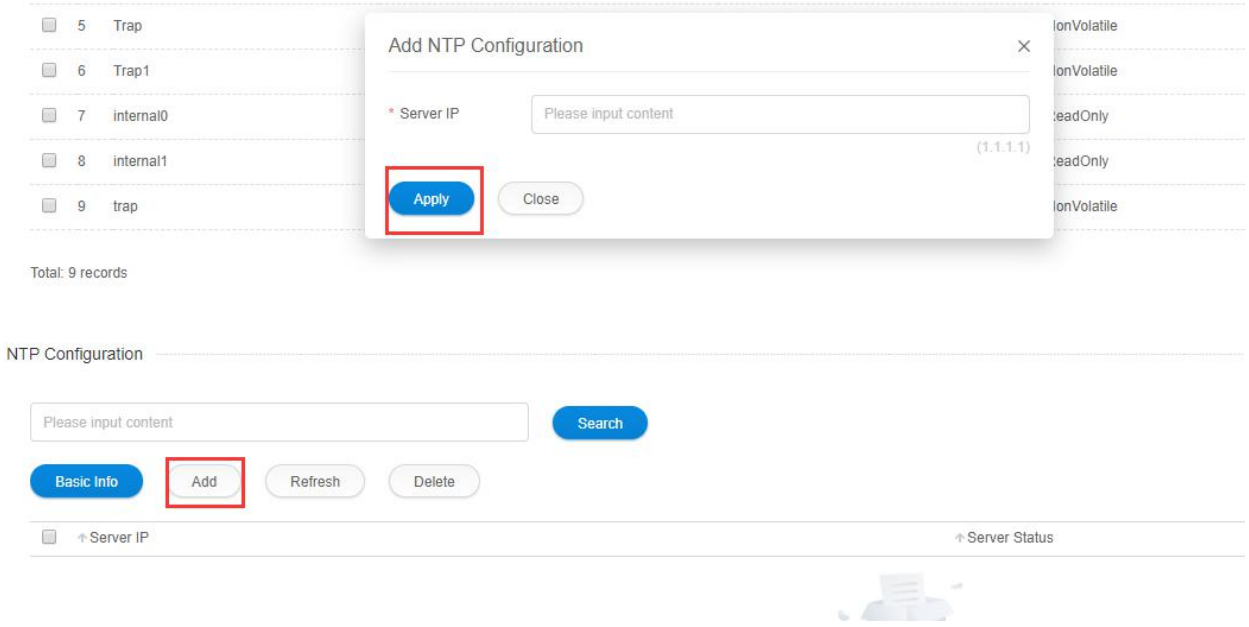



Figure2-22 NTP Server Configuration

## 2.8.2. Configure NE Time

***Steps:***

1. Click on the NE which has been added;
2. Click on"*NE Configuration*"on the right to enter the configuration interface;

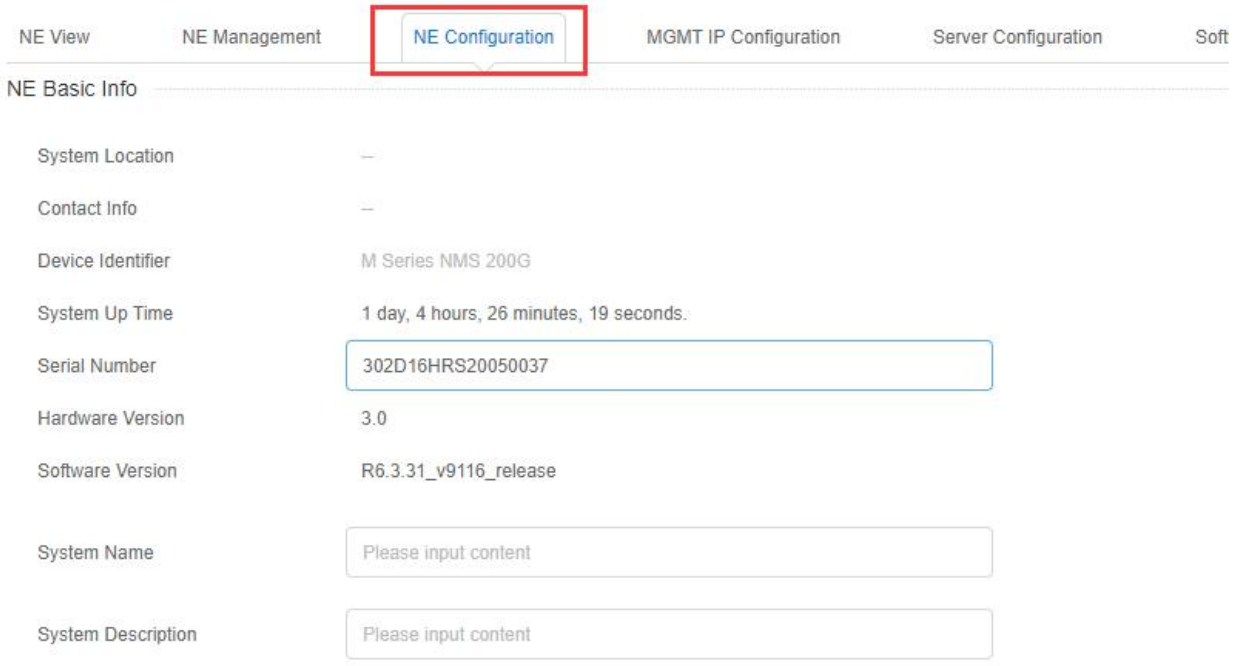



Figure2-23 NE Time Configuration

3. Configure the current time of NE,

4. Click on"*Apply*"to save the configuration.

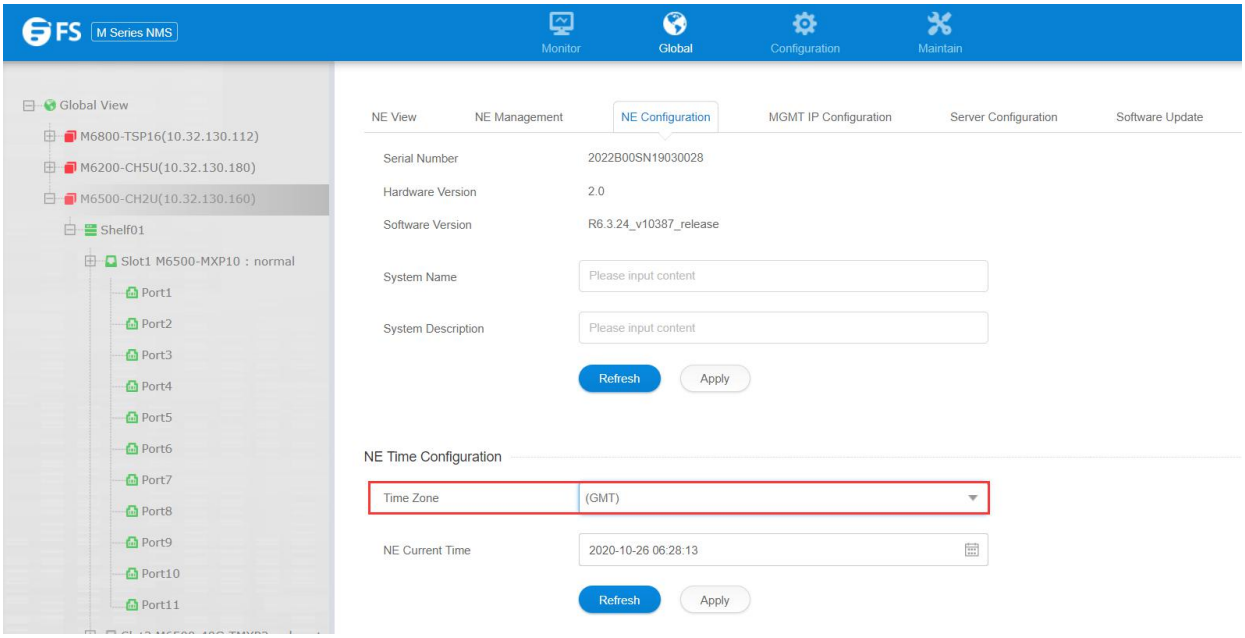



Figure2-24 NE Time configuration

# 2.9. Configure NE Data

Configure NE Data:

- Save NE Configuration: In the case of configuring the network element, in order to prevent the network element from abnormal restarting, the network element configuration is saved regularly. At present, the configuration data of the network element is automatically saved once per minute.
- Upload NE Configuration: In order to avoid data loss caused by abnormal operation, it needs to upload the NE configuration to local NMS server regularly.
- Download NE Configuration: In order to avoid the loss or modification of the original configuration caused by the abnormal operation of the network element by the engineer, the previous configuration is downloaded from the local NMS server to the network element. After it is successfully downloaded, the network element will be restarted automatically. After the restart, the configuration will be automatically saved on the network element.
- To restore NE default configuration: In the case of field debugging, various configurations of the network element have been made. After debugging, in order to prevent some of the configurations from being not restored, it needs to use this configuration to restore the network element to the factory settings.

## 2.9.1. Save NE Configuration

Click on the NE which has been added→Click on"*NE Configuration*"on the right→Select"*Configuration Data Save*"module and Click on"*Save*".

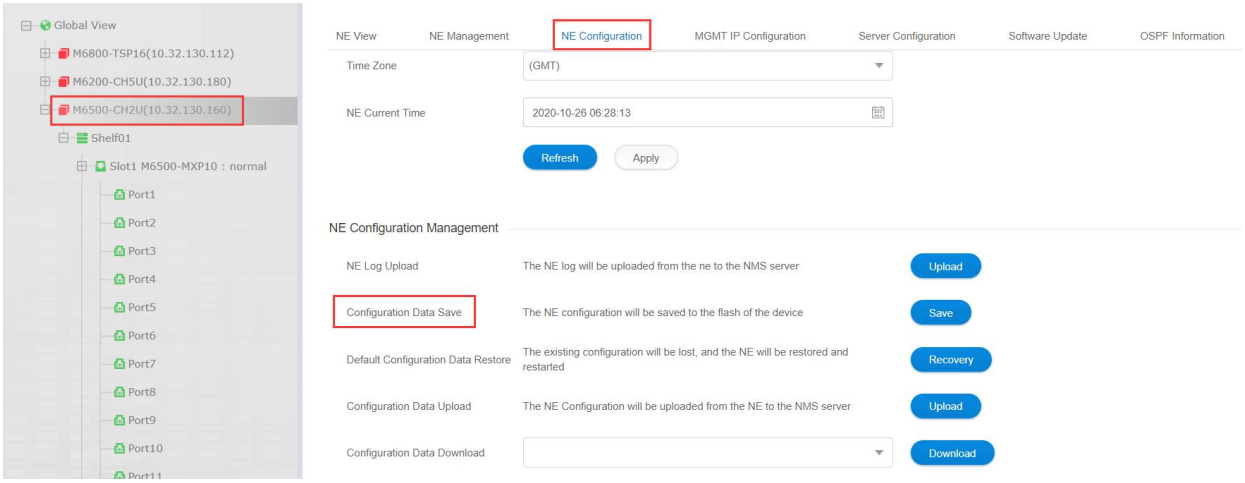



Figure2-25 Configuration Data Save

## 2.9.2. Upload NE Configuration

Click on the NE which has been added→Click on"*NE Configuration*"on the right→Click on"*Configuration Data Upload*".

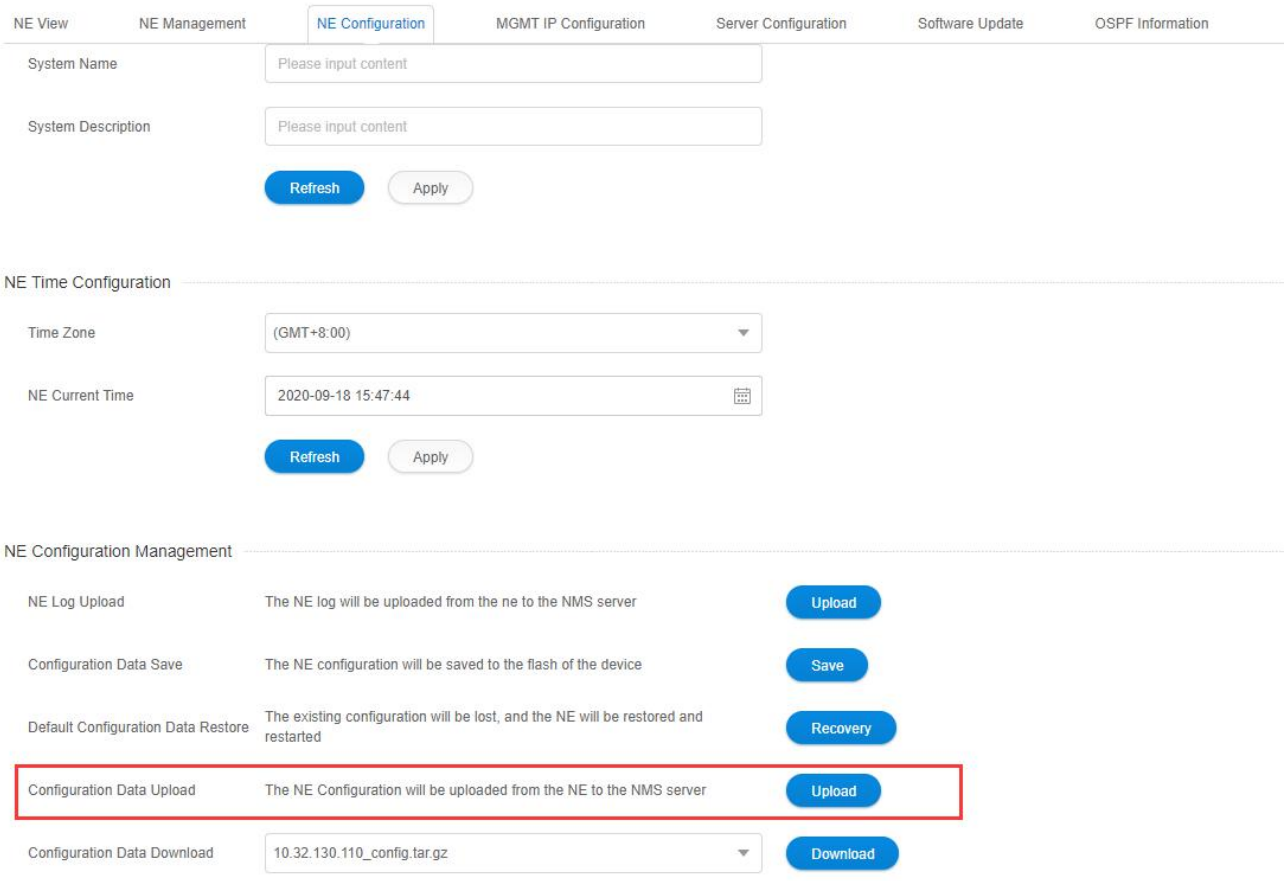



Figure2-26 Configuration Data Upload

Input the name of the configuration file which needs to be uploaded, and click on "*Upload*".

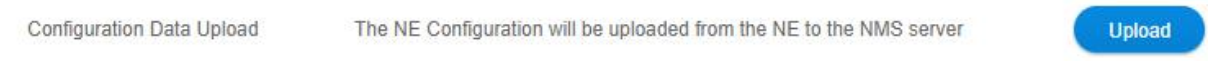


Figure2-27 Input NE Configuration File Name

The path to upload network element configuration is: the NMS installation directory → TFTP → config folder, as shown in the figure below:

### 2.9.3. Download NE Configuration

Click on the NE which has been added→Click on"*NE Configuration*"on the right→Select"*Configuration Data Download*" module.


Figure2-28 Configuration Data Download

Select the configuration file which needs to be downloaded, and click on"*Download*".

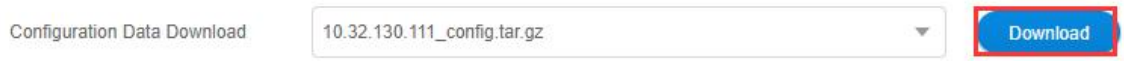



Figure2-29 Select Configuration File To Be Downloaded

### 2.9.4. Restore NE Default Configuration

Click on the NE which has been added→Click on"*NE Configuration*"on the right→Select"*Default Configuration Data Restore*" module→Click on"*Recovery*"button.

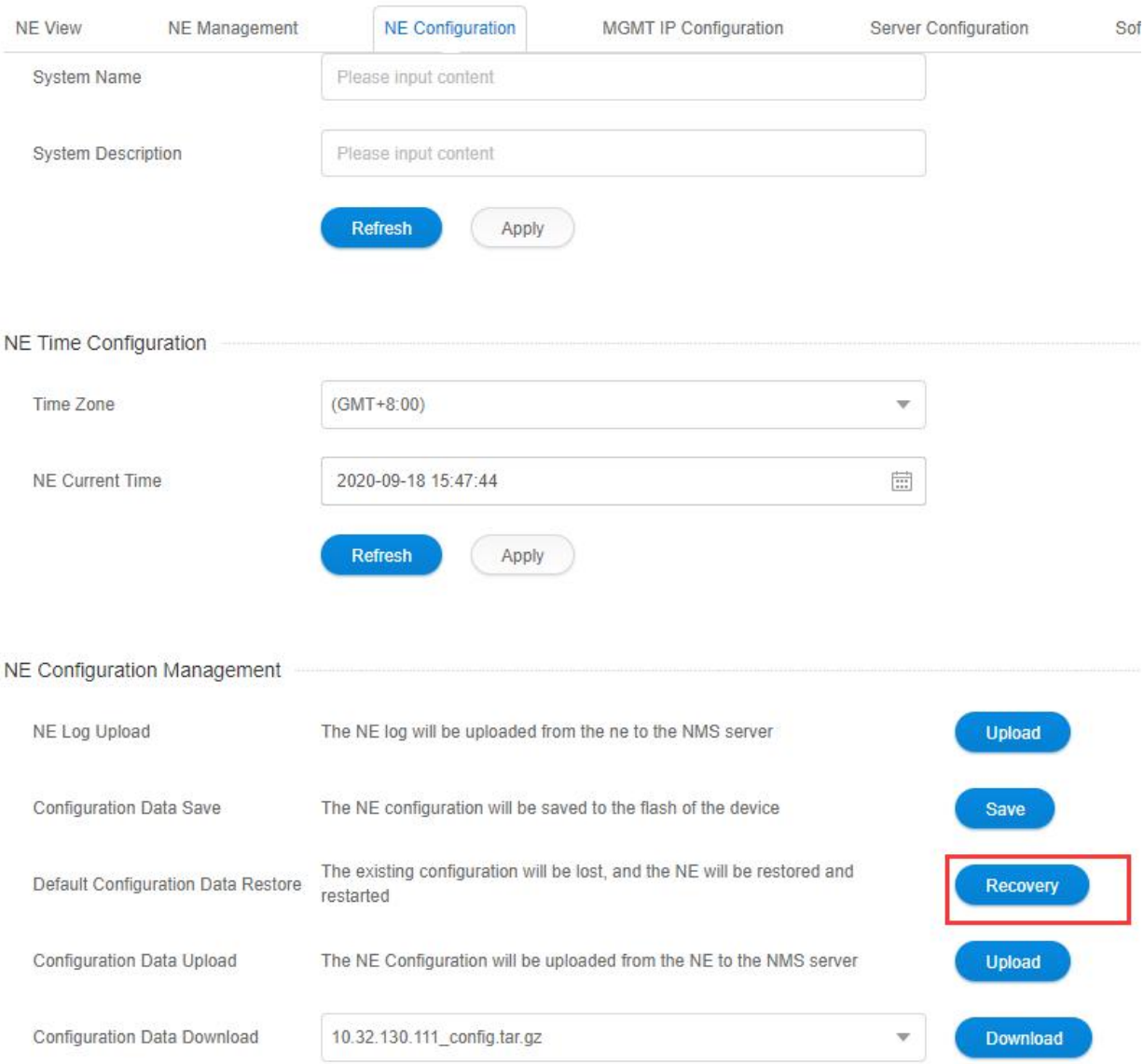



Figure2-30 Default Configuration Data Restore

# 2.10. Create Fiber Optic

## 2.10.1. Adjust NE Layout

Click on Global View, and click on NE or node in the global view and then drag it to the right place.

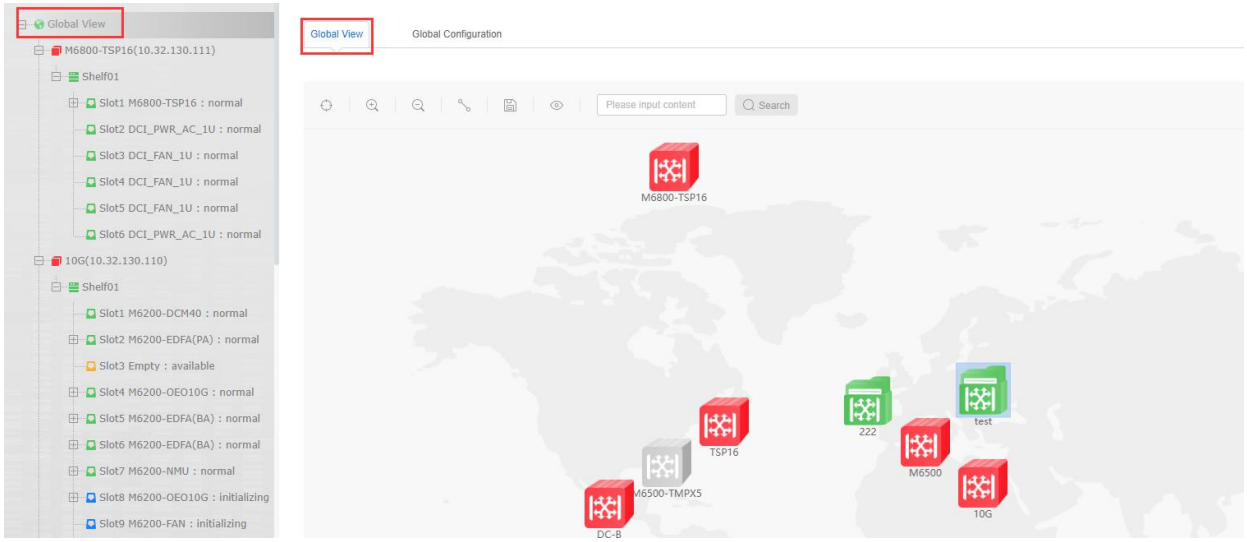



Figure2-31 Adjust NE Layout

## 2.10.2. Create Link between NEs

Click on"*Connect*"button in the global view.

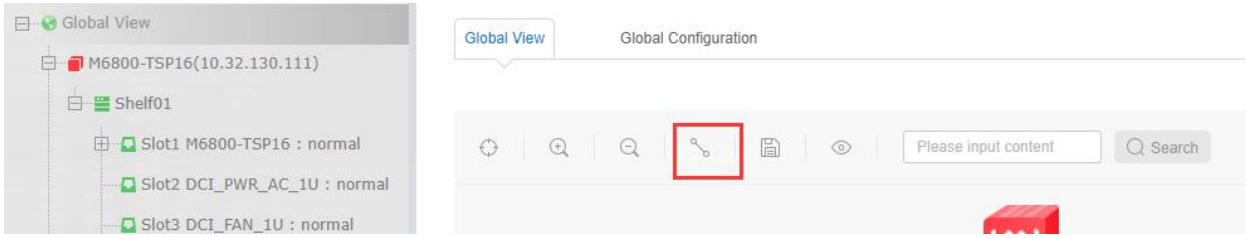



Figure2-32 Click"Connect"Button

Input name, NE IP address, shelf number, slot number and port number in the pop-up, and then click on"*Apply*".

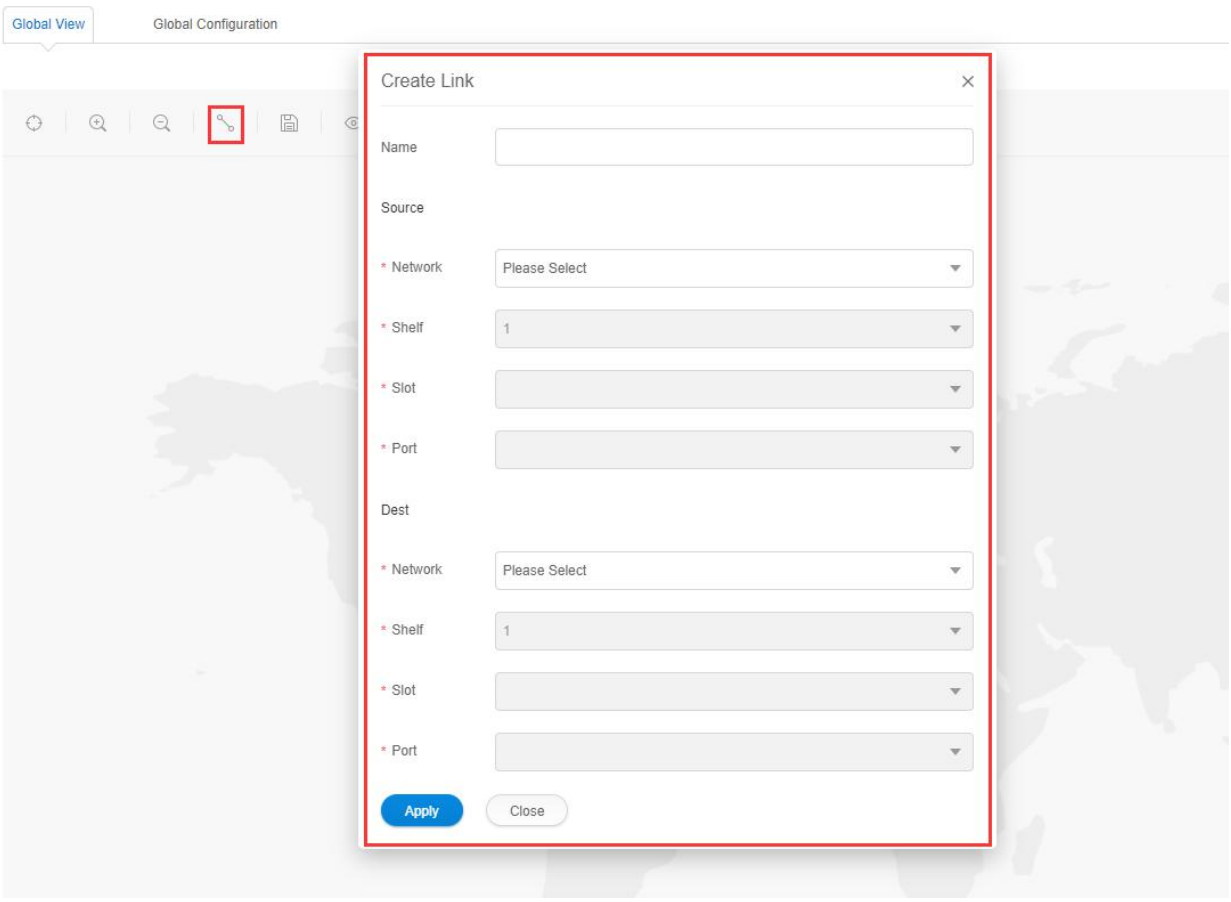



Figure2-33 Create Link between NEs

### 2.10.3. Save Layout

Click on"*Save*"button in the global view.

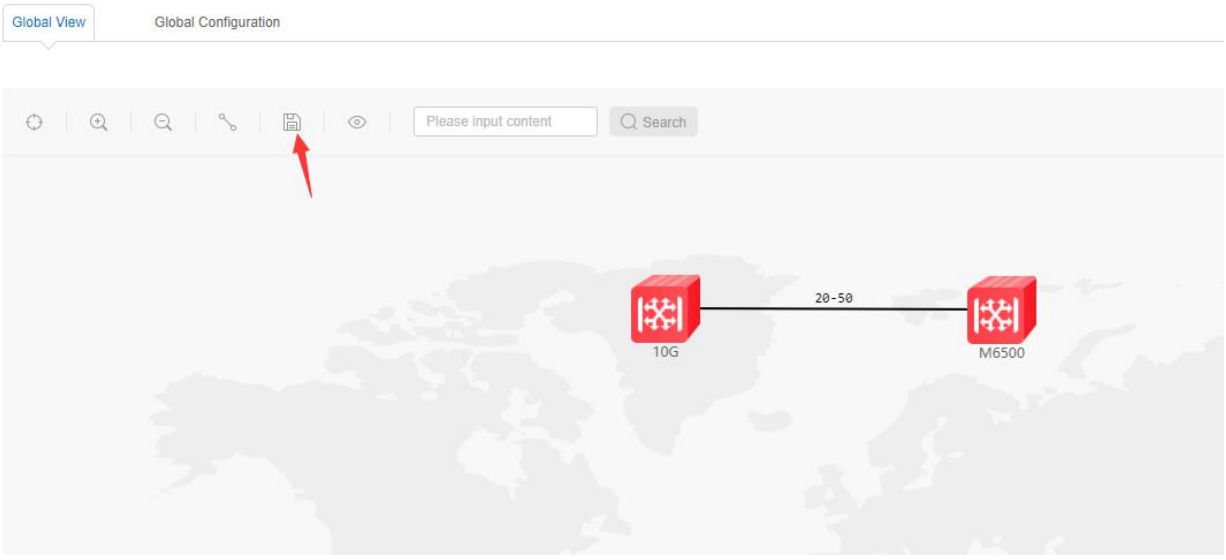



Figure2-35 Save Layout

# 3. DCN Configuration

## 3.1. DCN Introduction

DCN (Data Communication Network) controls remote NE through optical fiber and forms the in-band management channel of NE through GCC.

OTN provides a dedicated communication channel (GCC0/1/2/1+2) which can realize in-band management.

The basic environment of DCN is as shown in the figure below:

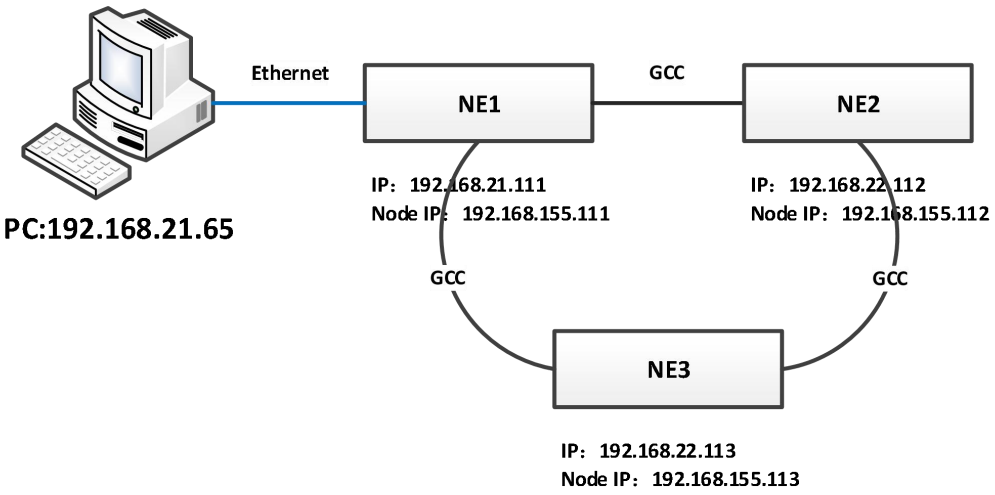



Figure3-1 Basic Environment Map of PC Direct Connection

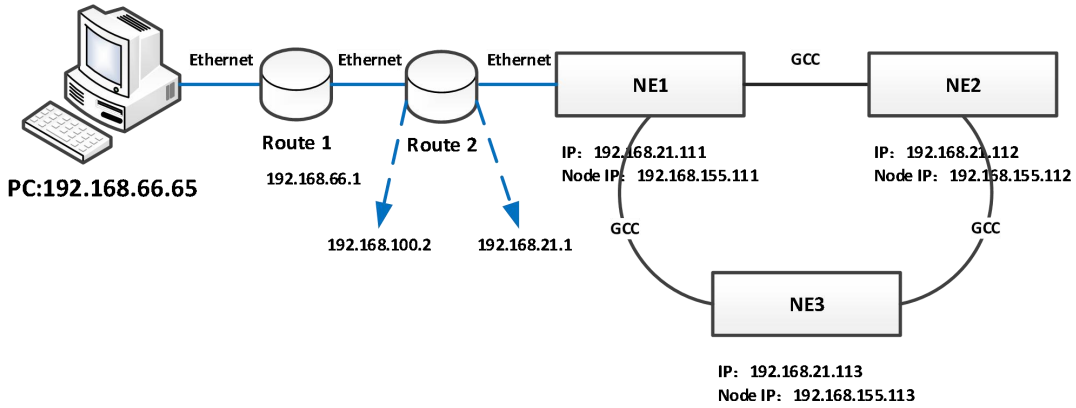



Figure3-2 Basic Environment Map of Connection between PC and Router

## 3.2. Configuration Steps

### 3.2.1. Direct Connection between PC and Device

- Open the GCC channel of the occupied port
- Configure the node IP of the gateway NE and enable OSPF function
- Configure the node IP of the remote NE

- Configure routing on the NMS server
- Connect the occupied port through optical fiber
- Manage the device through the node IP

### 3.2.2. Forwarding through Router

- Open the GCC channel of the occupied port
- Configure the node IP of the gateway NE as well as enable OSPF and default routing redistribution function
- Configure the node IP of remote NE
- Configure routing on the NMS server
- Connect the occupied port through optical fiber
- Manage the device through the node IP

## 3.3. Configuration Example

Here we take M6500-MXP10 as an example.

### 3.3.1. Direct Connection between PC and Device

Step 1:

Open the GCC channel of the occupied port: the NMS port of PC is connected with the MGMT2 port of the device. Add the IP of 10.32.130.220 on NMS. Operations of the device can be made through NMS.

Enable the management status of the occupied port. The port mode needs to be set as OTU2/OTU2e/OTU4/OCh (OTU4).

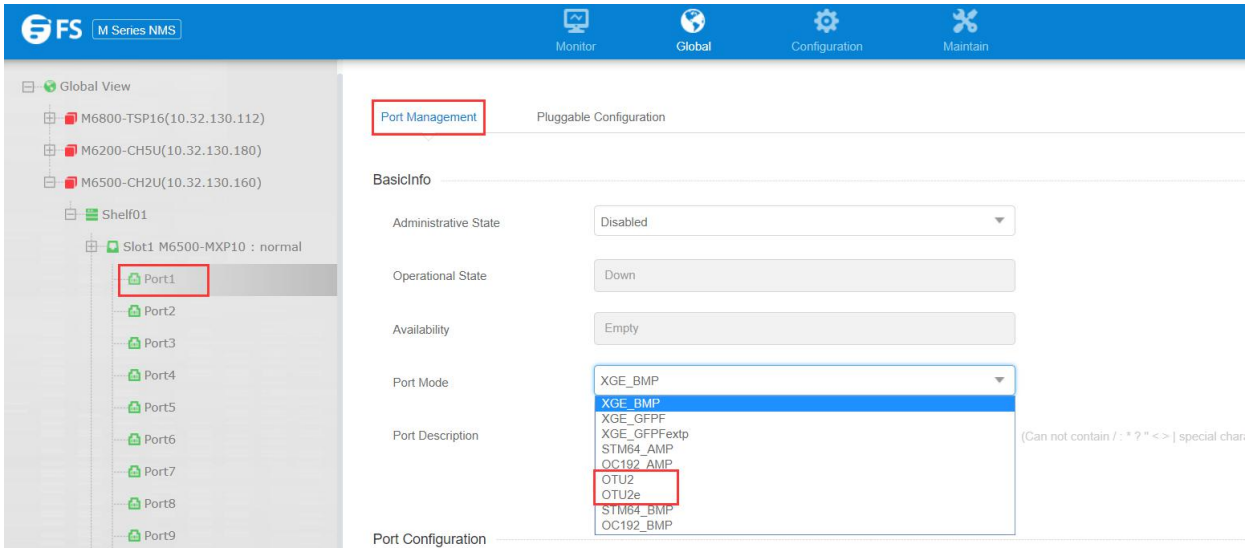



Figure3-3 Enable OTU2/2e Port

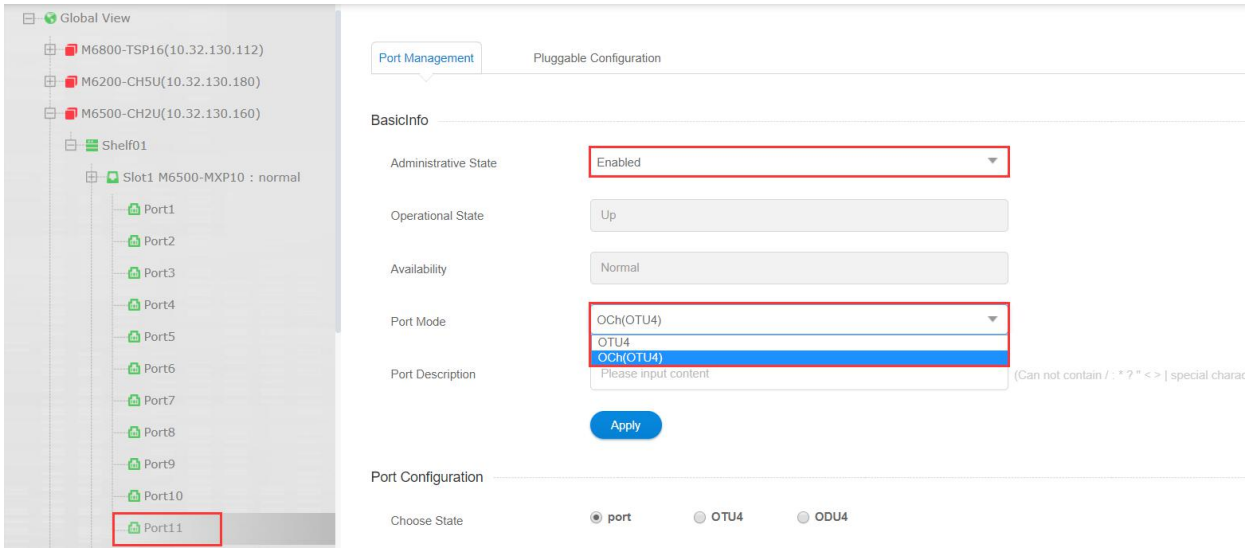



Figure3-4 Enable OTU4/OCh (OTU4) Port

Click on OTU2/OTU2e/OTU4/OCh (OTU4) or ODU2/ODU2e/ODU4 which is on the left of “Port Configuration” interface

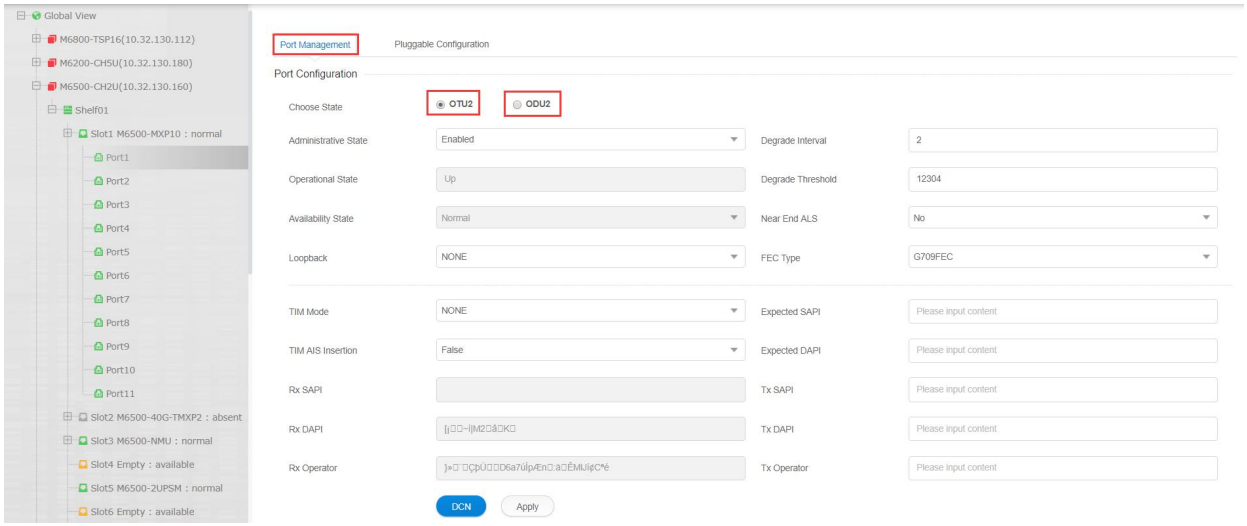



Figure3-5 Preparation before Enable GCC Channel of OTU2/ODU2

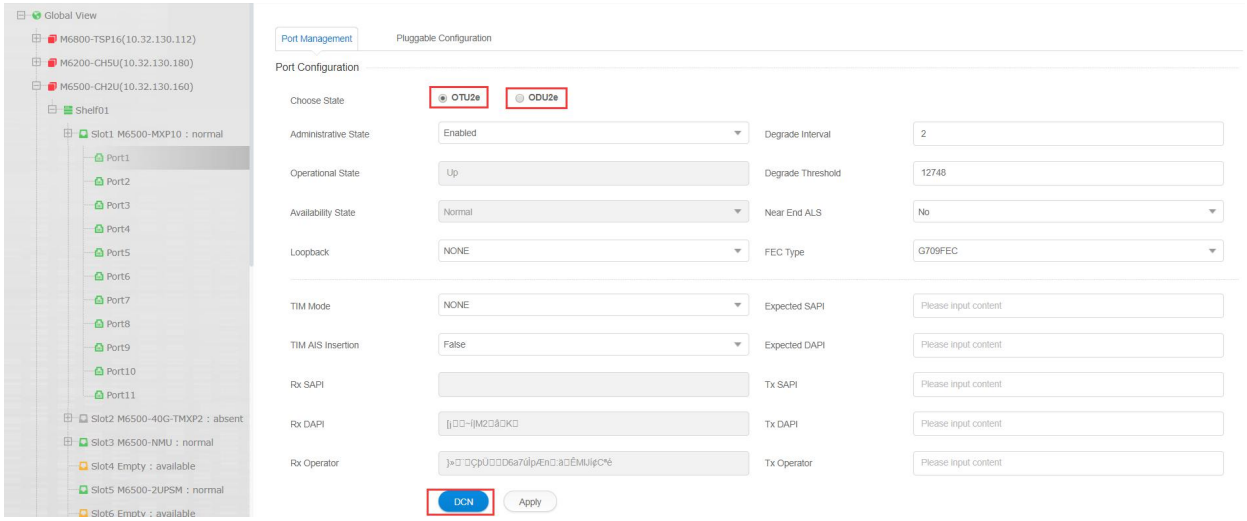


Figure3-6 Preparation before Enable GCC Channel of OTU2e/ODU2e

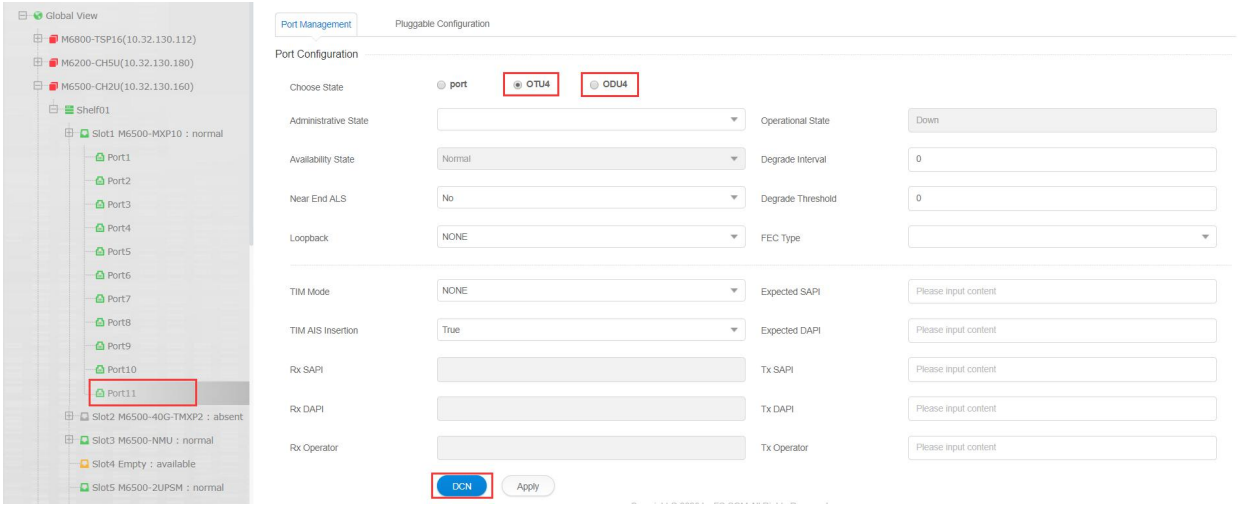



Figure3-7 Preparation before Enable GCC Channel of OTU4/ODU4

Then click on DCN in the lower to enter DCN configuration interface. Select GCC type (The GCC type of OTU layer is GCC0 and the GCC type of ODU layer is GCC1, GCC2 and GCC1+2), as shown in the figure below:

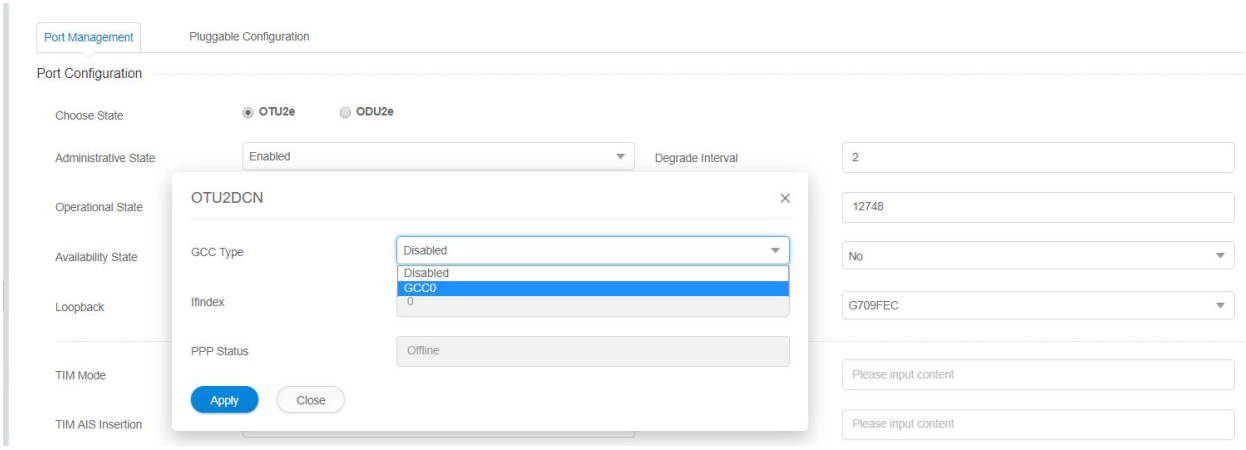



Figure3-8 Open GCC Channel of OUT Layer

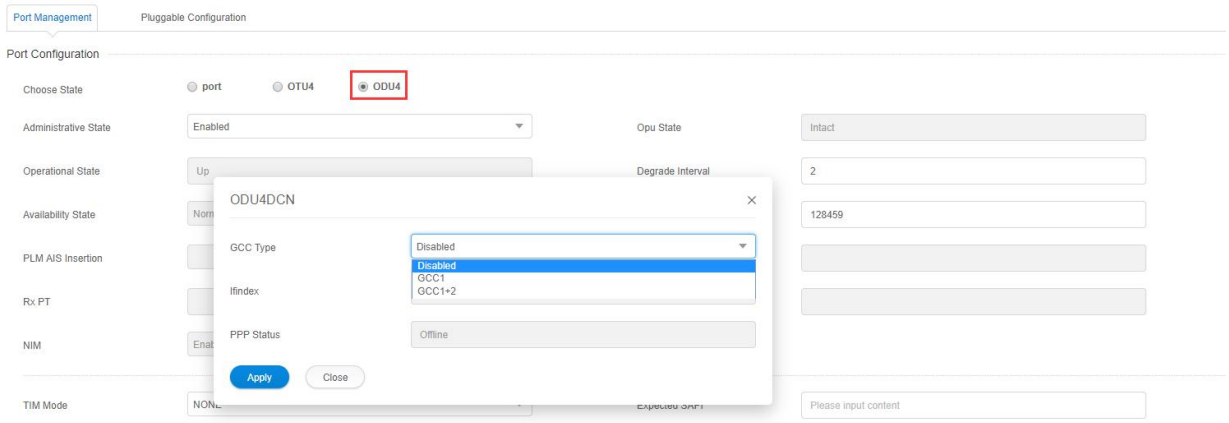



Figure3-9 Open GCC Channel of ODU Layer

The GCC types of the occupied ports for adjacent NE need to be set as the same.

Step 2:

Configure the node IP of the gateway NE and enable OSPF function: Select a NE as the gateway NE. After selecting the NE, click on"*MGMT IP Configuration*"and select"*MGMT IP Configuration*"module .

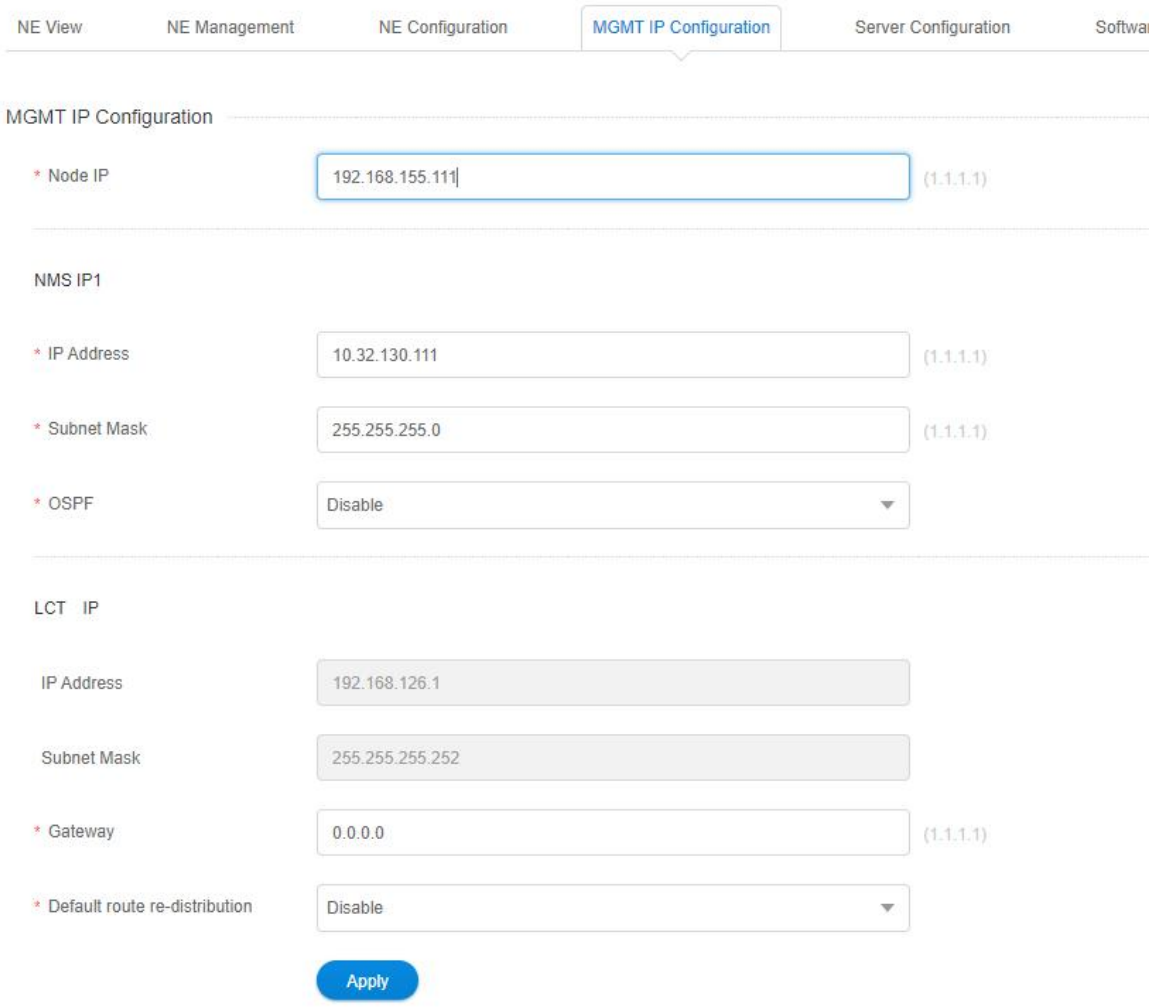



Figure3-10 Select NE and Manage IP Configuration

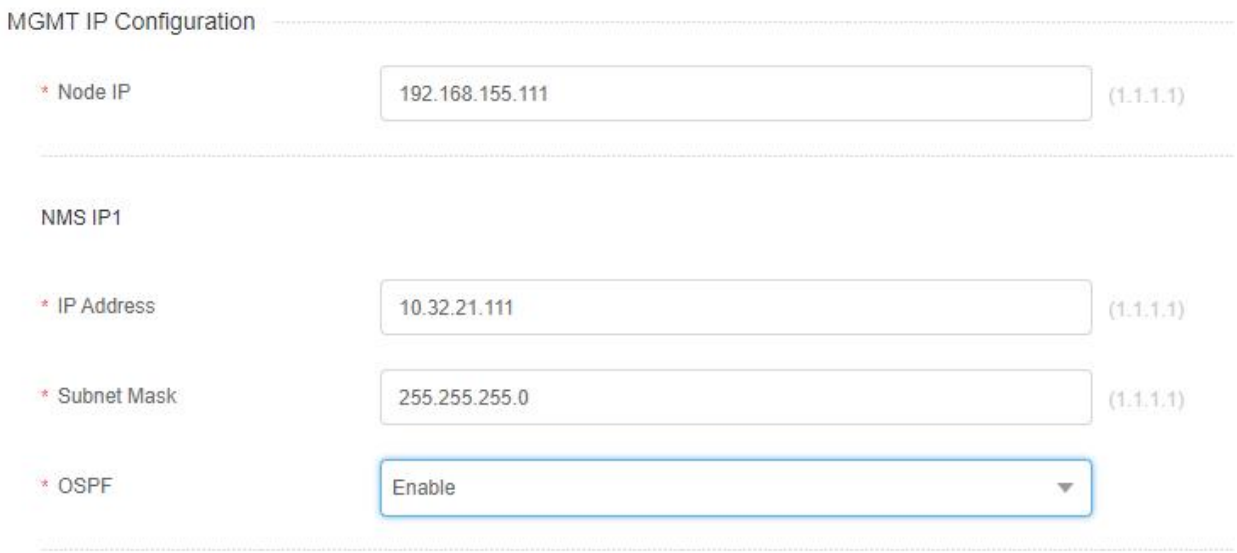



Figure3-11 Open Manage IP Configuration Interface

Configure node IP (The node IP cannot be in the same network segment with the out-band management port IP), and click on"*Apply*" after enabling OSPF function.

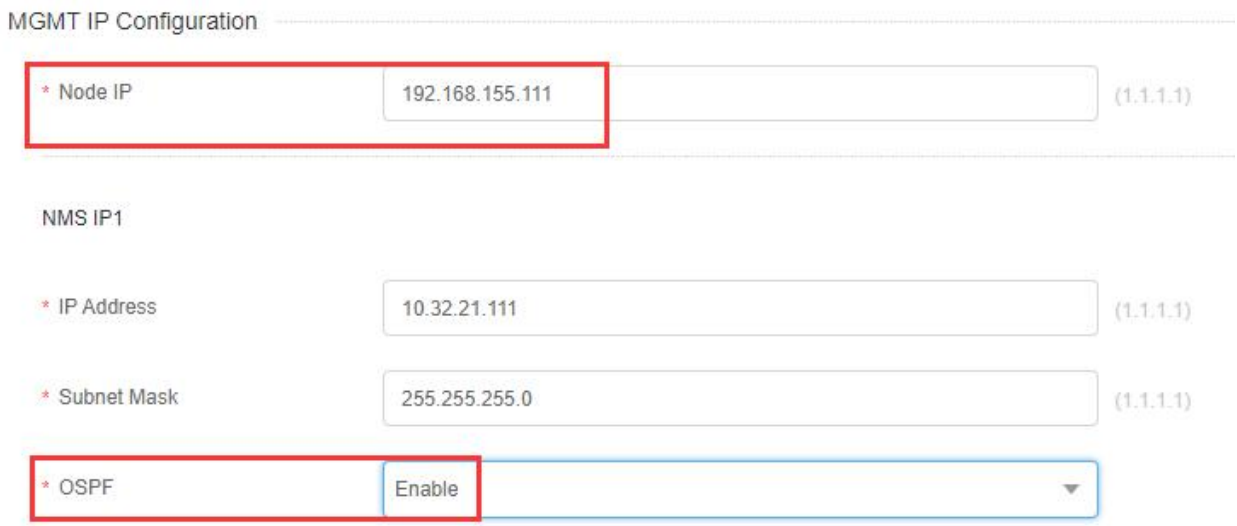



Figure3-12 Configure Gateway NE IP

The method to configure node IP of remote NE is the same as that to configure the node IP of gateway NE. However, the node IP should be different from that of the gateway NE and the IP of NMS IP1 cannot be in the same network segment with the gateway NE IP.

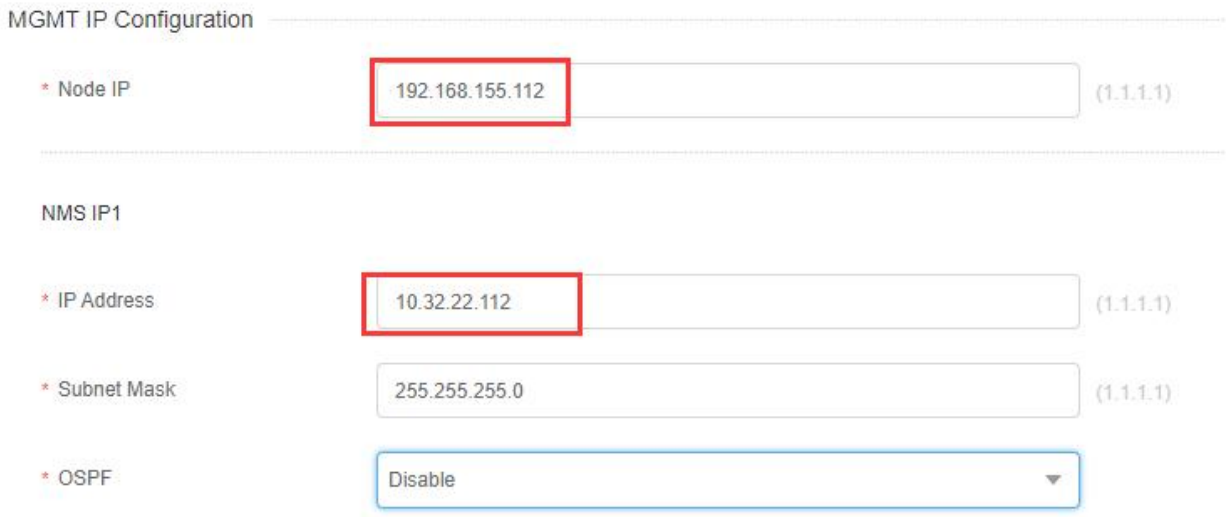



Figure3-13 Configure Remote NE IP

Step 3:

Configure the route on the computer to run CMD as an administrator and enter following two routes: route add 192.168.155.111 mask 255.255.255.255 192.168.21.111 and route add 192.168.155.112 mask 255.255.255.255 192.168.21.111.

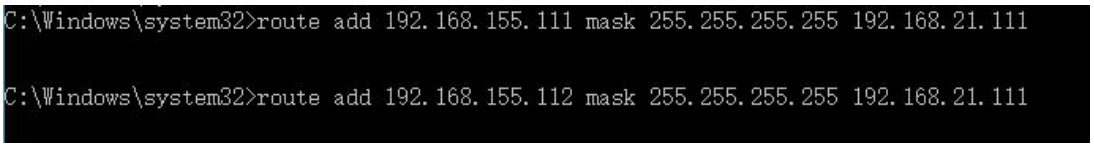



Figure3-14 Add Local Route

Check the input route through route print command.

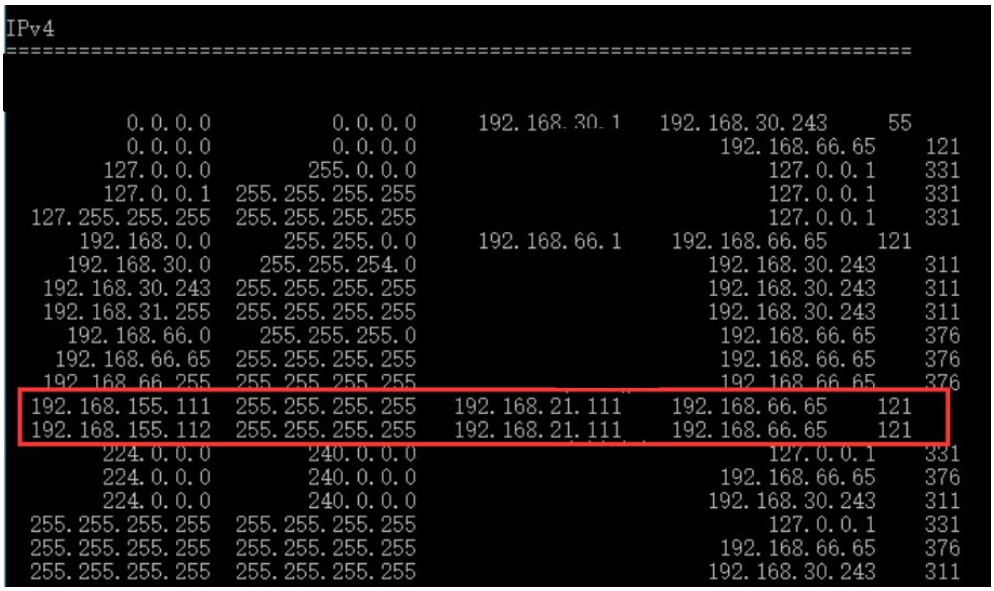



Figure3-15 View Local Route

Use optical fiber to connect occupied ports: Use optical fiber to connect the occupied ports of the two network elements, and to form fiber-optic channels.

Manage the equipment through the node IP, unplug the network cable of the remote NE, and add the two IP addresses of 192.168.155.111 and 192.168.155.112 to the NMS system. After the IP addresses are successfully added, normal management of the two devices can be achieved.

### 3.3.2. Forwarding Trough Routers

The configuration method is the same as that described in 3.3.1. Besides that, the following configuration needs to be added:

Add configuration 1:

Enable the default route redistribution function of the gateway NE, as shown in the figure below:

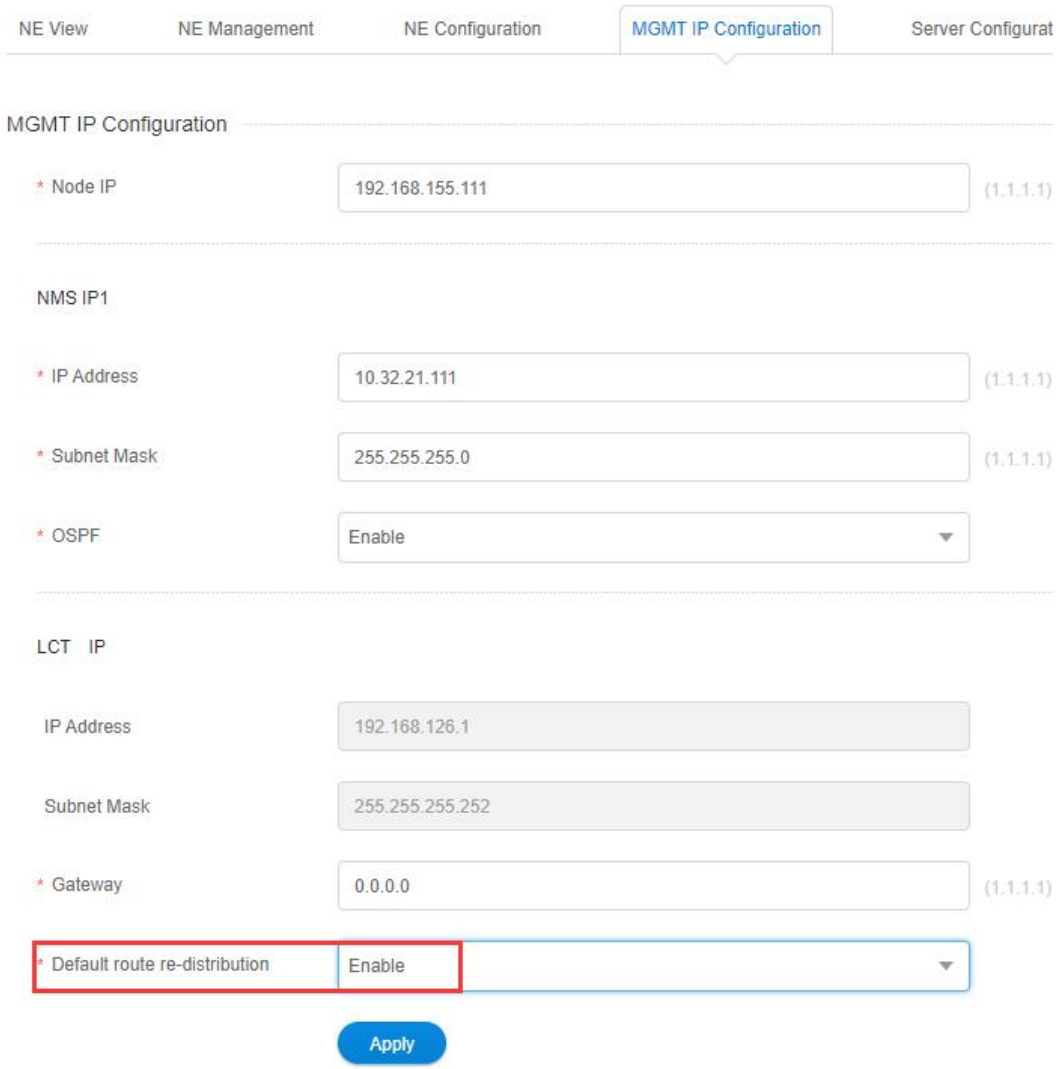



Figure3-16 Enable Default Route Redistribution Function of the Gateway NE

Add Configuration 2: Set the gateway of the remote NE as 0.0.0.0.

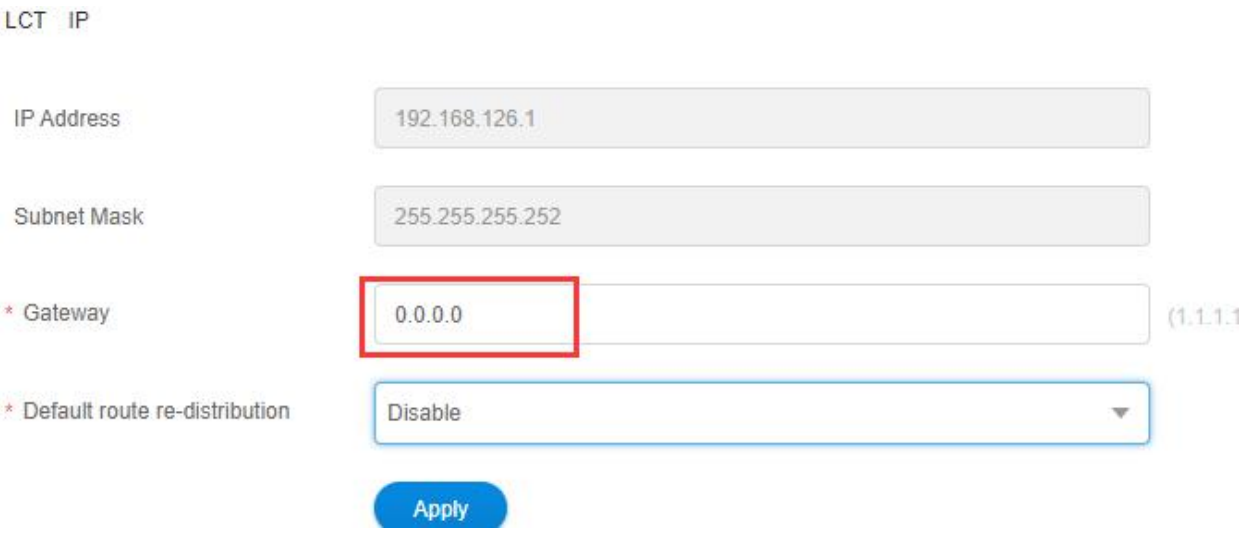



Figure3-17 Modify Gateway

Add Configuration 3：

When there are many devices, you can configure the node IP of the remote NE to the same network segment. For example, if you set the node IP of the remote NE to 155 network segment, you can add only one route to the computer: route add 192.168.155.0 mask 255.255.0 192.168.155.1 (Here the network segment of 192.168.155.0 is the actually configured node IP segment. 192.168.66.1 is the network segment of NMS server local IP.)

**Attention**

**1.The Ethernet IP address and the node IP address of all network elements can not be in the same network segment.**

**2.PC direct connection: the Ethernet IP addresses of gateway network element NE1 and remote network element N2 and NE3 cannot be in the same network segment.**

# 4. NE & Board Configuration

**Prerequisite**

1. Network devices and lines are normal.
2. Click on the desktop icon of "Run NMS Server" to open the NMS software.
3. Click on the icon of "Start NMS Server"in the software interface to open the NMS server.
4. Open the client Web server port on Google Browser: localhost: 9090, log in to the NMS root account.
5. The M Series NMS interface is displayed after successful login.

## 4.1. Shelf Information

Select NE and click on"*Shelf01*", then click on"*Shelf information* "on the right to open the Shelf information interface. Information such as Shelf type and temperature is displayed in this interface, as shown in Figure 4-1:

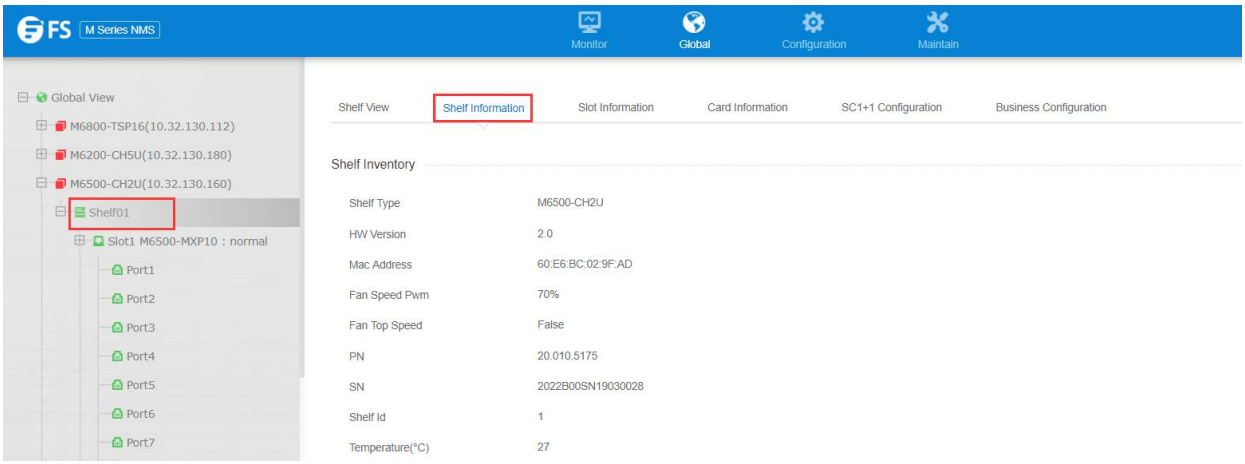



Figure4-1 Operation Steps to View Shelf Inventory

### 4.1.1. M6500-CH2U

The Shelf information interface of 2U device is as shown in the figure below:

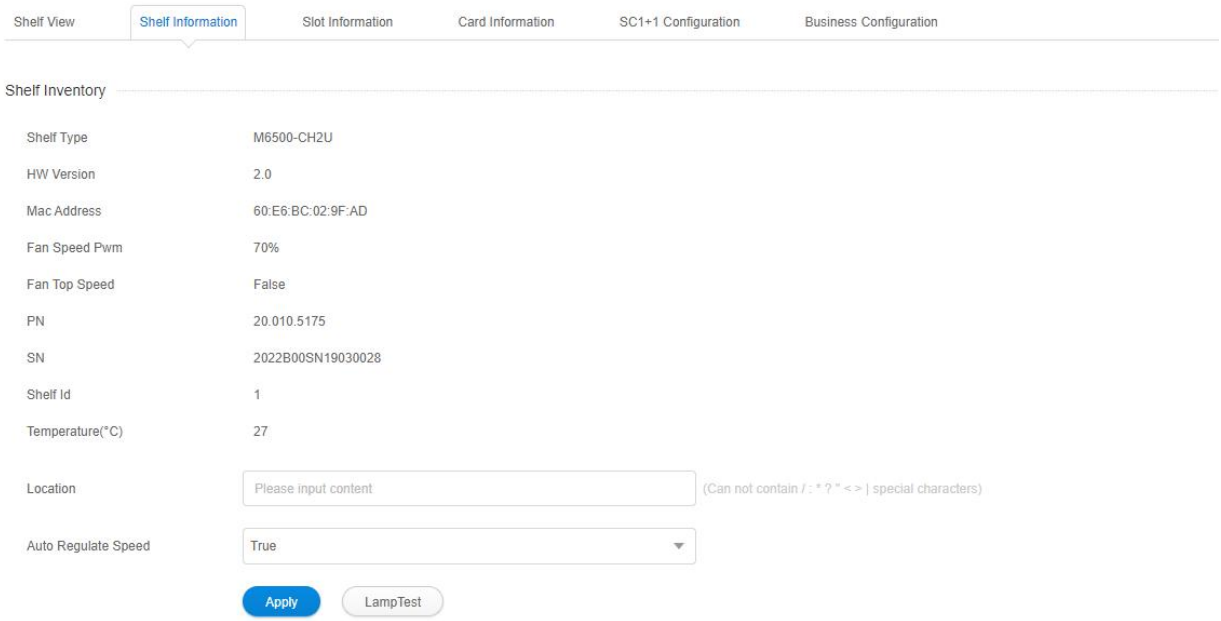



Figure4-3 M6500-CH2U Shelf Information

### 4.1.2. M6500-CH5U

The Shelf information interface of 5U device is as shown in the figure below:

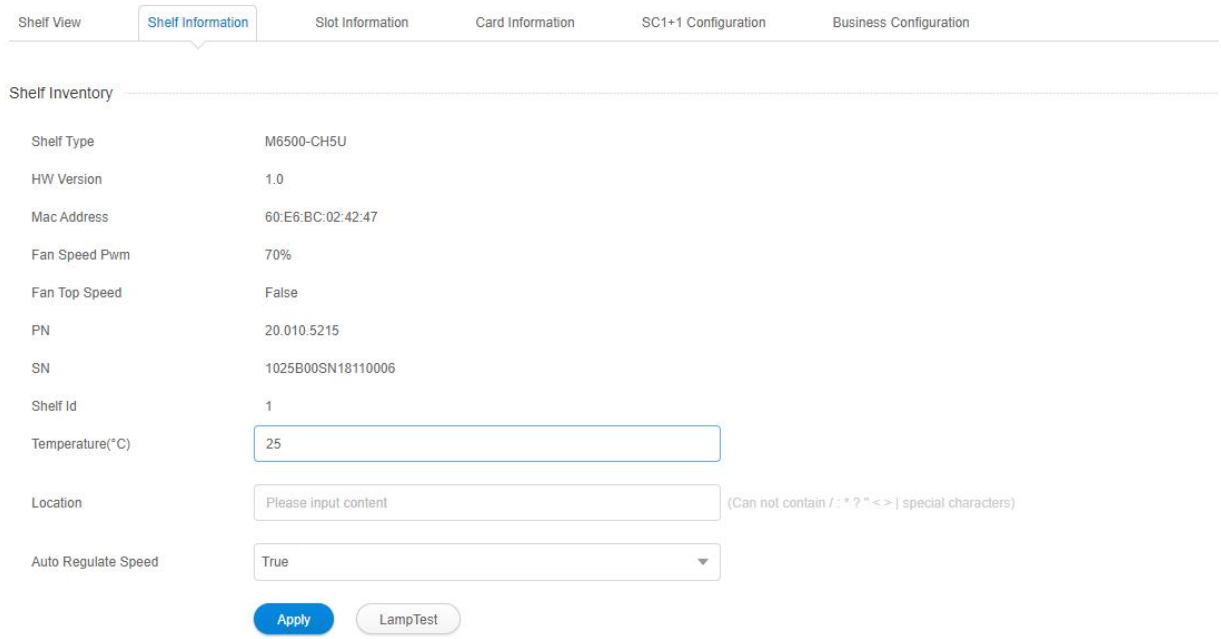



Figure 4-4 M6500-CH5U Shelf Information

## 4.2. LED Indicator Information

The LED indicators on different series of network elements, ports, boards, systems are different. The following is a list of LED indicator status of all series of boards, ports, systems and power indicators.

### 4.2.1. NMU Board

**Attention**

**When M6500 series network element replaces NMU board, pay attention that the SD board files must be consistent with those on the replaced NMU board. If not, it may cause all the LED lights of the NMU board flashing, and the NMS system cannot be connected. Therefore, it needs to be dealt with in time.**

Table4-1 LED Indicator Status of Separate NMU Board

| | | M6500-CH5U | M6500-CH2U |
|---|---|---|---|
| NMU Control System LED indicator<br>(Separate NMU Board) | RUN | Green Light Quick Blink: Software startup completed.<br>Green Light Off: The software is not started. | NA |
| | ACTIVE | Green Light On: NMU is Active.<br>Green Light Off: NMU is Standby. | NA |
| | FAULT/ALM | Red Light Slow Flash: There is latch-open alarm.<br>Red Light On: Alarm exists in NE.<br>Red Light Off: There is no alarm in NE. | NA |

Table4-2 LED Indicator Status of Integrated NMU Board

| | | M6500-CH5U | M6500-CH2U |
|---|---|---|---|
| NMU Control System LED Indicator<br>(NMU Board, Service Board Integration) | RUN | NA | Green Light Slow Flash: The software is successfully started, and it is Active board.<br>Green Light On: The software is successfully started, but it is Standby board.<br>Green Light Off: The software is not started. |
| | FAULT/ALM | NA | Red Light Quick Blink: The board is mismatched.<br>Red Light Slow Flash: There is latch-open alarm.<br>Red Light On: There is alarm.<br>Red Light Off: There is no alarm. |

Table4-3 LED Indicator Status of System Board Optical Management Port

| | | M6500-CH5U | M6500-CH2U |
|---|---|---|---|
| System Board<br>Optical Management Port<br>(MGMT) LED Indicator | Monochromatic Green Light | Off: The port is disabled/ There is los alarm.<br>Green Light On: There is no los alarm and the port is enabled. | Off: The port is disabled/There is los alarm.<br>Green Light On: There is no los alarm and the port is enabled. |

### 4.2.2. System Interface LED Indicator

Table4-4 System Interface LED Indicator Status

| | | M6500-CH5U | M6500-CH2U |
|---|---|---|---|
| System Interface LED Indicator | SYS | Located in Fan Tray: Green Light On: The system is successfully started.<br>Green Light Off: The system is not started. | On NMU Board:<br>Green Light On: The system is successfully started.<br>Green Light Off: The system is not started. |
| | CR/MJ/MN | Located in Fan Tray:<br>CR: Red Light On: There is Critical alarm.<br>MJ: Orange Light On: There is Major alarm.<br>MN: Yellow Light On: There is Minor alarm. | On NMU Board:<br>CR: Red Light On: There is Critical alarm.<br>MJ: Orange Light On: There is Major alarm.<br>MN: Yellow Light On: There is Minor alarm. |

### 4.2.3. Service Board LED Indicator

Table4-5 Service Board LED Indicator Status

| | | M6500-CH5U | M6500-CH2U |
|---|---|---|---|
| Service Board LED Indicator | RUN | Green Light Slow Flash: The software is started.<br>Green Light Off: The software is not started. | Green Light Slow Flash: The software is successfully started and it is active board.<br>Green Light On: The software is successfully started but it is standby board.<br>Green Light Off: The software is not started. |
| | FAULT/ALM | Red Light Quick Blink: The board is mismatched.<br>Red Light Slow Flash: There is latch-open alarm.<br>Red Light On: There is alarm.<br>Red Light Off: There is no alarm. | Red Light Quick Blink: The board is mismatched.<br>Red Light Slow Flash: There is latch-open alarm.<br>Red Light On: There is alarm.<br>Red Light Off: There is no alarm. |

### 4.2.4. Fan Tray LED Indicator

Table4-6 Fan Tray LED Indicator Status

| | | M6500-CH5U | M6500-CH2U |
|---|---|---|---|
| Fan Tray LED Indicator | RUN (Monochrome) | Green Light On: The system NMU board starts to manage the fan.<br>Green Light Off: The system NMU board does not manage the fan. | NA |
| | FAULT/ALM (Monochrome) | Red Light On: There is alarm of the fan.<br>Red Light Off: There is no alarm of the fan. | NA |
| | FAN (Two Colors) | NA | Red Light On: There is alarm of the fan.<br>Green Light On: There is no alarm of the fan. |

### 4.2.5. Port LED Indicator of Service Board

Table4-7 Port LED Indicator Status of Service Board

| | | M6500-CH5U | M6500-CH2U |
|---|---|---|---|
| Service Board Port LED Indicator | Bi-Color LED Indicator | Off: The port is disabled.<br>Red Light Quick Blink: There is mismatch alarm of the port.<br>Red Light On: There is los alarm of the port.<br>Green Light On: There is no los or mismatch alarm of the port. | Off: The port is disabled.<br>Red Light Quick Blink: There is mismatch alarm of the port.<br>Red Light On: There is los alarm of the port.<br>Green Light On: There is no los or mismatch alarm. |

### 4.2.6. LED Indicator of WDM Service Board

Table4-8 WDM Service Board LED Indicator Status

| | | M6500-CH5U | M6500-CH2U |
|---|---|---|---|
| LED Indicator of OA/OLP Board | Monochrome Green Light | Off: The port is disabled/There is LOS alarm of the port.<br>Green Light On: There is no los alarm and the alarm is enabled. | Off: The port is disabled/There is LOS alarm of the port.<br>Green Light On: There is no los alarm of the port and the port is enabled. |

### 4.2.7. Power Tray LED Indicator

Table4-9 Power Tray LED Indicator Status

| | | M6500-CH5U | M6500-CH2U |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Power Tray LED Indicator | PWR (Monochrome) | NA | Off: The power tray is not powered.<br>Green Light On: Normal power supply. |
| | FAULT<br>(Monochrome) | Off: There is not any alarm of the power tray.<br>Red Light On: There is alarm that the power supply is not powered on or there is power failure. | Off: There is not any alarm of the power tray.<br>Red Light On: There is alarm that the power supply is not powered on or there is power failure. |
| | PWR1 (Monochrome) | Off: The power tray is not powered.<br>Green Light On: Normal power supply. | NA |
| | PWR2 (Monochrome) | Off: The power tray is not powered.<br>Green Light On: Normal power supply. | NA |

## 4.3. View Single Board Information

Select NE and click on"*Shelf01*", and then click "*Card information*" on the right.

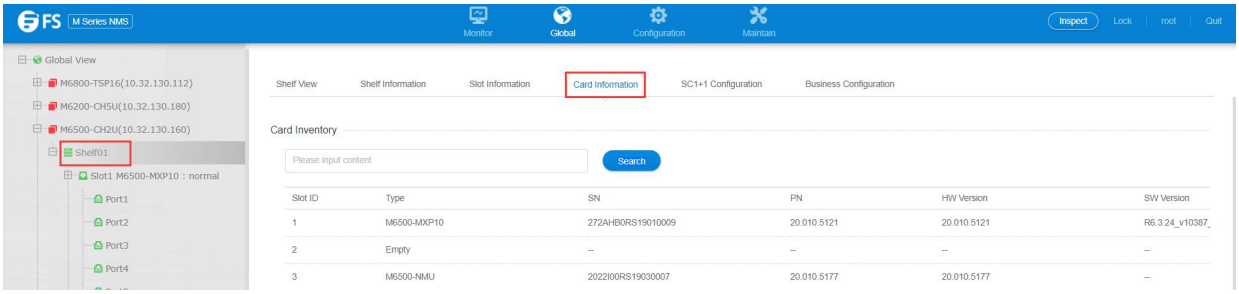



Figure4-5 View Single Board Information

After selecting "*Card information*" , the interface as shown in the figure below pops up. Information such as board type, hardware version, software version software version, Kernel version, Uboot version, central temperature and outlet temperature of each slot can be checked in this interface.

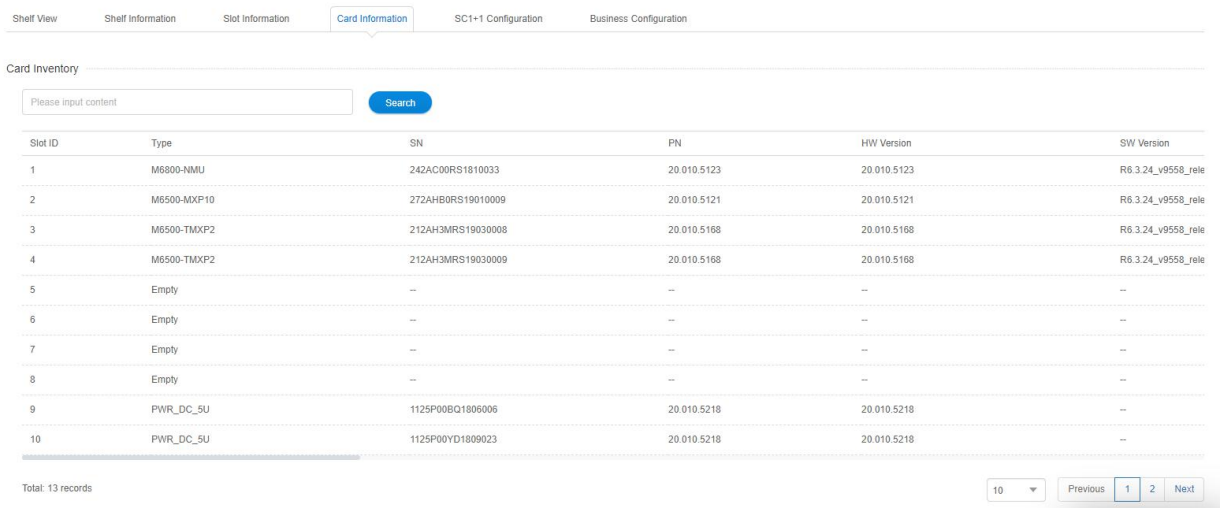



Figure4-6 Board Information Interface

# 4.4. Port Configuration

Select NE-Slot1 click on"*Port1*", and then select"*Port Management*"on the right ， as shown in the figure below:

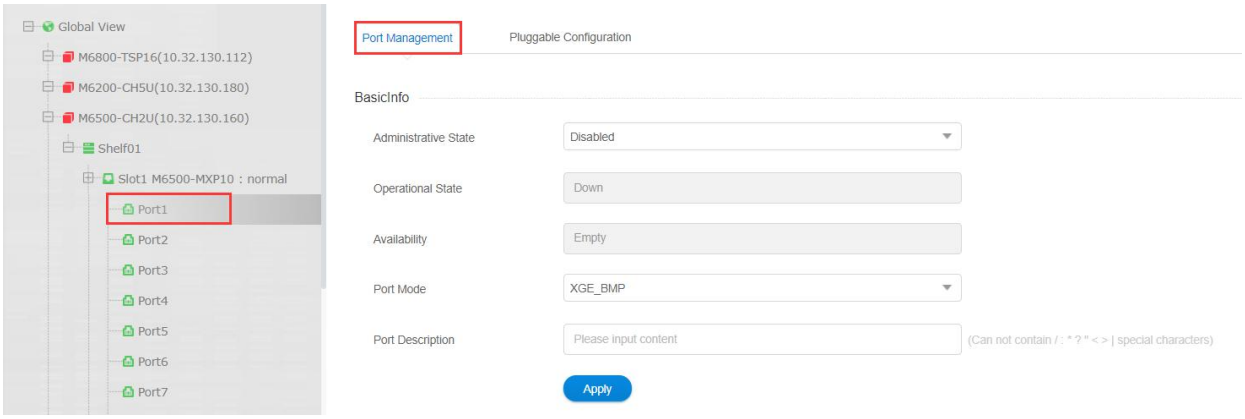



Figure4-7 View Port Configuration Information

## 4.4.1. Basic Information

There are two port types: client side port and line side (system side) port.

Client side port type supports: FE, GE, 10GE, 40GE, and 100GE, STM-1/4/16, OC-3/12/48, STM-64, OC-192 and OTU2 (2e)/OTU3/OTU4.

For line side (system side) port type, the grey light supports OTU2/2e and OTU4, and the color light supports OCh (OTU2/2e) and OCh (OTU4).

Select NE-Slot 1, click on"*Port1*", and select"*Port Management*"on the right, the interface as shown in the figure below pops up. The configuration status and port mode can be modified in basic information.

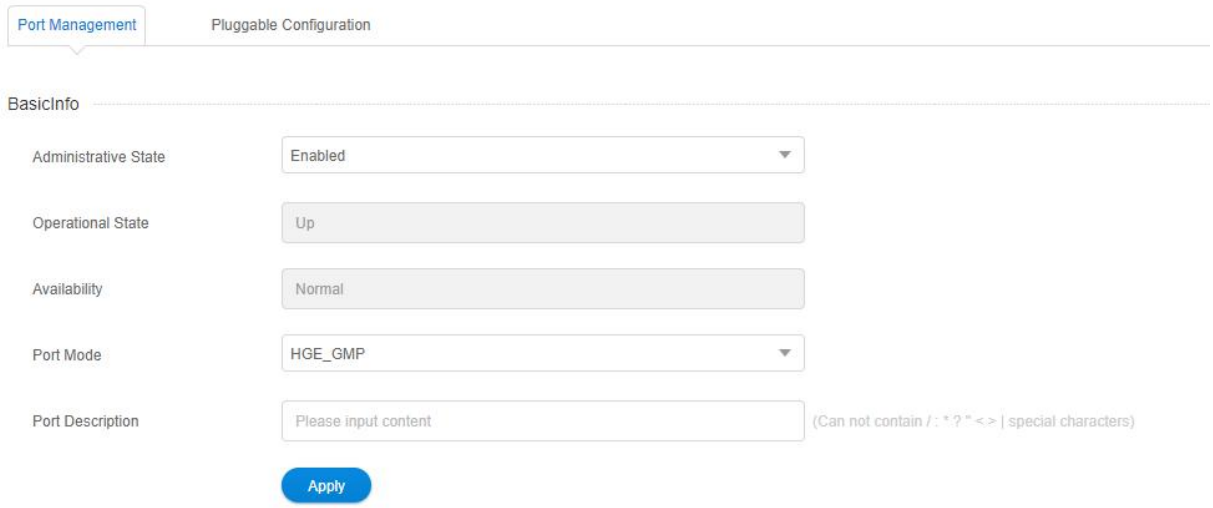



Figure 4-8 Port Management Interface

The client side port mode of M6500-TMXP2 board is different from that of other boards. When the port 2 is disabled, it is in unused status, as shown in the figure below:

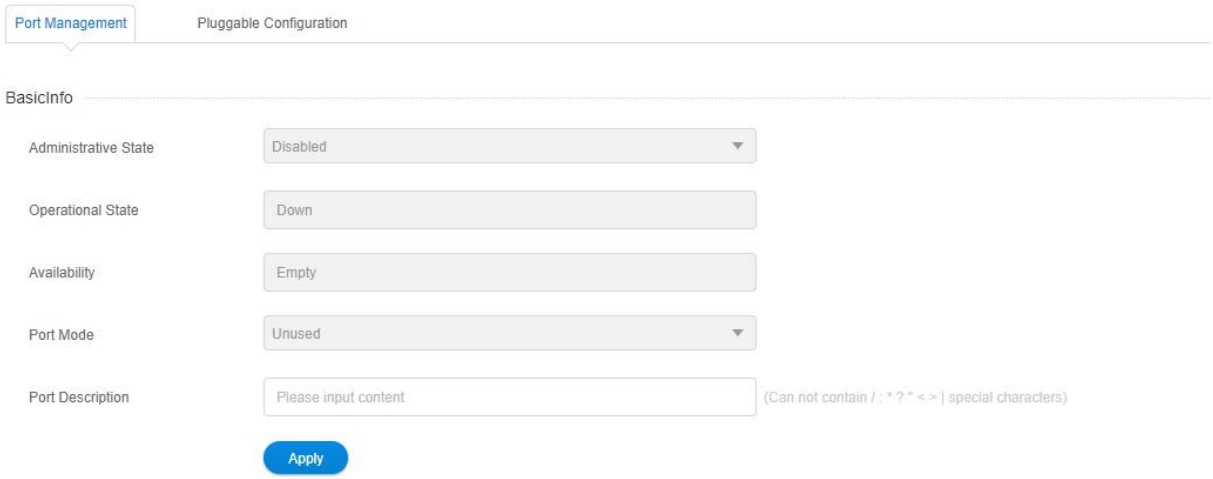



Figure4-9 M6500-TMXP2 Board Client Side Port Disabled Interface

While enabling the port, firstly select the port mode and click on apply. After clicking on apply, you can make selection in the management status bar, as shown in the figure below:

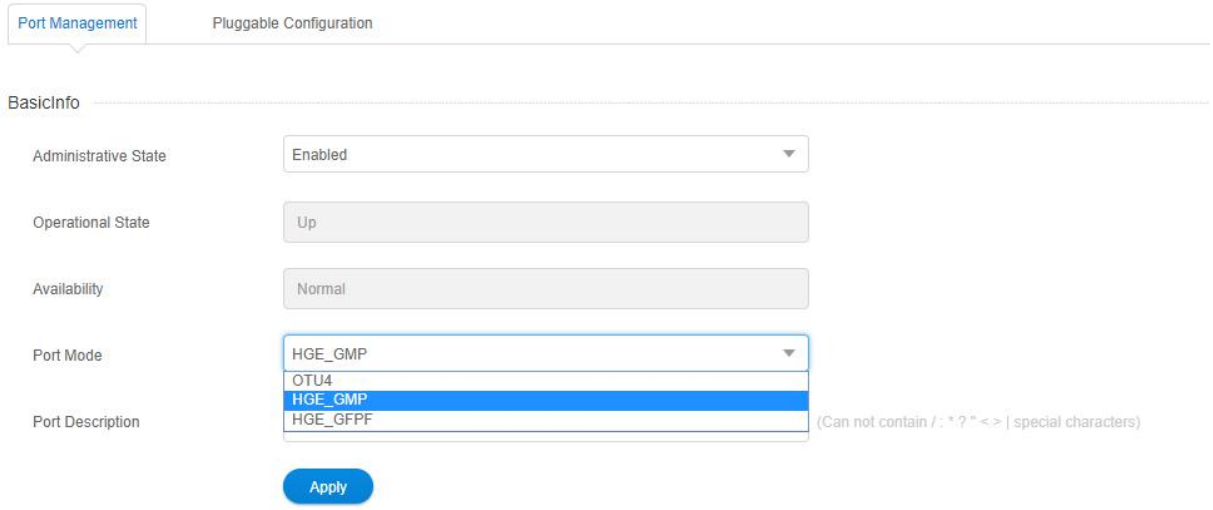



Figure4-10 M6500-TMXP2 Client Side-Select Port Mode

Select "Enable" in the management status bar to enable the port, as shown in the figure below:

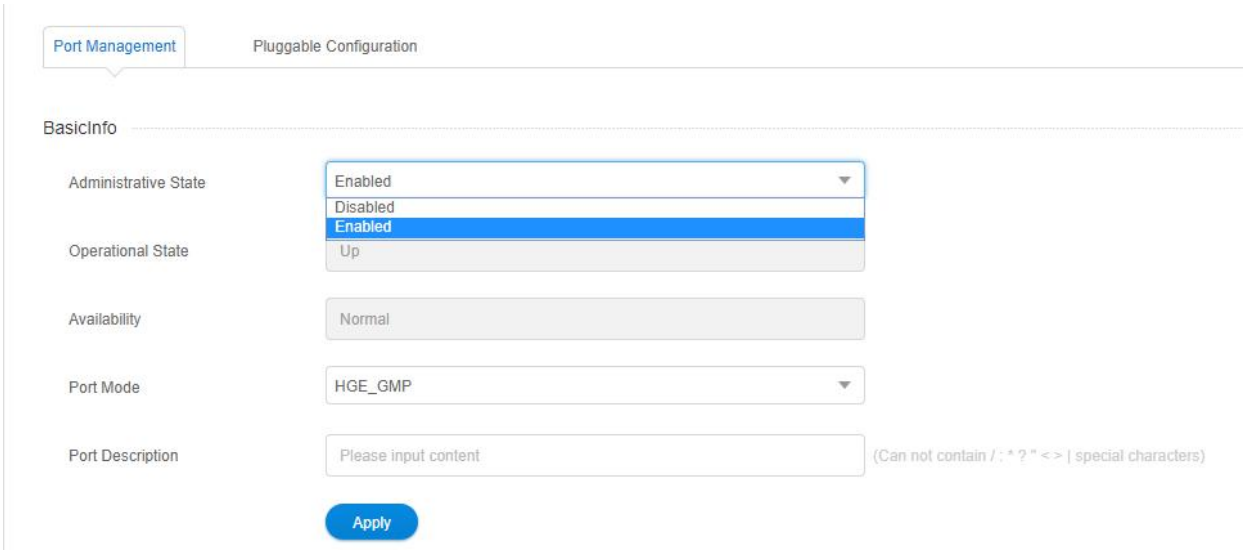



Figure4-11 Enable M6500-TMXP2 Client Side Port

#### 4.4.1.1. Interface Configuration

Select NE-Slot 1, click on"*Port1*" and select"*Port Management*"on the right, the port management interface shows up.Select the interface options of the"*Port Configuration*"module, the information such as management status, the near-end no light laser shutdown (ALS), turn off light while alarm occurs, loop-back, patch trace mismatch (TIM) mode can be modified in the toolbar interface.

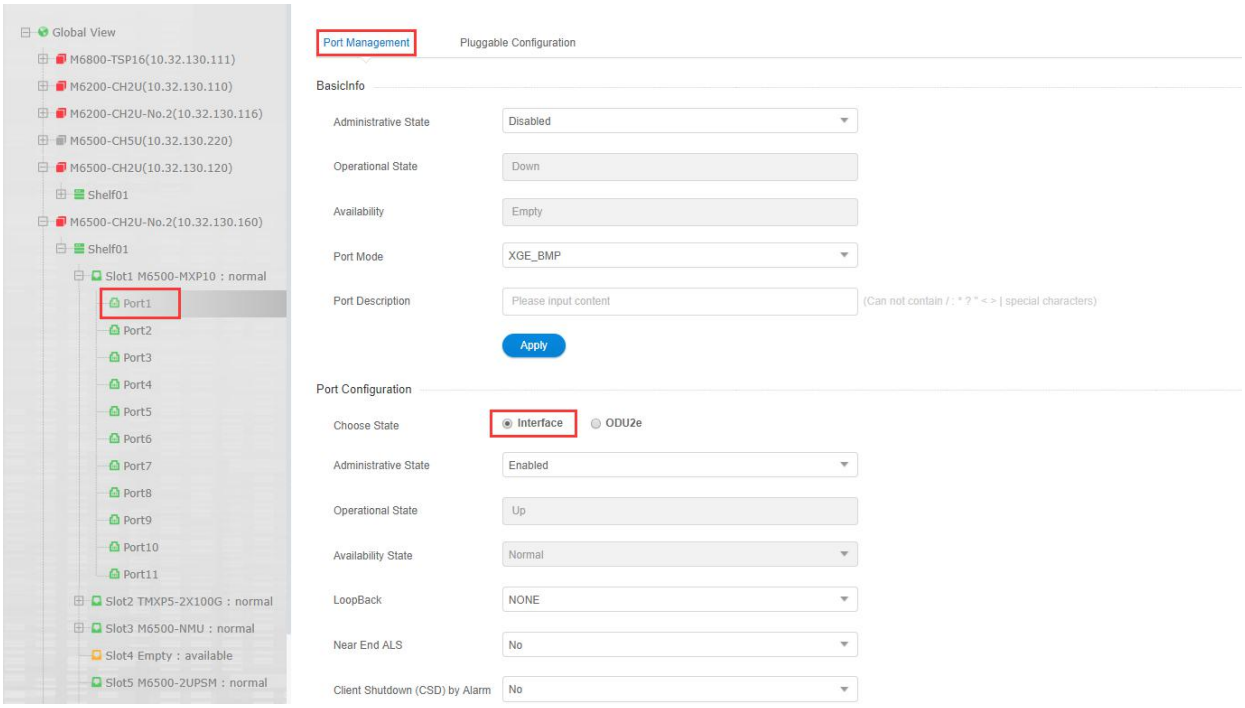



Figure4-12 Port Management-Interface Information

### 4.4.1.2. ODU2/ODU2e Configuration

- ODU2 Configuration

Select NE-Slot 1,click on"*Port1*"and select "*Port Management*"on the right, the port management interface shows up （here we take ODU2 corresponding to XGE_GFPF port mode as an example）. Click on ODU2 option from"*Port Configuration*"in this interface, as shown in the figure below. It shows ODU2 toolbar interface.

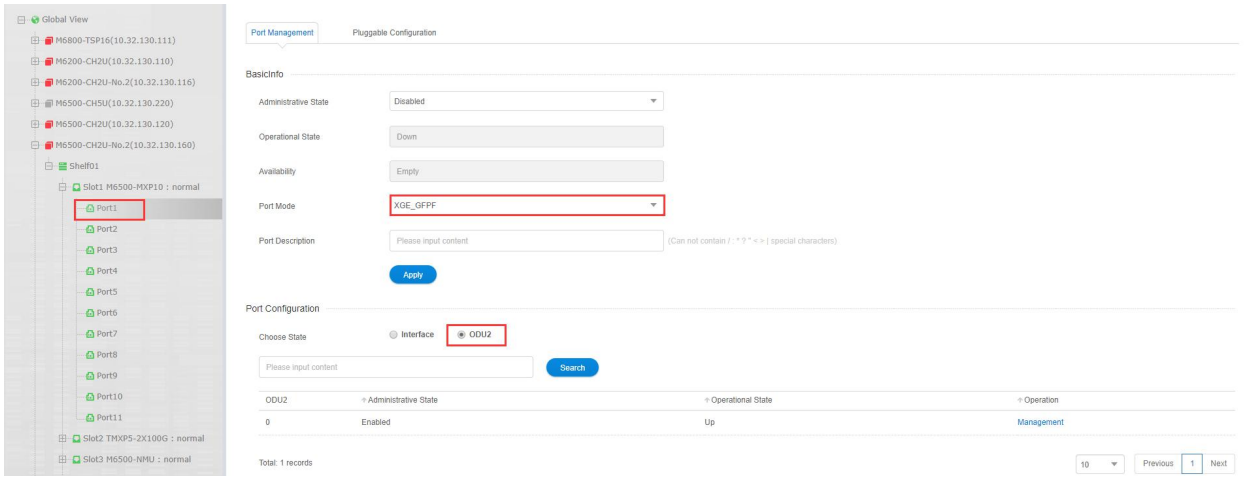



Figure4-13 ODU2 Toolbar Interface

Click on"*Management*" button in ODU2 toolbar interface, the toolbar management interface pops up. Detailed information about ODU2 can be viewed in the interface, as shown in the figure below:

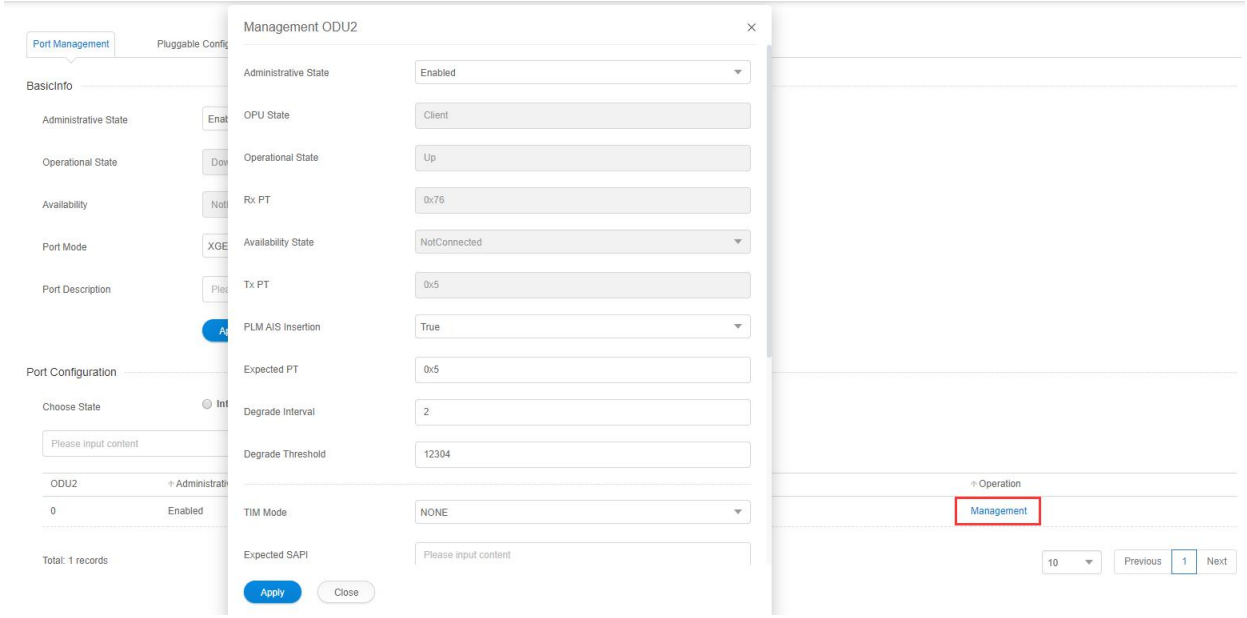



Figure4-14 ODU2 Toolbar Management Interface

- ODU2e Configuration

Select NE-Slot 1, click on"*Port1*" and select"*Port Management*"on the right, the port management interface shows up（here we take ODU2e corresponding to XGE_BMP port mode as an example）. Click on ODU2e option from"*Port Configuration*"in this interface, as shown in the figure below. It shows ODU2e toolbar interface.

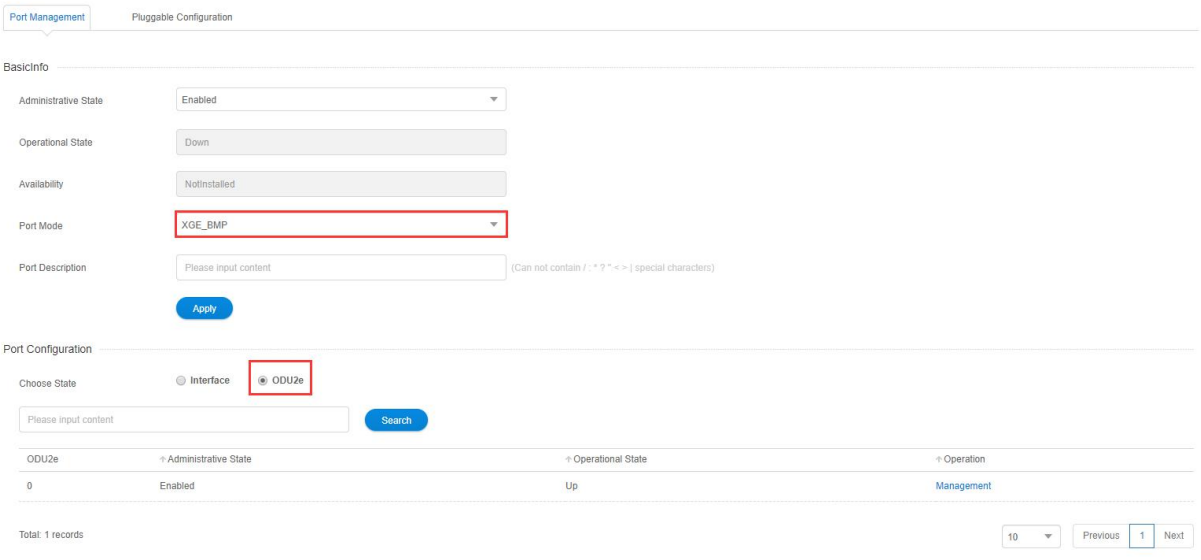



Figure4-15ODU2e Toolbar Interface

Click on "*Manage*" button in ODU2e toolbar interface, the toolbar management interface pops up. Detailed information about ODU2e can be viewed in the interface, as shown in the figure below:

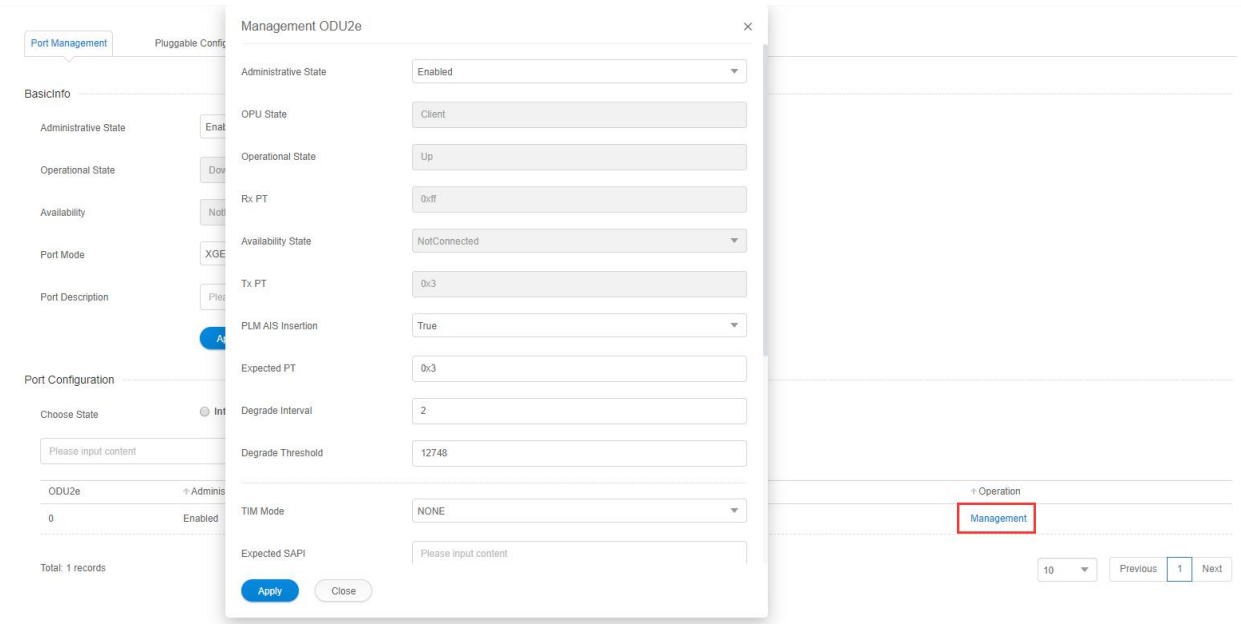



Figure4-16 ODU2e Toolbar Management Interface

### 4.4.1.3. OTU2/OTU2e Configuration

- OTU2 Configuration

Select NE-Slot 1, click on"*Port1*" and select"*Port Management*"on the right(here we take OTU2 corresponding to OTU2 port mode as an example), the port management interface pops up. Click on OTU2 option from"*Port Configuration*"in this interface, as shown in the figure below. It shows OTU2 toolbar interface.

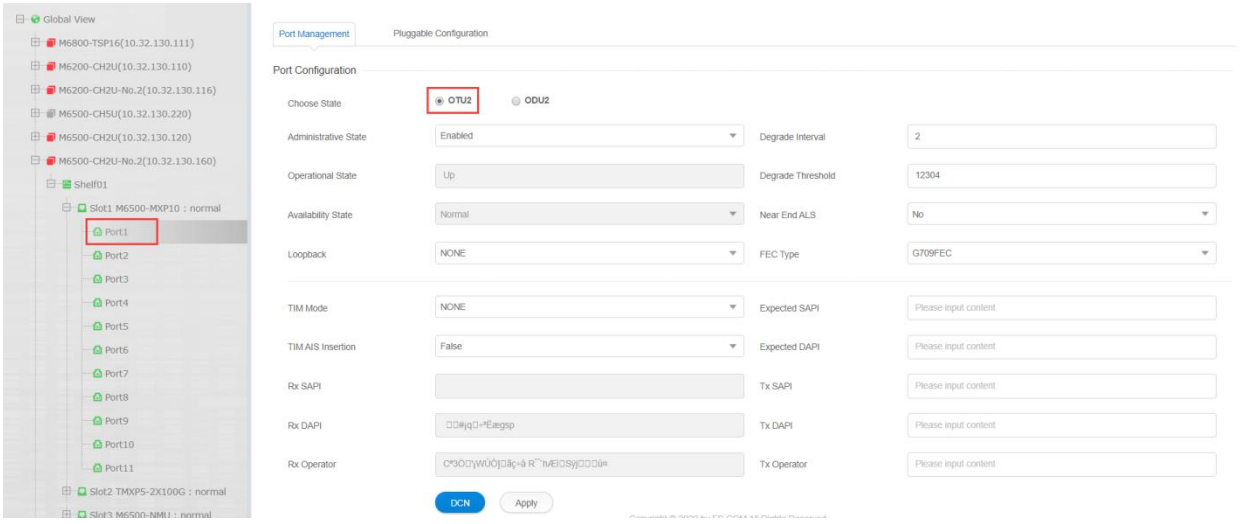



Figure4-17 OTU2 Toolbar Interface

- OTU2e Configuration

Select NE-Slot 1, click on"*Port1*" and select"*Port Management*"on the right, the port management interface pops up (here we take OTU2e corresponding to OTU2e port mode as an example). Click on OTU2e option from"*Port Configuration*"in this interface, as shown in the figure below. It shows OTU2e toolbar interface.

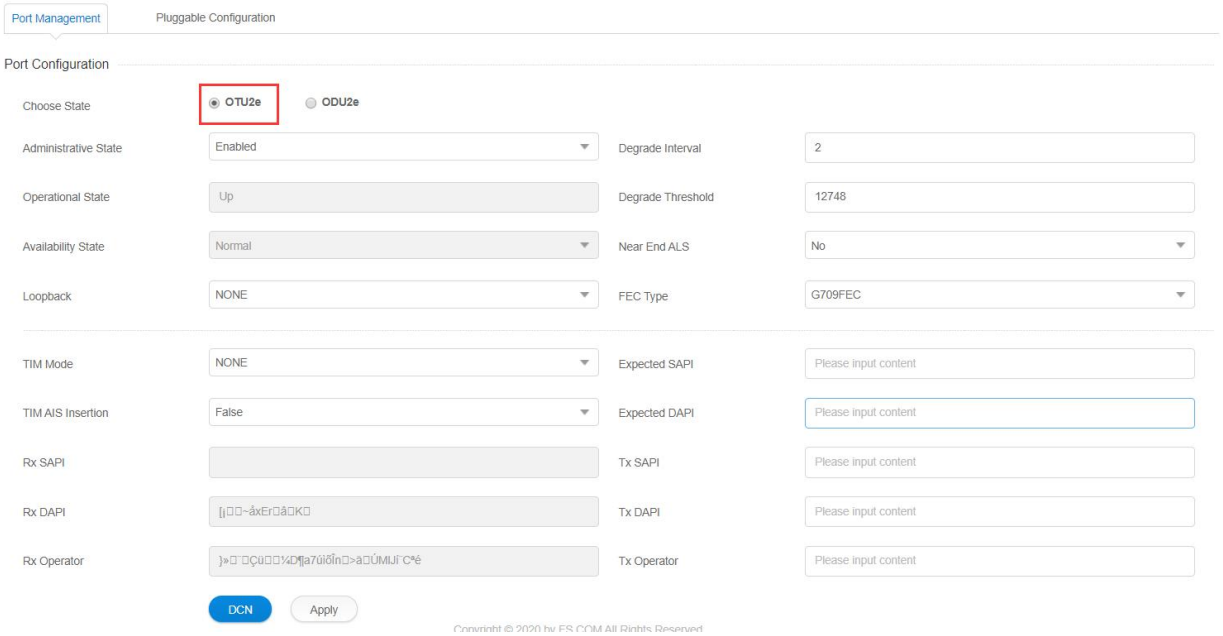



Figure4-18 OTU2e Toolbar Interface

### 4.4.1.4. ODU4 Configuration

Select NE-Slot 2, click on"*Port1*" and select"*Port Management*"on the right, the port management interface shows up (here we take ODU4 corresponding to HGE_GMP port mode as an example). Click on ODU4 option from"*Port Configuration*"in this interface, as shown in the figure below. It shows ODU4 toolbar interface.

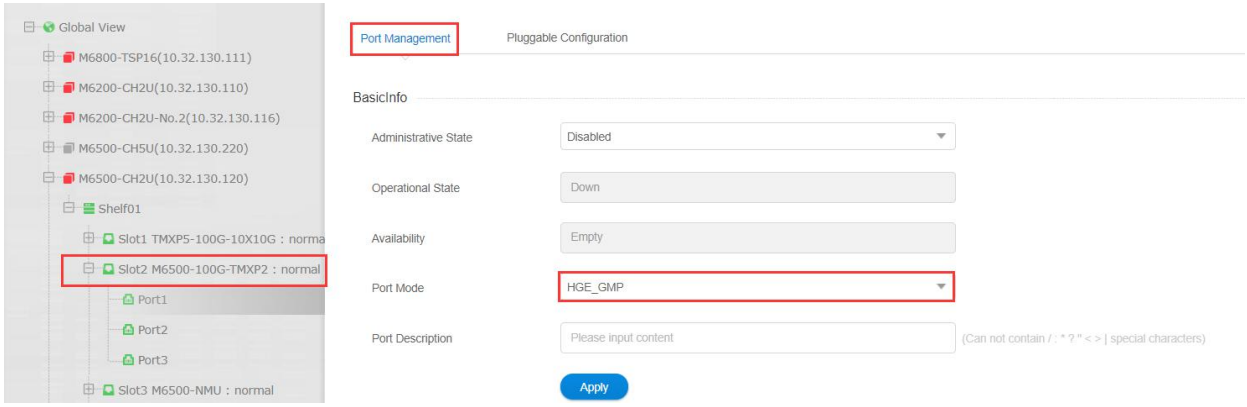



Figure4-19 ODU4 Toolbar Interface

### 4.4.1.5. OTU4 Configuration

Select NE-Slot 2, click on"*Port 3*" and select"*Port Management*"on the right, the port management interface pops up (here we take OTU4 corresponding to OCh (OTU4) port mode as an example). Click on OTU4 option from"*Port Configuration*"in this interface, as shown in the figure below. It shows OTU4 toolbar interface.

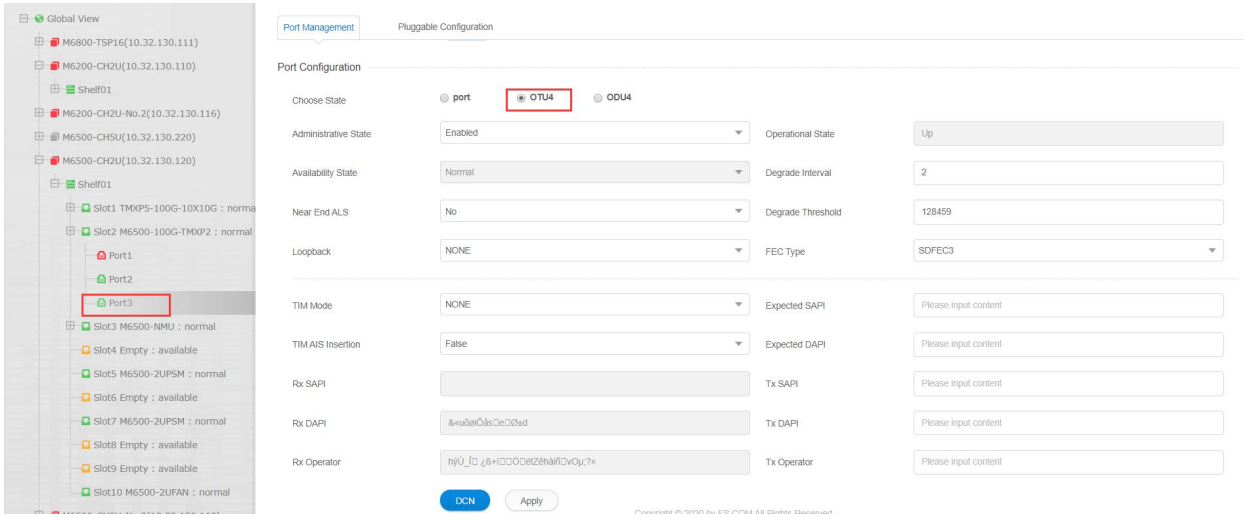



Figure4-20 OTU4 Toolbar Interface

#### 4.4.1.6. OTUC2 Configuration

Select NE-Slot 2, click on"*Port 1*" and select"*Port Management*"on the right, the port management interface shows up (here we take OTUC2 corresponding to OCh (OTUC2) port mode as an example). Click on OTUC2 option from"*Port Configuration*"in this interface, as shown in the figure below. It shows OTUC2 toolbar interface.

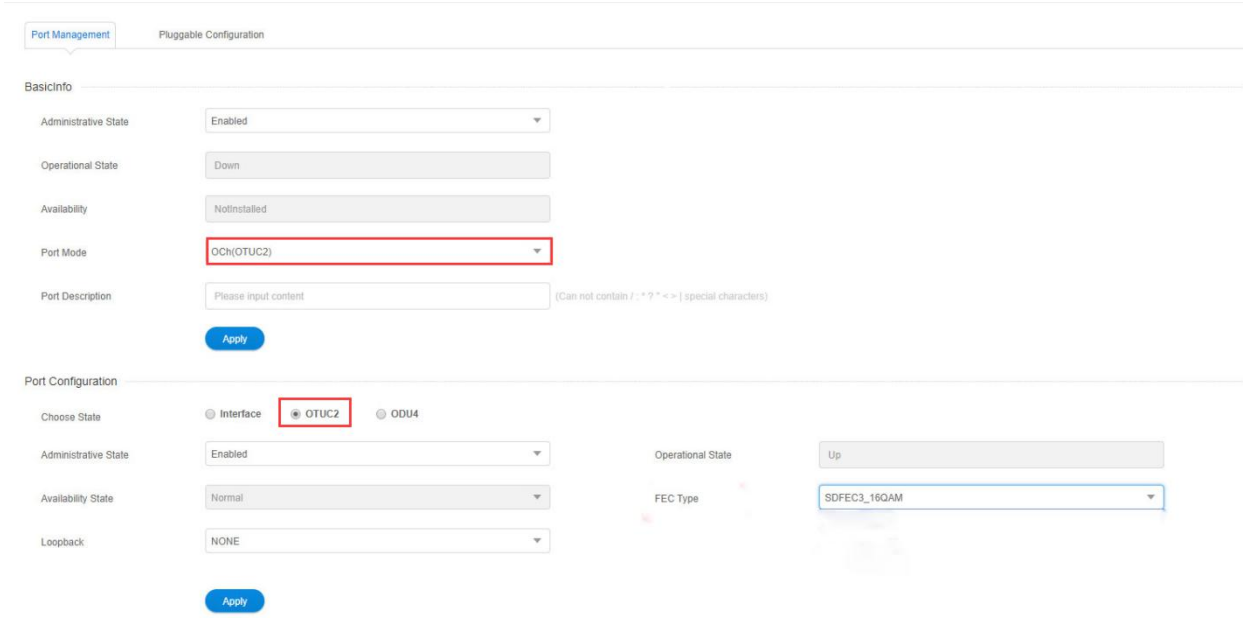



Figure4-21 OTUC2 Toolbar Interface

### 4.4.2. Parameter Description

For different service boards, their client sides and system sides support different port modes, as shown in the figure below:

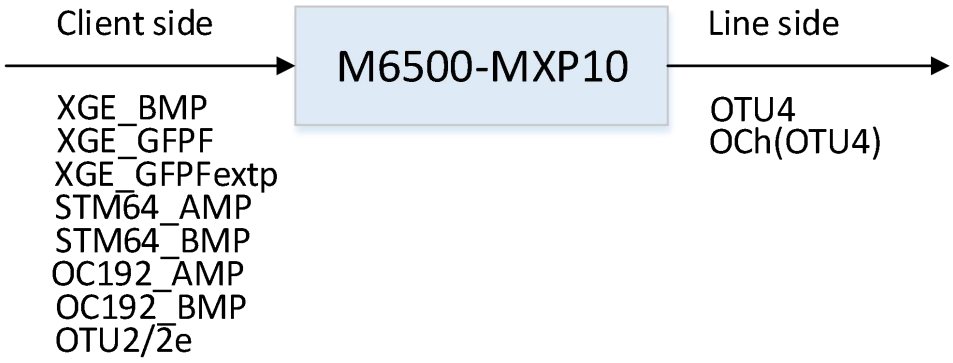



Figure4-22 M6500-MXP10 Port Mode

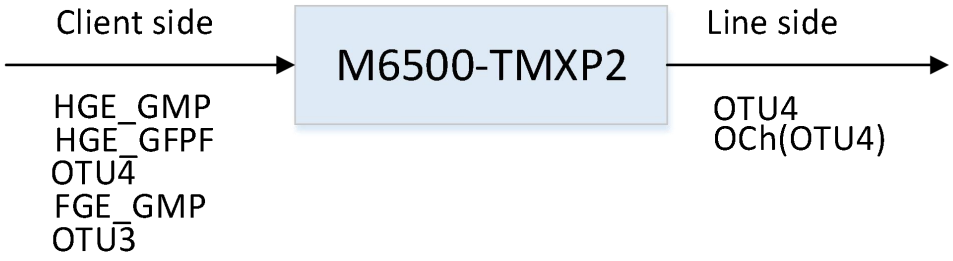



Figure4-23 M6500-TMXP2 Port Mode

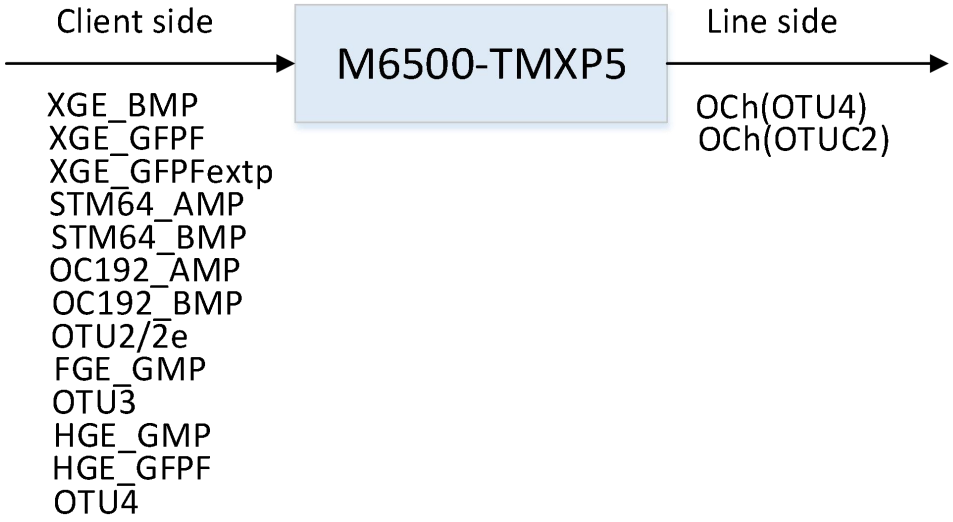
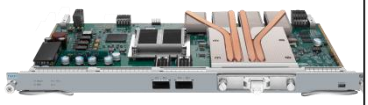



Figure4-24 M6500-TMXP5 Port Mode

Table4-10 Parameter Description of OTN Board

| Board | Interface | Description |
|---|---|---|

| | | |
|---|---|---|
| M6500-MXP10 | 1*100G line side interface (CFP)<br>10 * 10G client side interface (SFP+)<br>  | ◆ The client side signal (10GE, STM-64/OC-192) is mapped to ODU2/2e.<br>◆ The line side signal is demultiplexed from ODU4 to ODU2/2e and connected to the client side signal.<br>◆ 100G line side supports G.709 general FEC or Soft-Decision FEC.<br>◆ 10G OTU2/2e supports I.4 and I.7 EFEC, or G.709 general FEC<br>◆ Support GCC0, GCC1 and GCC2 in-band management<br>◆ Support SNC/I and SNC/N transmission protection |
| M6500-TMXP2 | 1*100G line side interface (CFP)<br>1*100G (QSFP28) or 2*40G client side interface (QSFP+)<br>  | ◆ The client side 100G signal (100GE or OTU4) is mapped to ODU4.<br>◆ The client side 40G signal (40GE or OTU3) is mapped to ODU3.<br>◆ The line side signal is terminated to ODU4 or ODU3, and is connected to the client side signal.<br>◆ 100G line side supports G.709 general FEC or Soft-Decision FEC<br>◆ Support GCC0, GCC1 and GCC2 in-band management<br>◆ Support SNC/I and SNC/N transmission protection |
| M6500-TMXP5 | 1*100G/200G line side interface (CFP2)<br>2*100G (QSFP28) or 4*40G client side interface (QSFP+) or 20* (4x5) 10G client side interface<br>  | ◆ The client side 100G signal (100GE or OTU4) is mapped to ODU4<br>◆ The client side 40G signal (40GE or OTU3) is mapped to ODU3.<br>◆ The client side 10G signal (10GE, STM-64/OC-192) is mapped to ODU2/2e<br>◆ The 100G signal on the line side is demultiplexed by ODU4 to ODU2/2e or ODU3, and is connected to the client side signal<br>◆ The 200G signal on the line side is demultiplexed from ODUC2 to ODU4, and then demultiplexed to low-order ODU2/2e or ODU3, which is connected to the client side signal<br>◆ 100G line side supports G.709 general FEC or Soft-Decision FEC<br>◆ 200G line side supports Soft-Decision FEC<br>◆ 10G OTU2/2e supports I.4 and I.7 EFEC, or G.709 general FEC<br>◆ Support GCC0, GCC1, GCC2, GCC1+2 in-band management |

## 4.5. Configuration of Optical Module Information

The operation steps to view optical module information are as follows:

Select NE-Slot1, click on "*Port*"and select "*Pluggable Configuration*"on the right, as shown in the figure below:

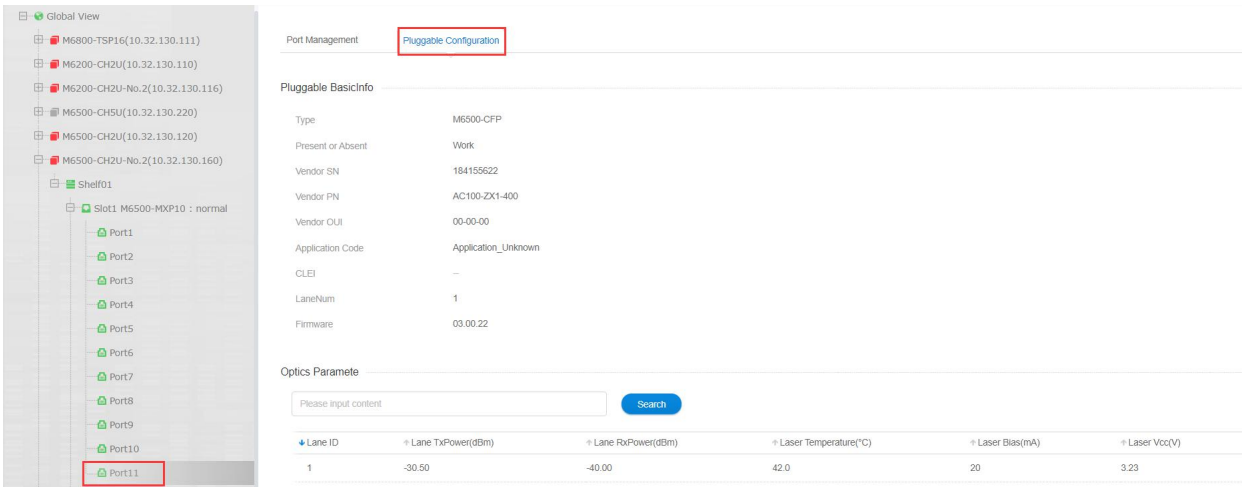



Figure4-25 View Optical Module Information

When the optical module is DWDM and the wavelength is tunable, its frequency and wavelength can be configured. The configuration interface is under the port configuration-interface menu.

### 4.5.1. SFP/SFP+ Optical Transceiver Information

The SFP and SFP + optical module information of M Series NMS system is not separately distinguished. Open the optical module configuration interface; you can see the basic information and parameter information of the optical module, as shown in the figure below:

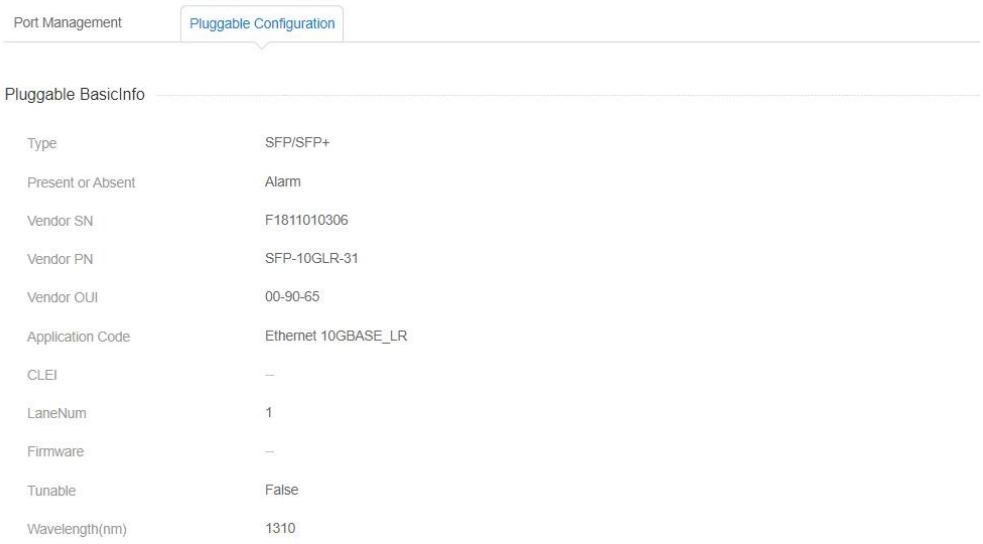



Figure4-26 Basic Information of SFP/SFP+ Optical Transceiver

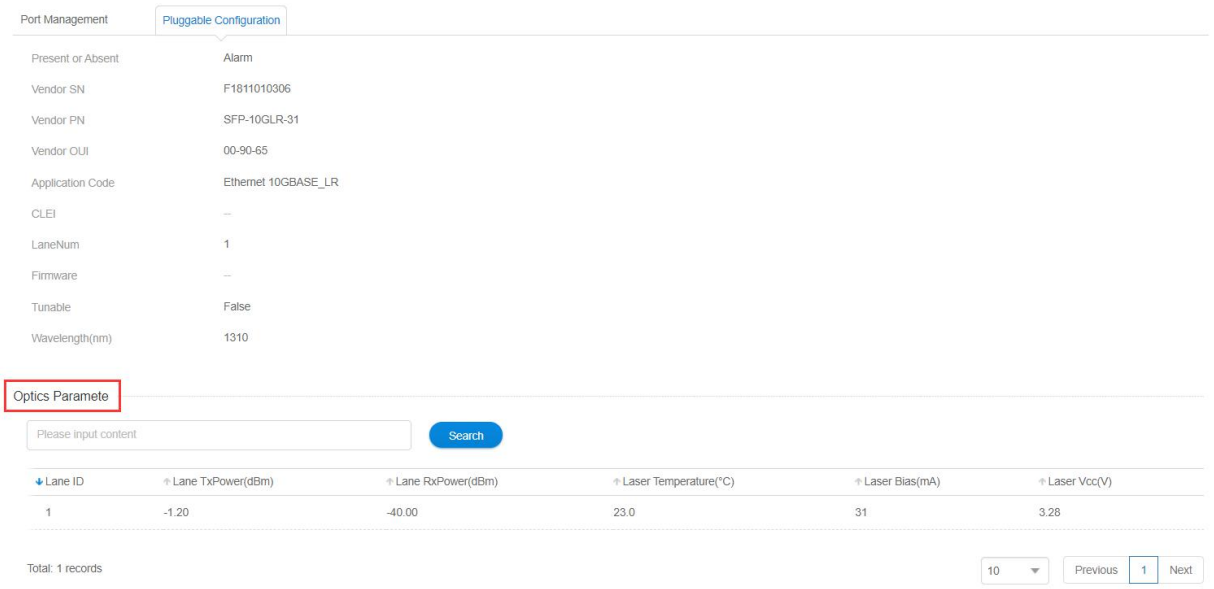



Figure4-27 Parameter Information of SFP/SFP+ Optical Transceiver

## 4.5.2. WDM CFP Optical Transceiver Information

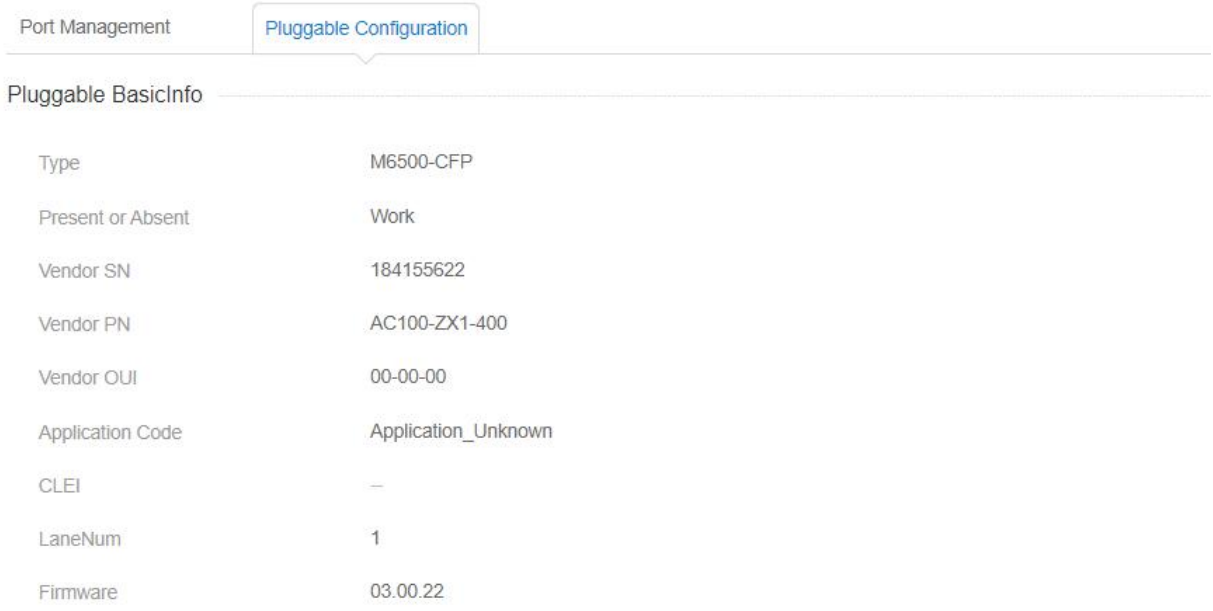



Figure4-28 Parameter Information of WDM CFP Optical Transceiver


Figure4-29 Parameter Information of WDM CFP Optical Transceiver

### 4.5.3. WDM CFP Optical Transceiver Configuration

Configure the port mode as OCh (OTU4), insert a WDM CFP optical module and select the interface; you can configure the working wavelength and transmitting optical power of the optical module, as shown in the figure below:

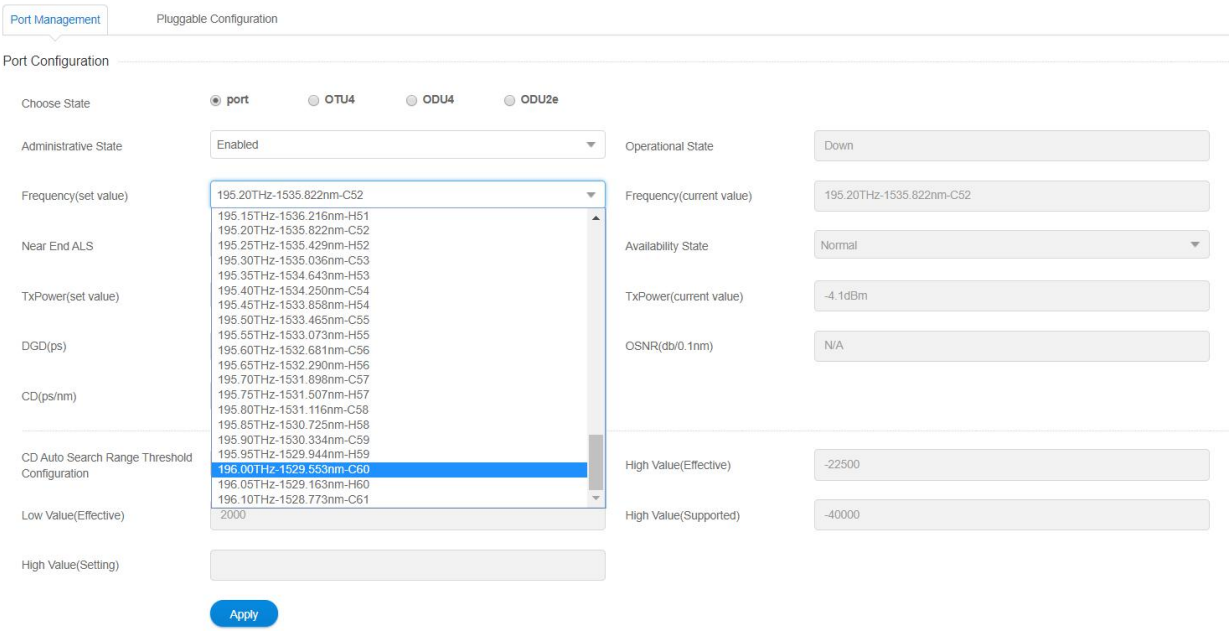



Figure4-30 Configure Operating Wavelength of WDM CFP

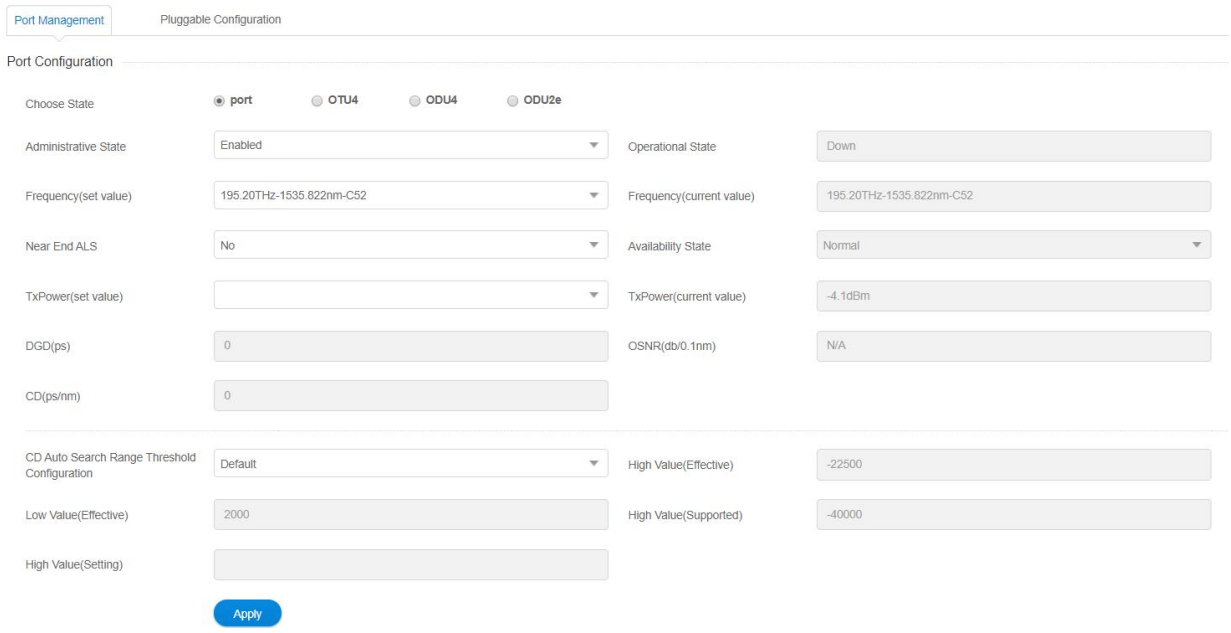



Figure 4-31 Parameter Reading of WDM CFP Optical Transceiver

### 4.5.4. WDM CFP2 Optical Transceiver Information

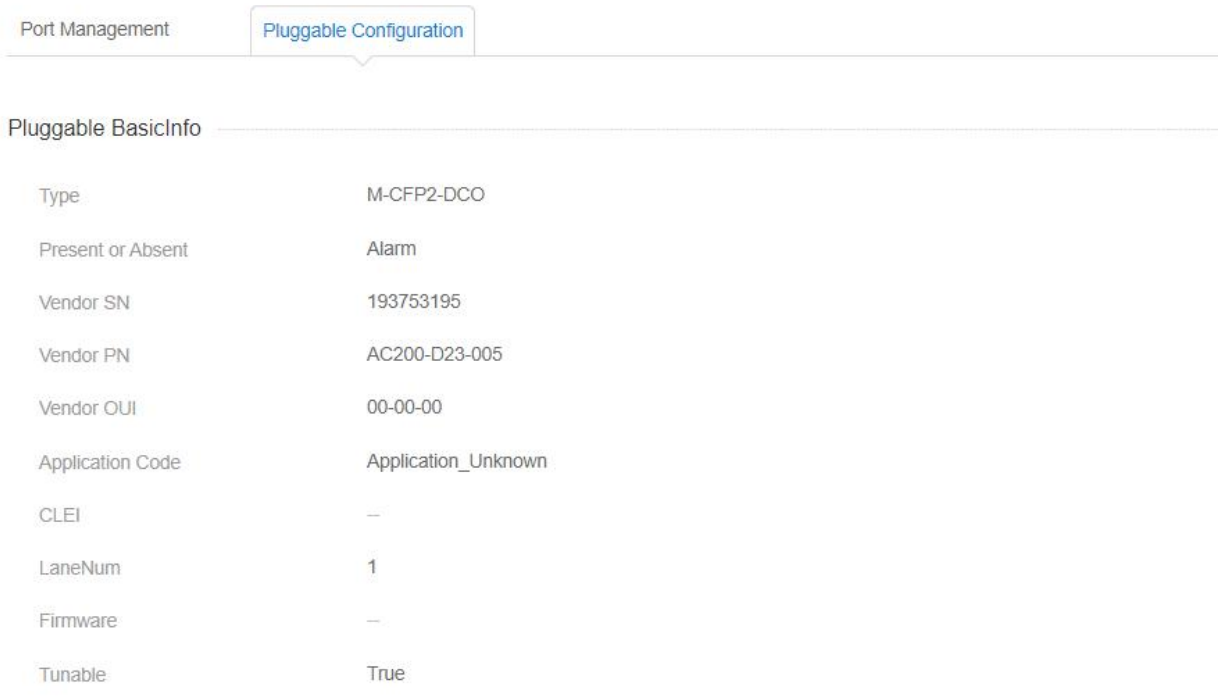



Figure 4-32 Basic Information of WDM CFP2 Optical Transceiver

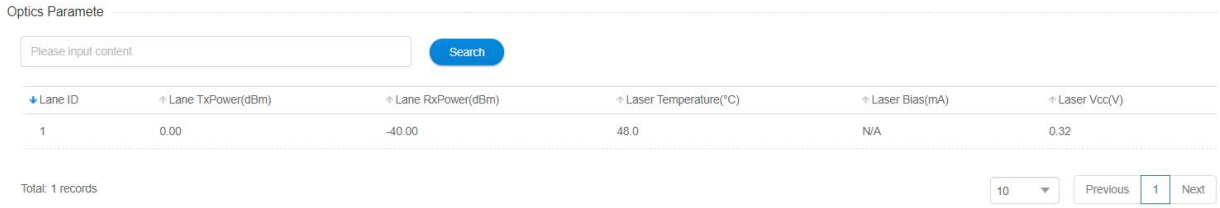



Figure 4-33 Parameter of WDM CFP2 Optical Transceiver

### 4.5.5. WDM CFP2 Optical Transceiver Configuration

Configure the port mode as OCh (OTUC2), insert a WDM CFP2 optical module and select the interface; you can configure the working wavelength and transmitting optical power of the optical module, as shown in the figure below:

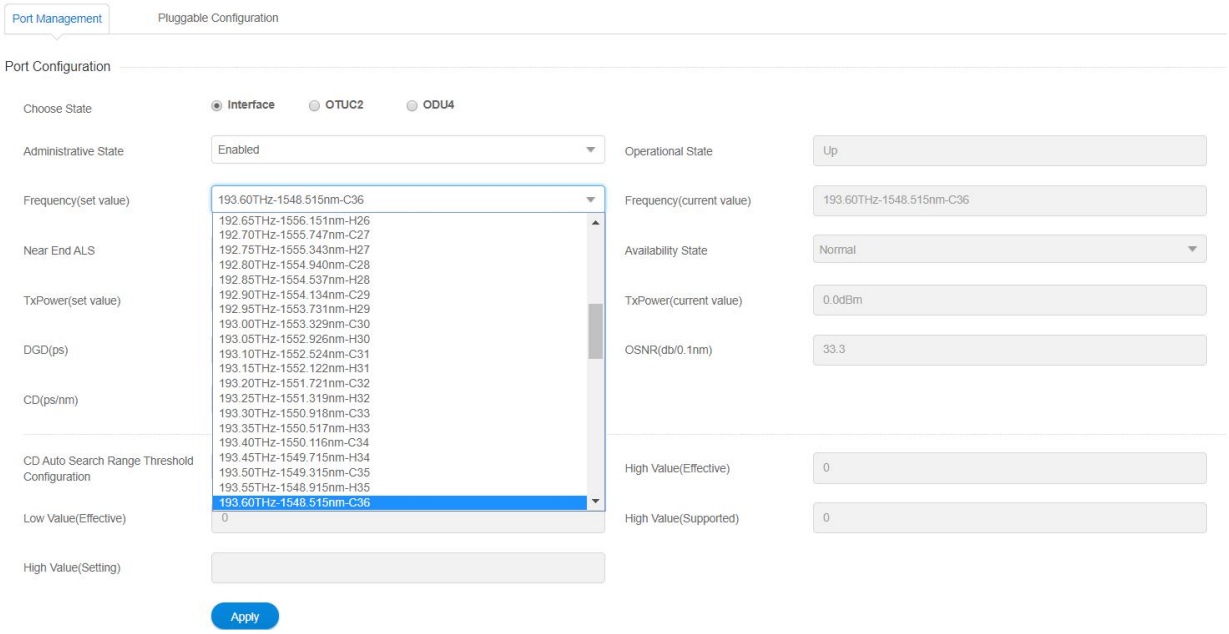



Figure 4-34 Configure Operating Wavelength of WDM CFP2

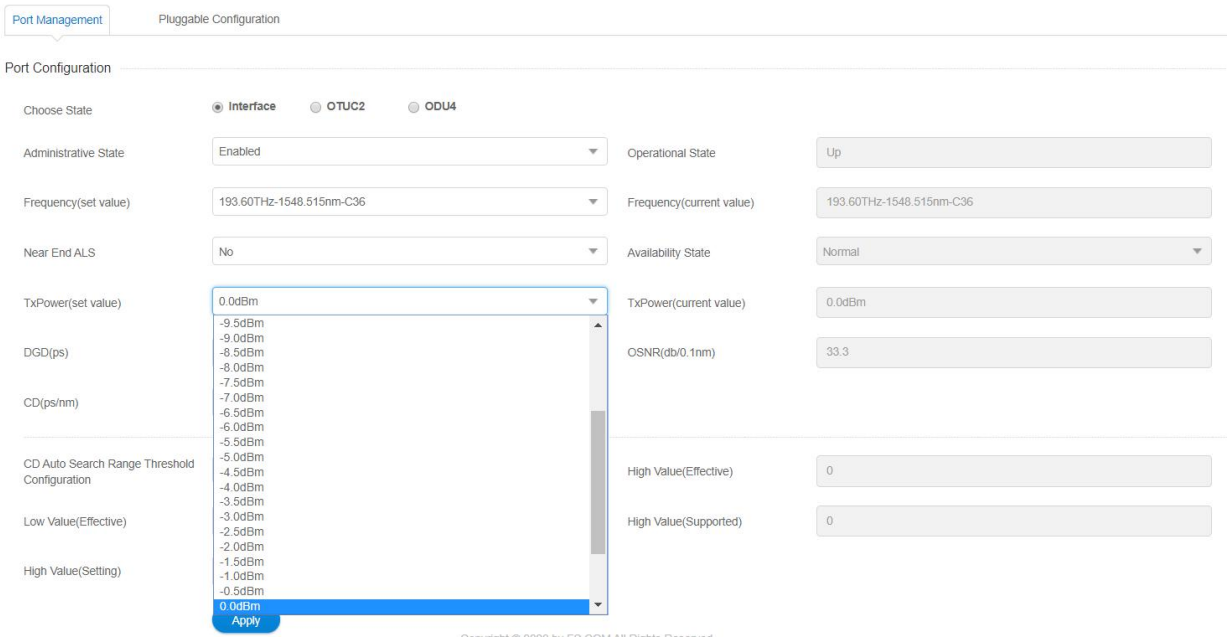



Figure 4-35 Configure WDM CFP2 Transmit Optical Power

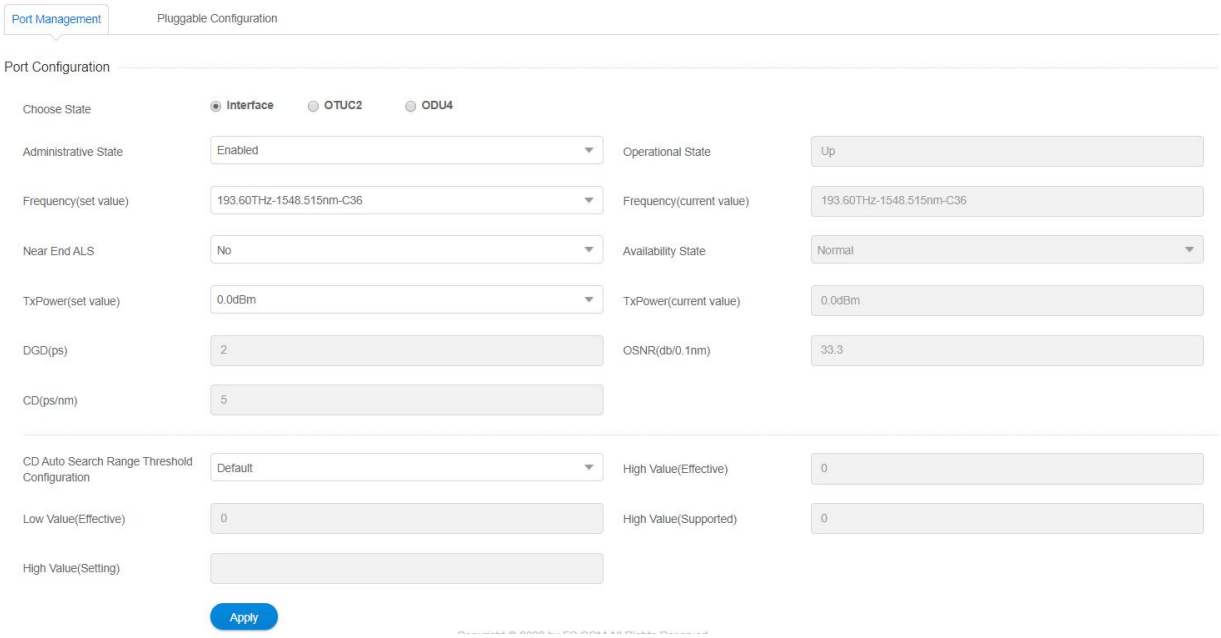



Figure 4-34 Parameter Reading of WDM CFP2 Optical Transceiver

# 5. Service Configuration

**Prerequisite**

1. Network devices and lines are normal.
2. The NE and the NMS system have been configured.
3. The NMS server has been running and logged into the NMS system.

## 5.1. Electric Cross-Connect Introduction

OTN electric cross-connect technology is based on ODUk as the particle for mapping, multiplexing and cross-connection. OTN electric cross-connect equipment also introduces high-order / low-order optical channel data unit (ODUk / ODUj). There are four types of OTN electric cross-connect:

- Unidirectional cross-connection without protection: one-way cross-connection, that is, the service is transmitted from site A--->site Z without line protection.
- Bidirectional cross-connection without protection: bidirectional cross-connection, that is, the service is transmitted from site A--->site Z and from site Z--->site A without line protection.
- Unidirectional cross-connection with protection: one-way cross-connection, that is, the service is transmitted from site A--->site Z. You can choose site A or site Z as the protection site (either of them). If site A is selected as the protection site, the service will be received only. When the service of site A fails, the service will be sent from A site protection (A') to Z site. If Z-site protection is selected, the service is double transmitted, that is, the service of site A is simultaneously sent to site Z- and Z site protection (Z').
- Bidirectional cross-connection with protection: bidirectional cross-connection, that is, the service is transmitted from site A--->site Z and from site Z--->site A. The service is double transmitted and selectively received. If Z site protection is selected, the service of site A is simultaneously transmitted to site Z and Z protection site (Z'); otherwise, if A site protection is selected, the service of site Z is simultaneously transmitted to site A and A protection site (A').

**Configuration Steps**

Select NE, click on"*Shelf01*"and select"*Business Configuration*"on the right，the operation steps are as shown in the figure below:

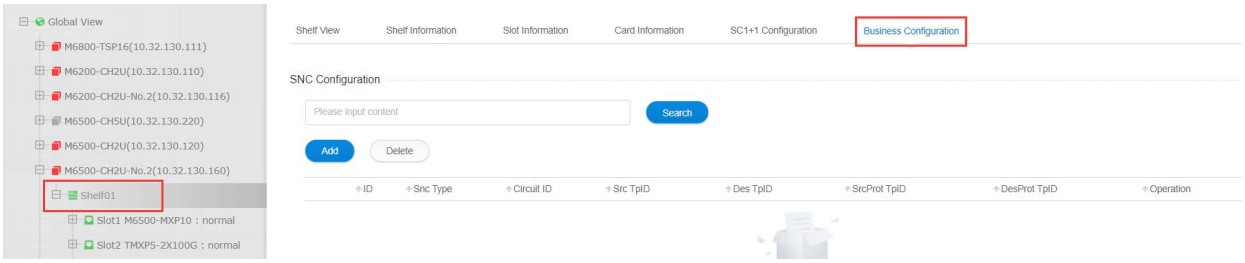



Figure5-1 Operation Steps of SNC Configuration

The"*SNC Configuration*"interface shows up, as shown in the figure below:

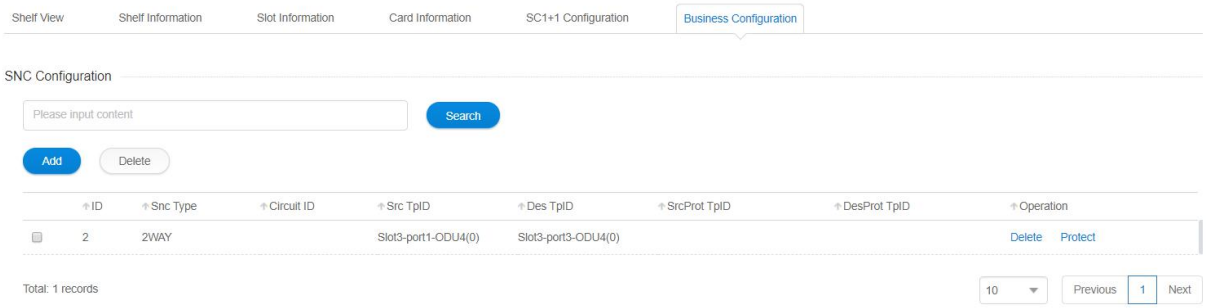



Figure5-2 Traffic Configuration Interface

The configuration includes two types—with protection and without protection. For the type with protection, there are A protection and Z protection, as shown in the figure below:

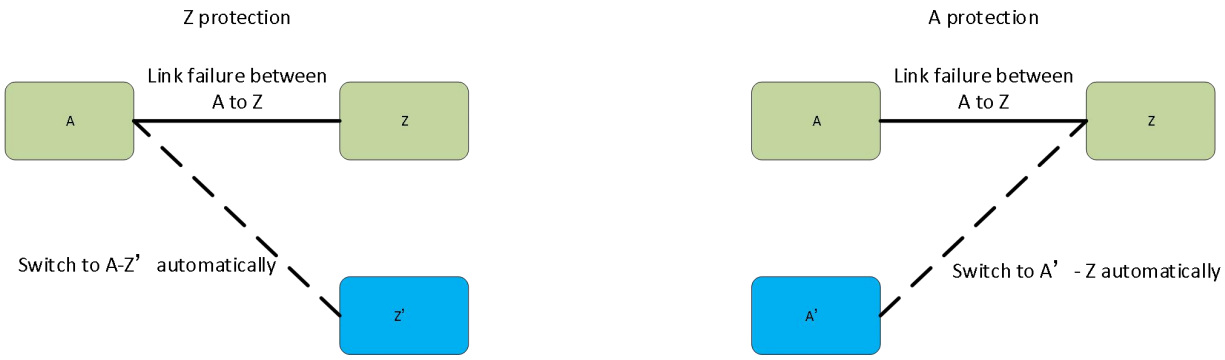



Figure5-3 Protection Schematic Diagram

### 5.1.1. Unidirectional Cross-Connection without Protection

Select NE, click on"*Shelf01*"and select"*Add*"button in "*SNC Configuration*" of"*Business Configuration*"interface; you can create unidirectional cross-connection without protection (here we take M6500-MXP10 port 1-port 11 cross-connection as an example to select the corresponding slot, cross-connection type and capacity information).

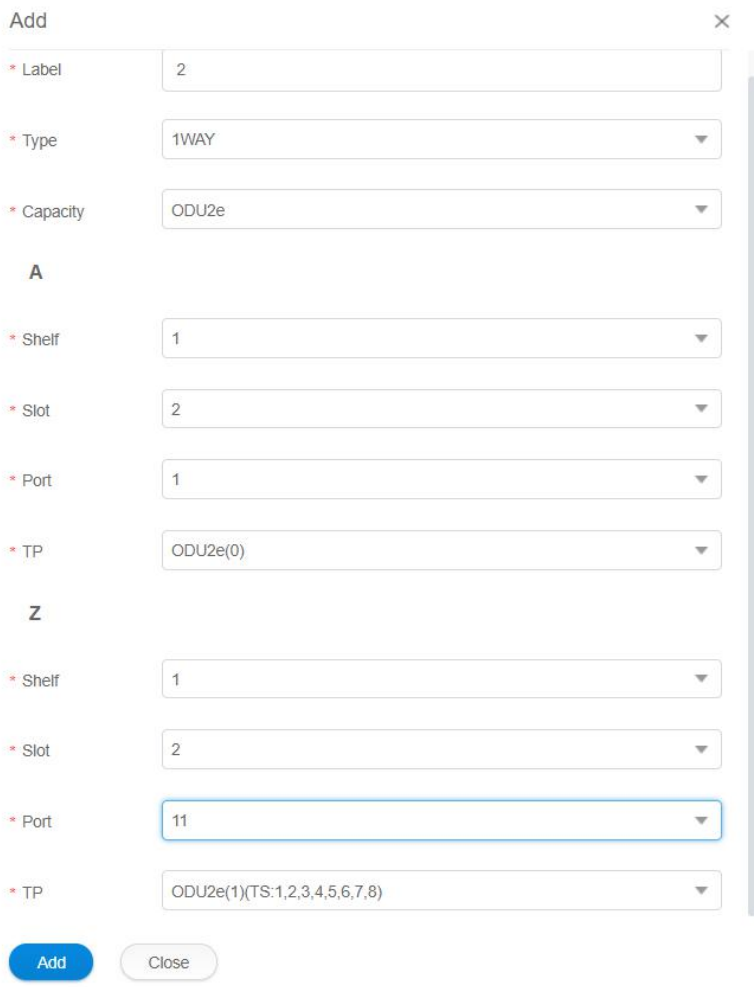



Figure5-4 Configuration of Unidirectional Cross-Connection without Protection

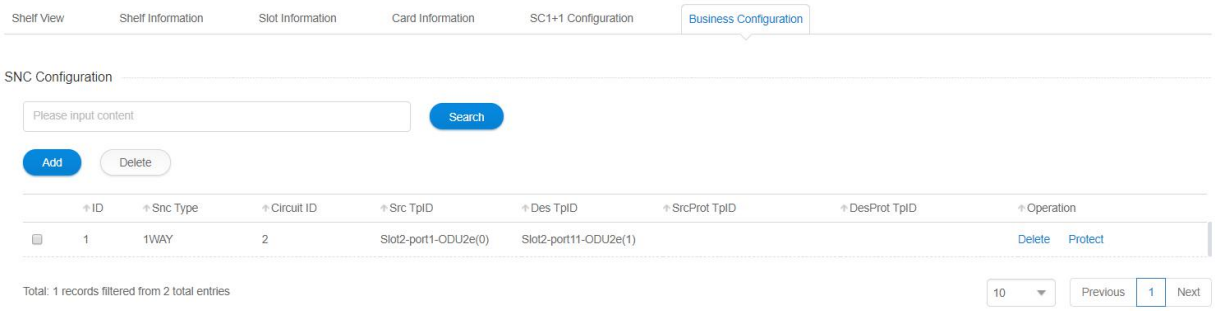



Figure5-5 Configuration Result of Unidirectional Cross-Connection without Protection

### 5.1.2. Bidirectional Cross-Connection without Protection

Select NE, click on"*Shelf01*"and select"*Add*"button in "*SNC Configuration*" of"*Business Configuration*"interface; you can create bidirectional cross-connection without protection (here we take M6500-MXP10 port 1-port 11 cross-connection as an example to select the corresponding slot, cross-connection type and capacity information).

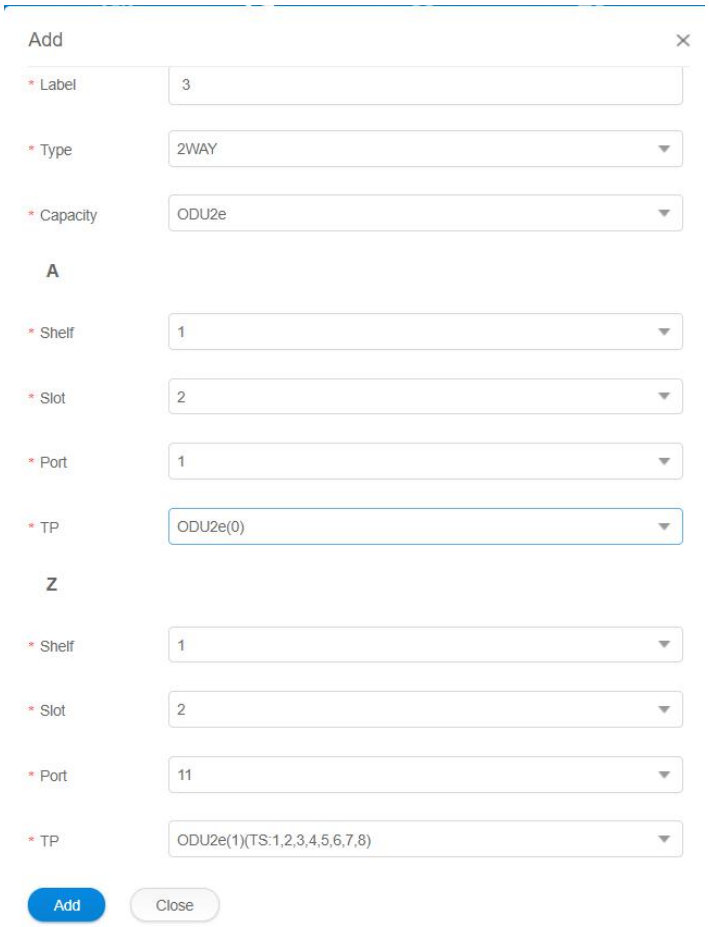



Figure5-6 Configuration of Bidirectional Cross-Connection without Protection

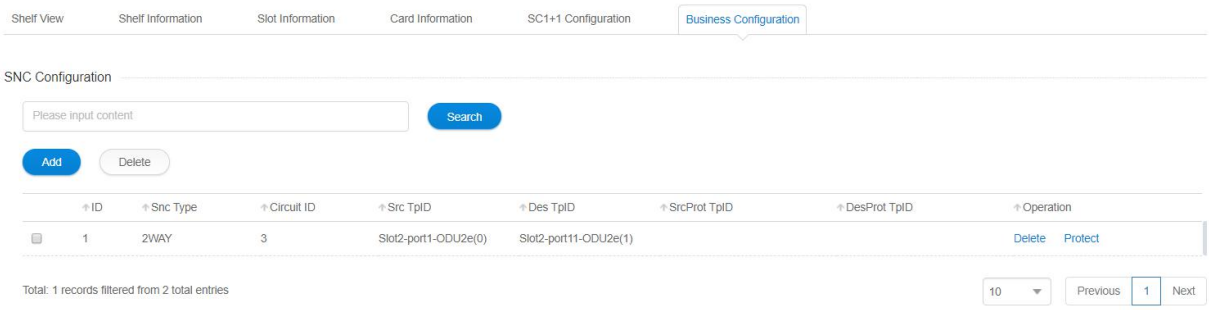



Figure5-7 Configuration Result of Bidirectional Cross-Connection without Protection

### 5.1.3. Unidirectional Cross-Connection with Protection

Select NE, click on"*Shelf*",click on"*Business Configuration*"and select"*Add*"button in "*SNC Configuration*" of"*Business Configuration*"interface; you can create unidirectional cross-connection with protection (here we take M6500-MXP10 as an example, the 11 ports from Port 1-Port 11 of one board create unidirectional cross-connection with protection, and the 11 ports of the other board act as the protection to select the corresponding slot, cross-connection type and capacity information).

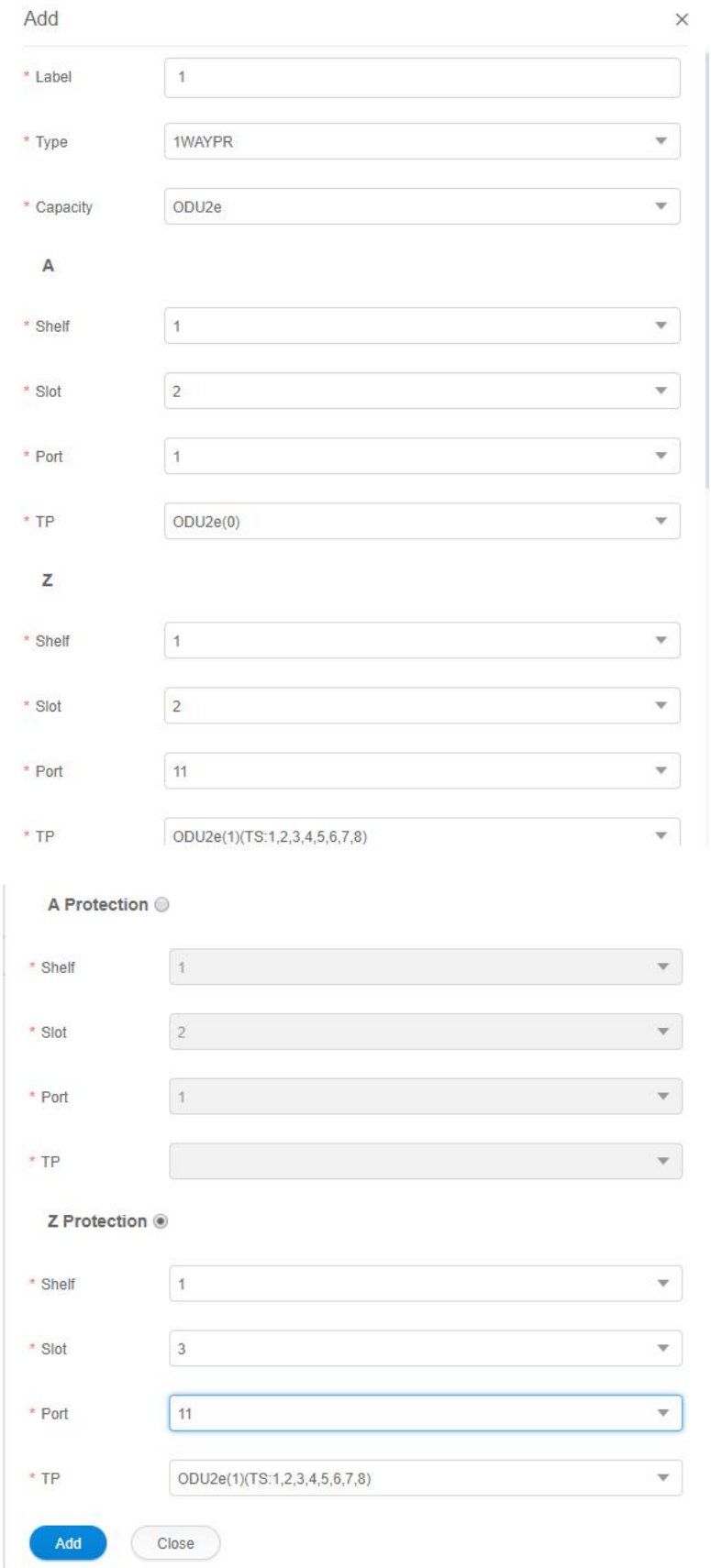



Figure5-8 Configuration of Unidirectional Cross-Connection with Protection

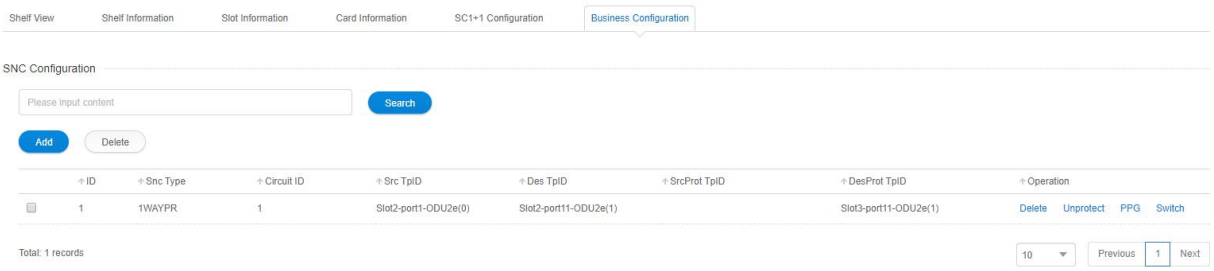
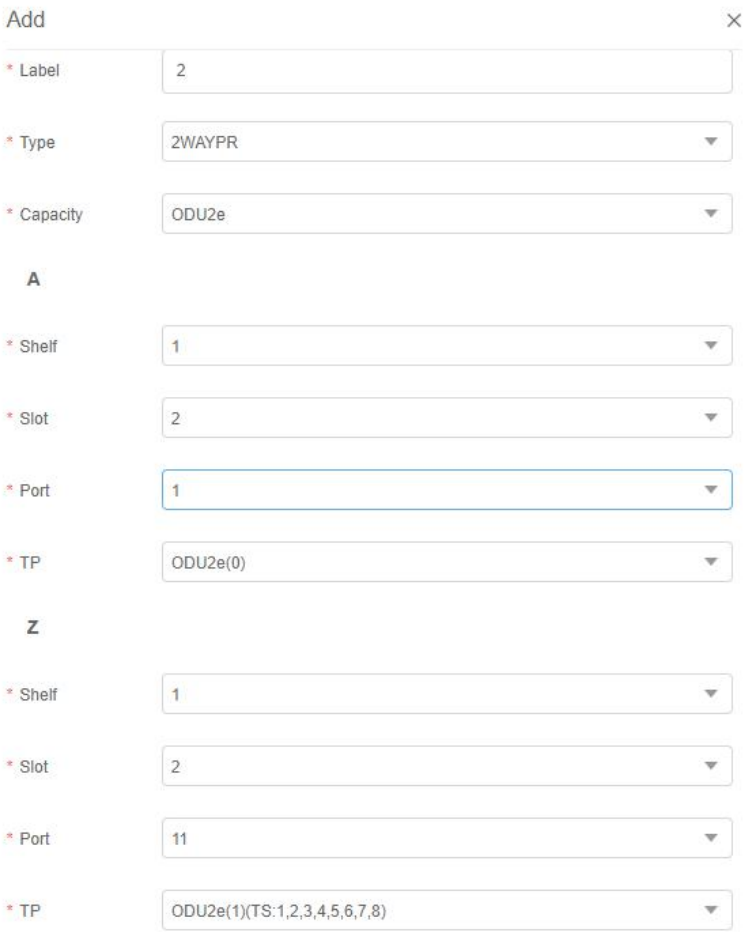



Figure5-9 Configuration Result of Unidirectional Cross-Connection with Protection

### 5.1.4. Bidirectional Cross-Connection with Protection

Select NE, click on"*Shelf*"and select"*Add*"button in "*SNC Configuration*" of"*Business Configuration*"interface; you can create bidirectional cross-connection with protection (here we take M6500-MXP10 as an example, the 11 ports from Port 1-Port 11 of one board create bidirectional cross-connection with protection, and the 11 ports of the other board act as the protection to select the corresponding slot, cross-connection type and capacity information).



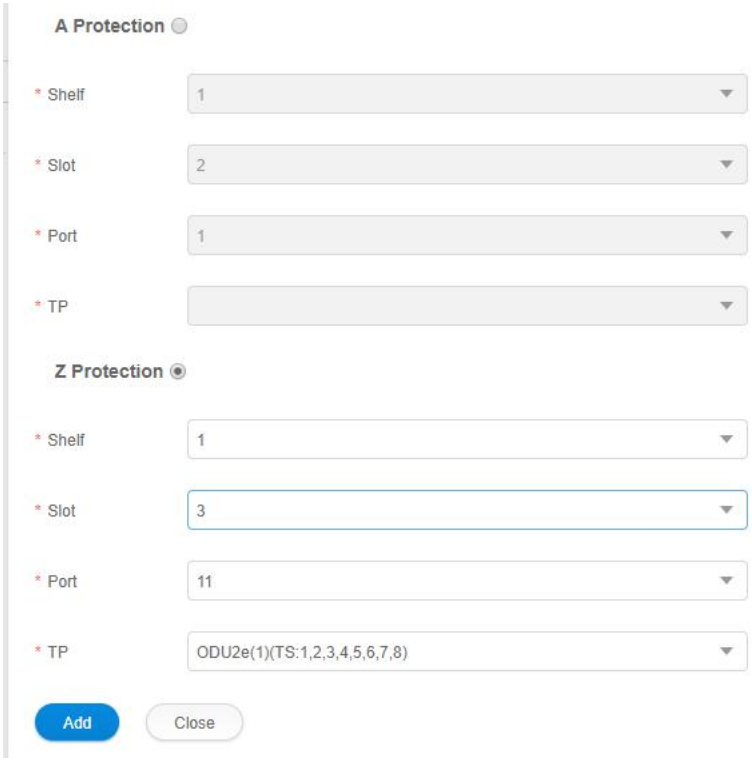



Figure5-10 Configuration of Bidirectional Cross-Connection with Protection

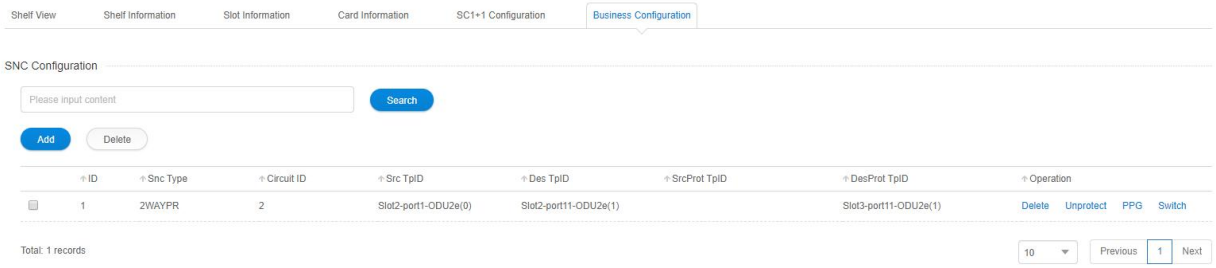



Figure5-11 Configuration Result of Bidirectional Cross-Connection with Protection

# 5.2. Service Type

## 5.2.1. Service Type

Select NE-Slot 1, click on“*Port1*”and select“*Port Management*”on the right, as shown in the figure below:

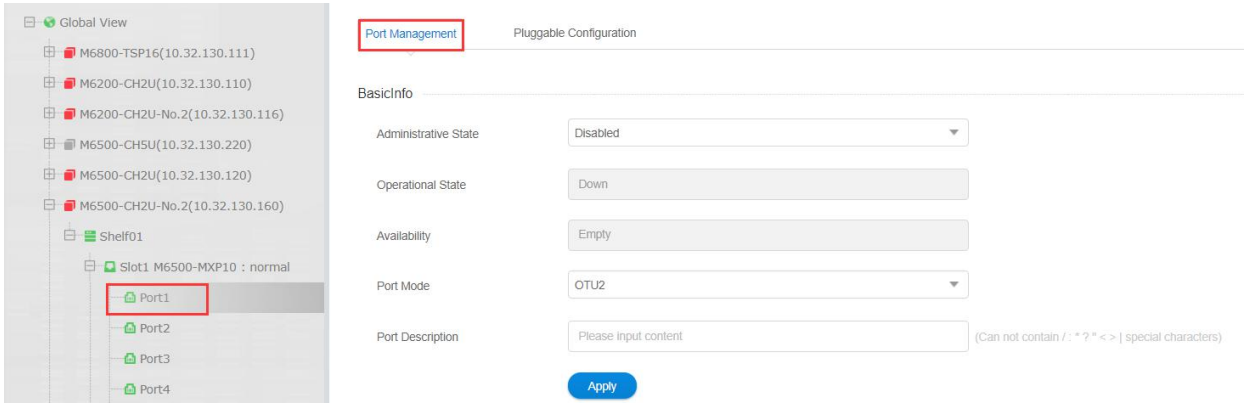


Figure5-12 Operation Steps of How to View Service Type

As shown in the figure below, open the port management interface, and select the service type from basic information-port mode.

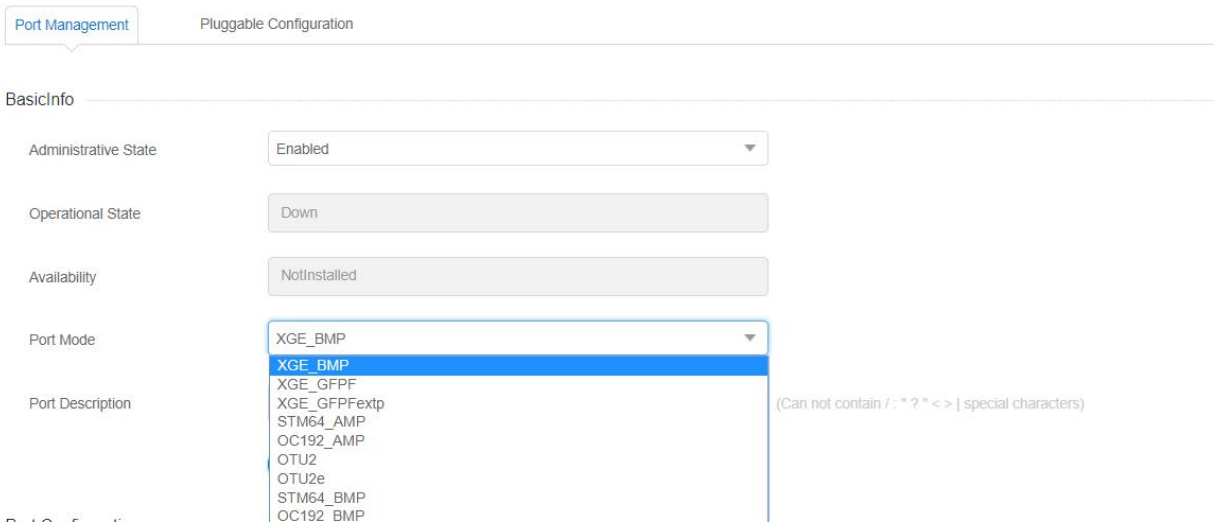



Figure5-13 Port Service Type Interface

## 5.2.2. Service Mapping

In M Series NMS, you can select the service mapping mode in the port management-port mode interface. Here we take the M6500-MXP10 board as an example. As shown in the figure below, the left of the underline is port mode and the right is the mapping mode (OTU signal is not included).


Figure5-14 Mapping Mode Interface

### 5.2.2.1. AMP

AMP (Asynchronous Mapping Procedure)has no restrictions on the structure of the mapped signal (whether the signal has a frame structure or not), and no need to synchronize with the network (for example, PDH signal and SDH network are not fully synchronized). The mapping method of adapting the signal into VC by adjusting the code rate makes the rate of the service layer signal match that of the client layer signal.

Here we take M6500-MXP10 board as an example. Select NE-Slot, click on"*Port1*"and select"*Port Management*"on the right, and then select STM64_AMP mode.

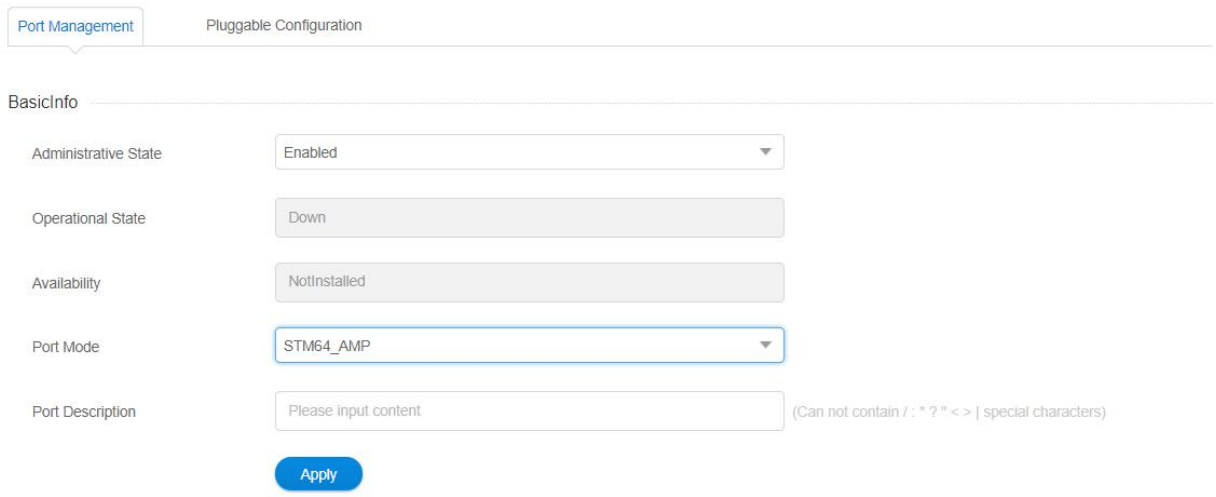



Figure5-15 STM64_AMP Mapping Mode

#### 5.2.2.2. BMP

BMP (Bit-synchronous Mapping Procedure BMP) requires the rate of the service layer signal to match that of the client layer signal, and there is no frequency deviation.

Here we take M6500-MXP10 board as an example. Select NE-Slot, click on"*Port1*"and select"*Port Management*"on the right, and then select XGE_BMP mode.

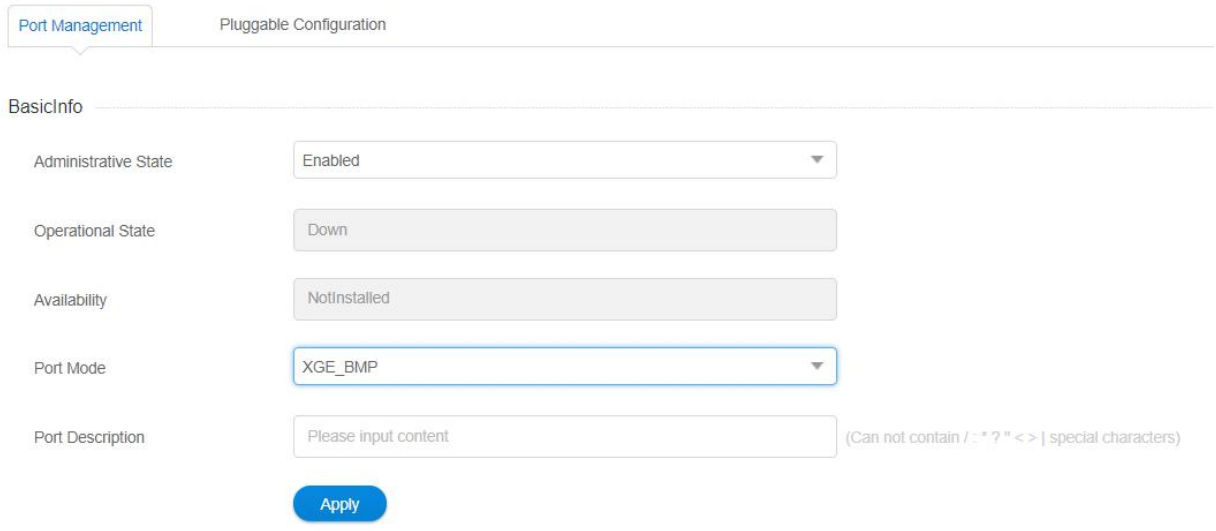



Figure5-16 XGE_BMP Mapping Mode

#### 5.2.2.3. GMP

For GMP (Generic Mapping Procedure), in all cases (such as the maximum ppm frequency offset of the client signal and the minimum ppm frequency offset of the server signal), the rate of the server signal must be higher than the rate of the client signal. Any rate of the client signal can be mapped to any server payload rate by using this method, that is, the rate of the service layer is required to be greater than that of the client layer; otherwise, it cannot be transmitted.

Here we take M6500-TMXP5 board as an example. Select NE-Slot, click on"*Port 3*"and select"*Port Management*"on the right, and then select HGE_GMP mode.

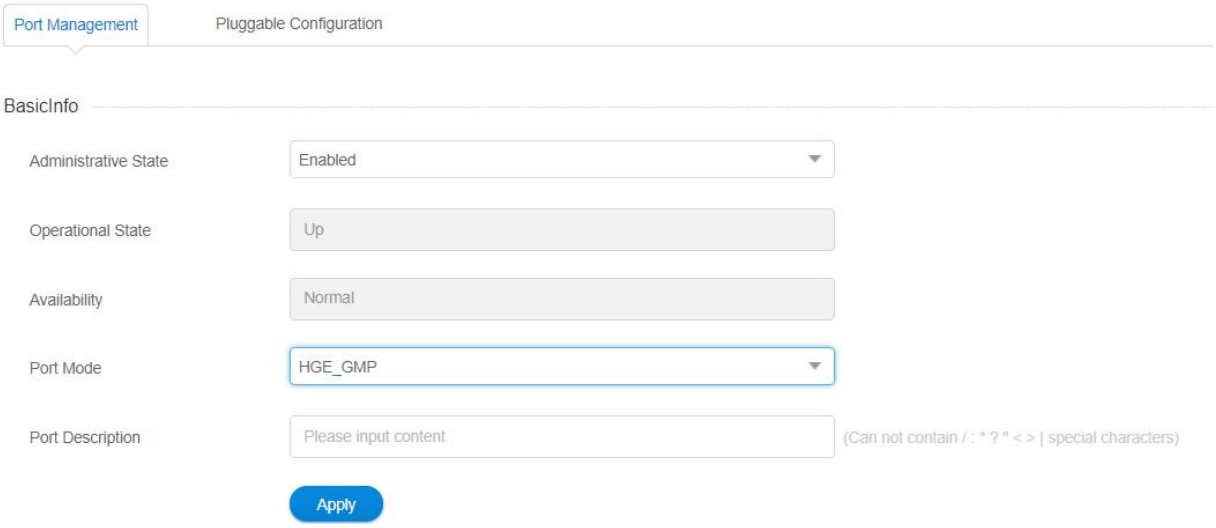



Figure5-17 HGE_GMP Mapping Mode

### 5.2.2.4. GFP-F

The encapsulation of GFP-F (Frame mapped Generic Framing Procedure) can completely map the traffic signal frame into a GFP frame with variable length and there is no need to make any changes to the encapsulated data. In this method, data processing is performed after receiving a complete data frame, which is most suitable for packet data with variable length such as Ethernet services.

Here we take M6500-MXP10 board as an example. Select NE-Slot, click on"*Port1*"and select"*Port Management*"and then select XGE_GFPF mode.

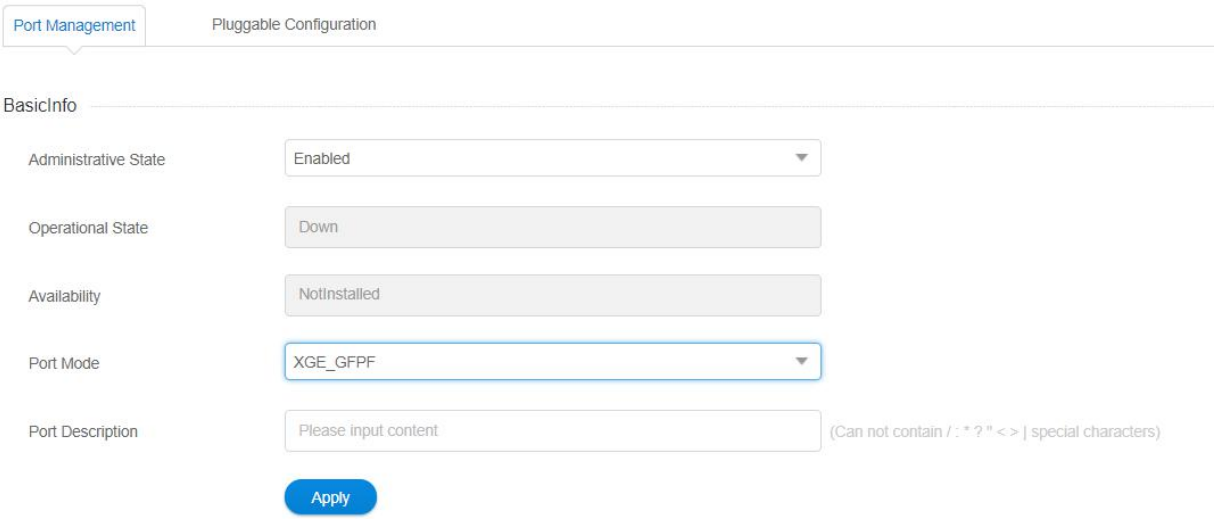



Figure5-18 XGE_GFPF Mapping Mode

### 5.2.2.5. GFP-Fextp

Here we take M6500-MXP10 board as an example. Select NE (10.32.130.160)-Slot 2, right click on "*Port 1*"and select "*Port Management*", and then select XGE_GFPFextp mode.

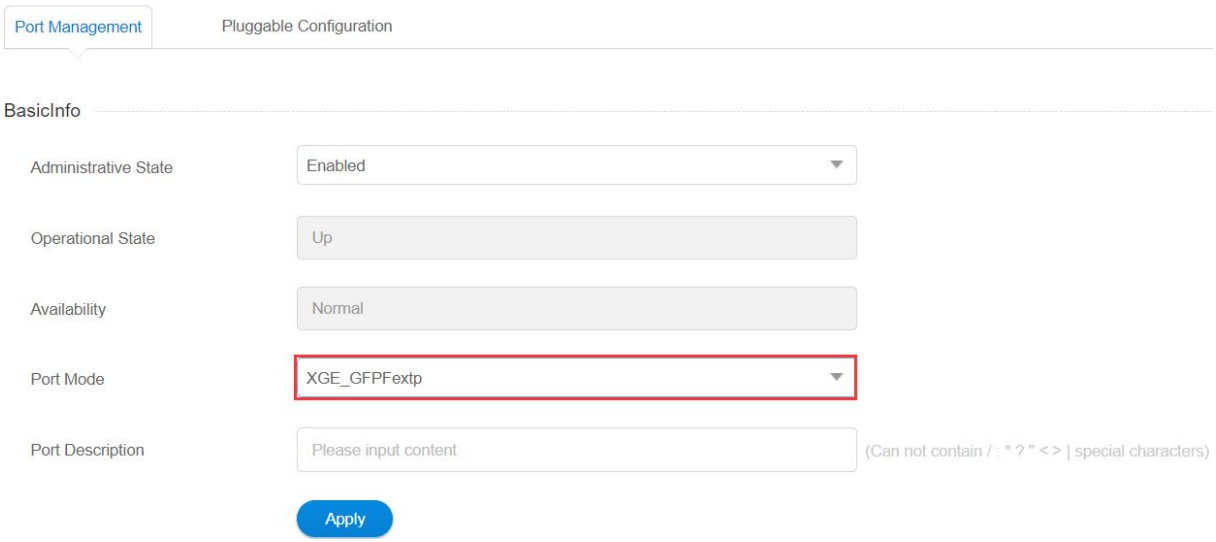



Figure5-19 XGE_GFPFextp Mapping Mode

# 5.3. Service Configuration Process

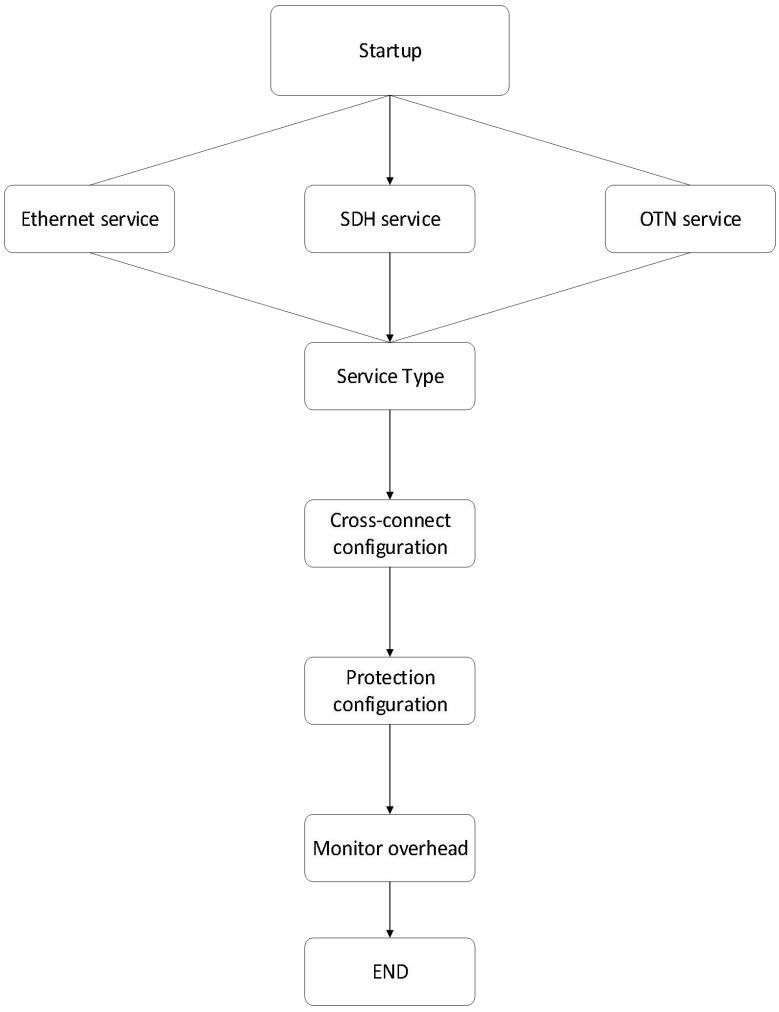



Figure5-20 Service Configuration Process

# 5.4. Configuration instructions

## 5.4.1. M6500-MXP10

The port type of M6500-MXP10 includes 1 (port 11)*100G line side interface (CFP) and 10 (port 1-10)*10G client side interfaces (SFP+).

### 5.4.1.1. Service Type

- **Line Side Port**

Select NE-Slot 1, click on"*Port11*"and select"*Port Management*"on the right，the operation interface is as shown in the figure below:

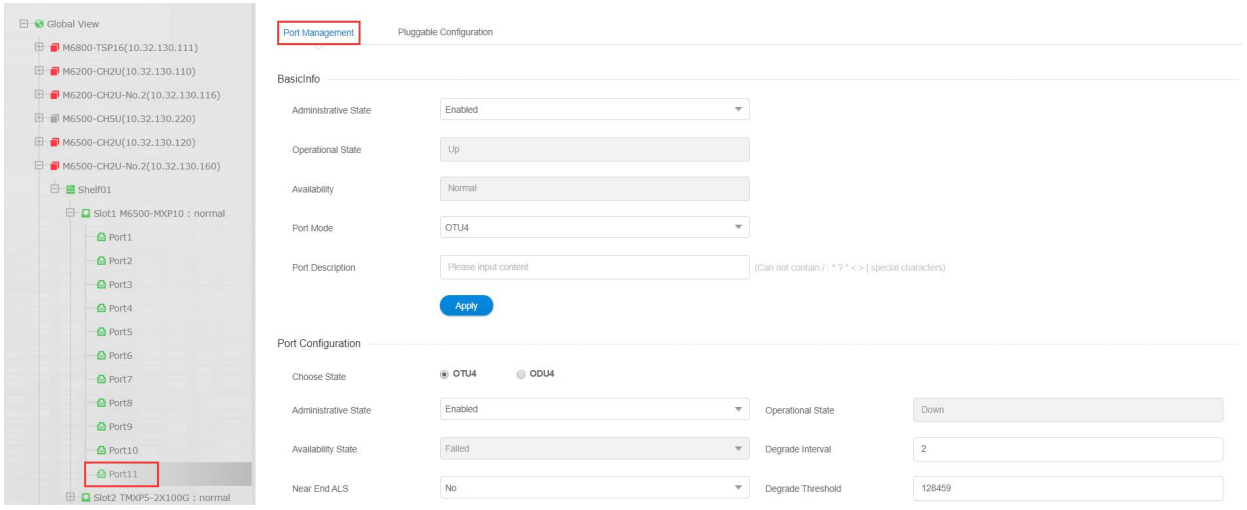



Figure5-21 M6500-MXP10 Line Side Port Information

The line side port management interface is as shown in the figure below, and the service type can be selected in port mode.

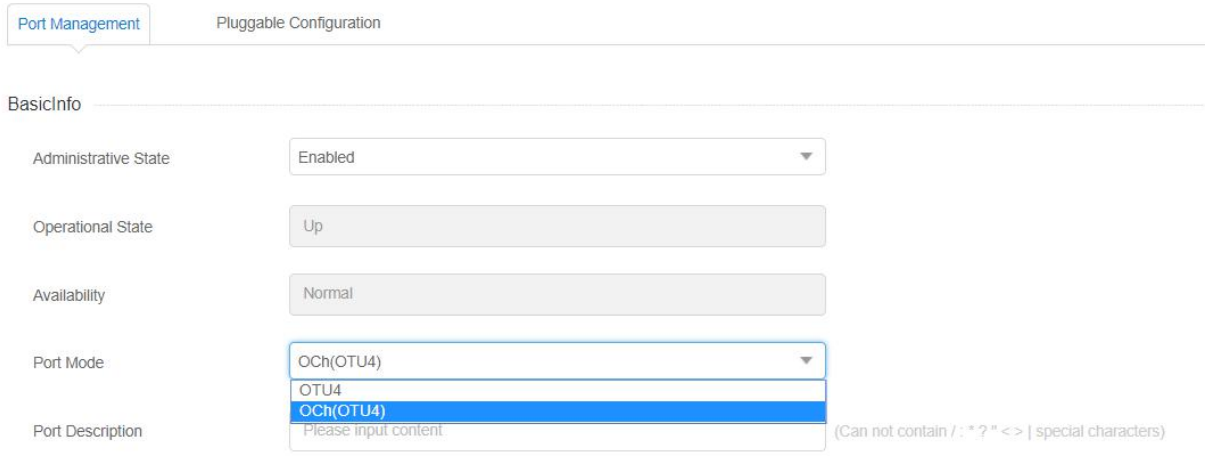



Figure5-22 M6500-MXP10 Line Side Port Interface

- **Client Side Port**

Select NE-Slot 1, click on“*Port1*”and select“*Port Management*”on the right，the operation interface is as shown in the figure below:

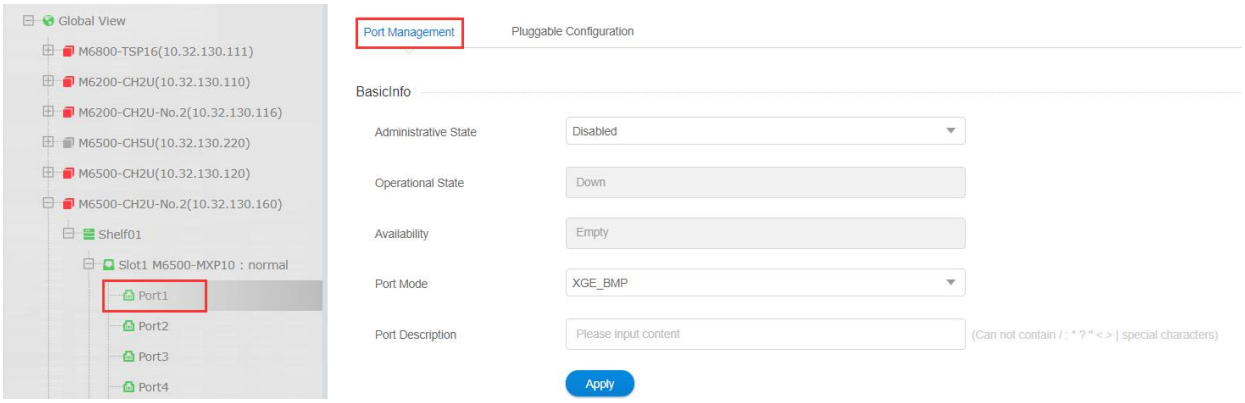



Figure5-23 M6500-MXP10 Client Side Port Information

The client side port management interface is as shown in the figure below and the service type can be selected in port mode.

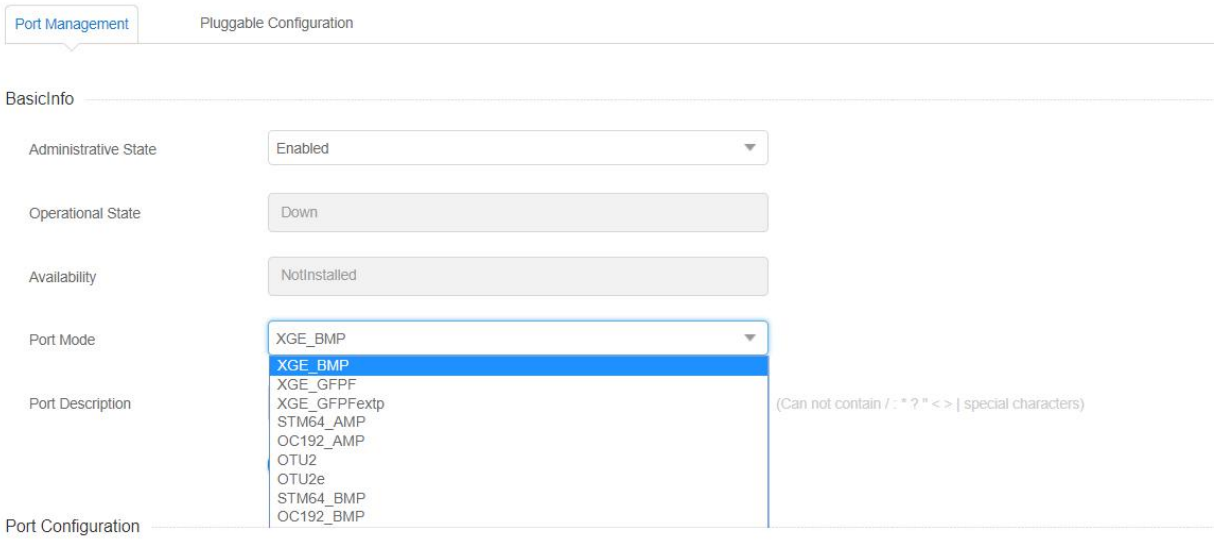



Figure5-24 M6500-MXP10 Client Side Port Interface

### 5.4.1.2. Time Slot Configuration

Select NE and click on“*Slot 1* ”, and then select“*TP Multiplexing Structure*”module on the right，as shown in the figure below:

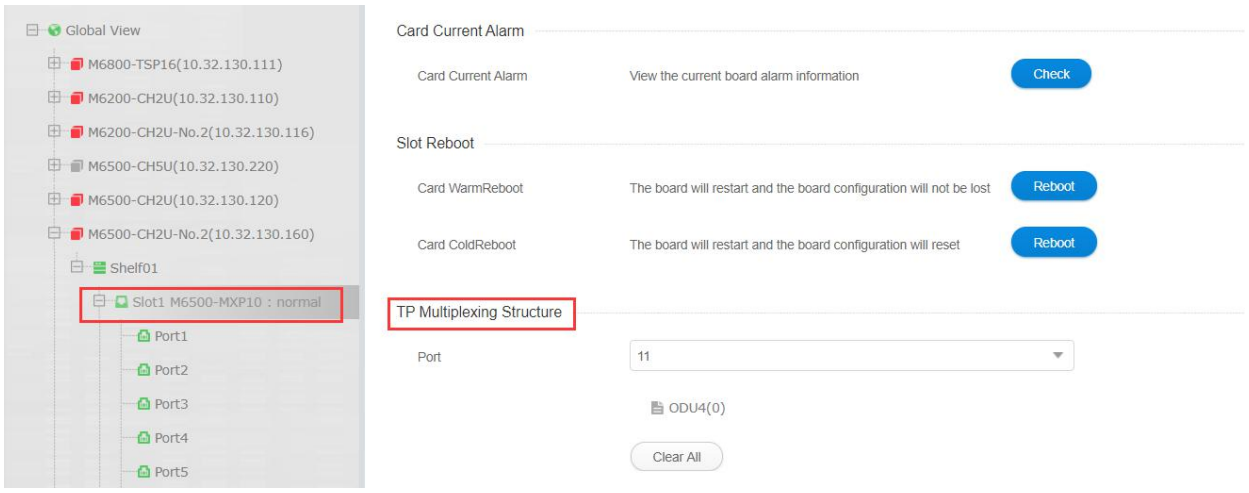



Figure5-25 Operation Steps of M6500-MXP10 TP Multiplexing Configuration

Click on"*ODU4*"button and the interface is as shown in the figure below. Select ODU4 to demultiplex to ODU2/ODU2e.

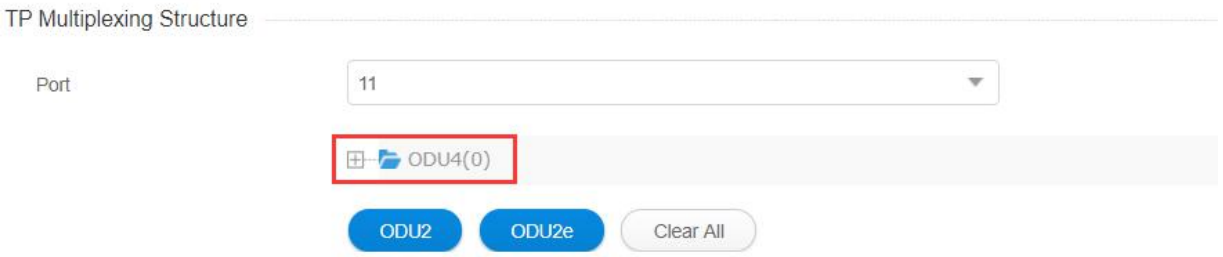



Figure5-26 M6500-MXP10 Demultiplexing Configuration Interface

ODU4 can be demultiplexed to 10*ODU2/ODU2e (here we take ODU2e as an example), 8 time slots need to be configured for each ODU2/ODU2e.

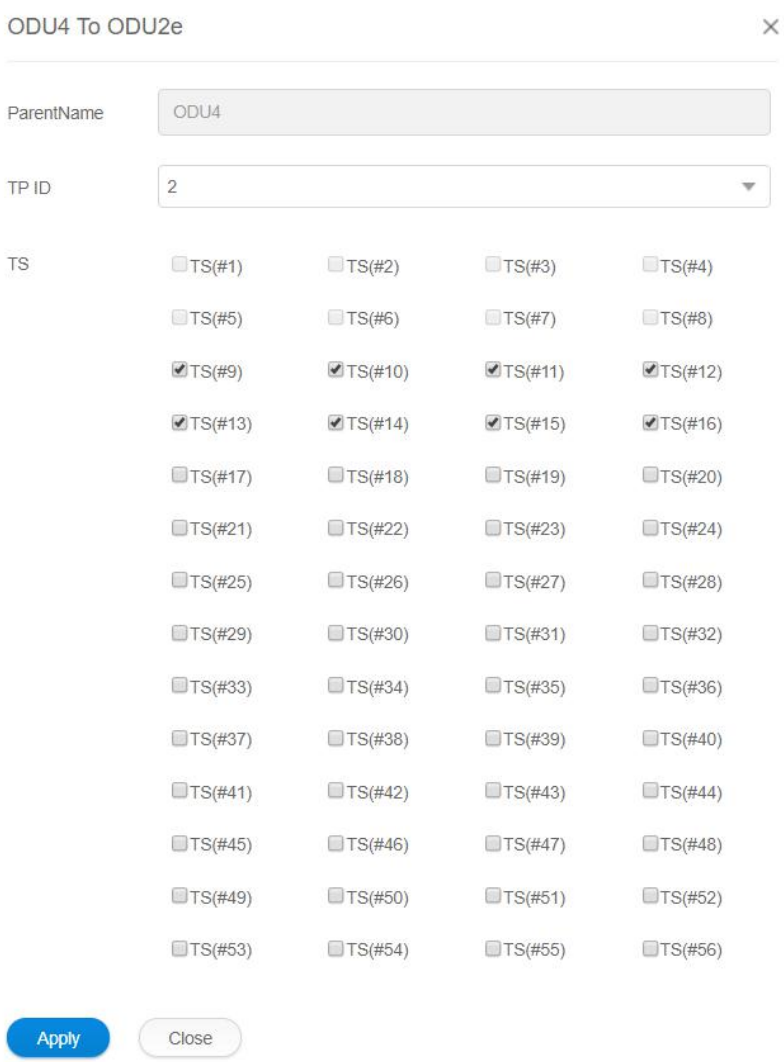



Figure5-27 M6500-MXP10 Demultiplexing ODU2e Configuration

The result when it is with full configuration of 10*ODU2e is as shown in the figure below:

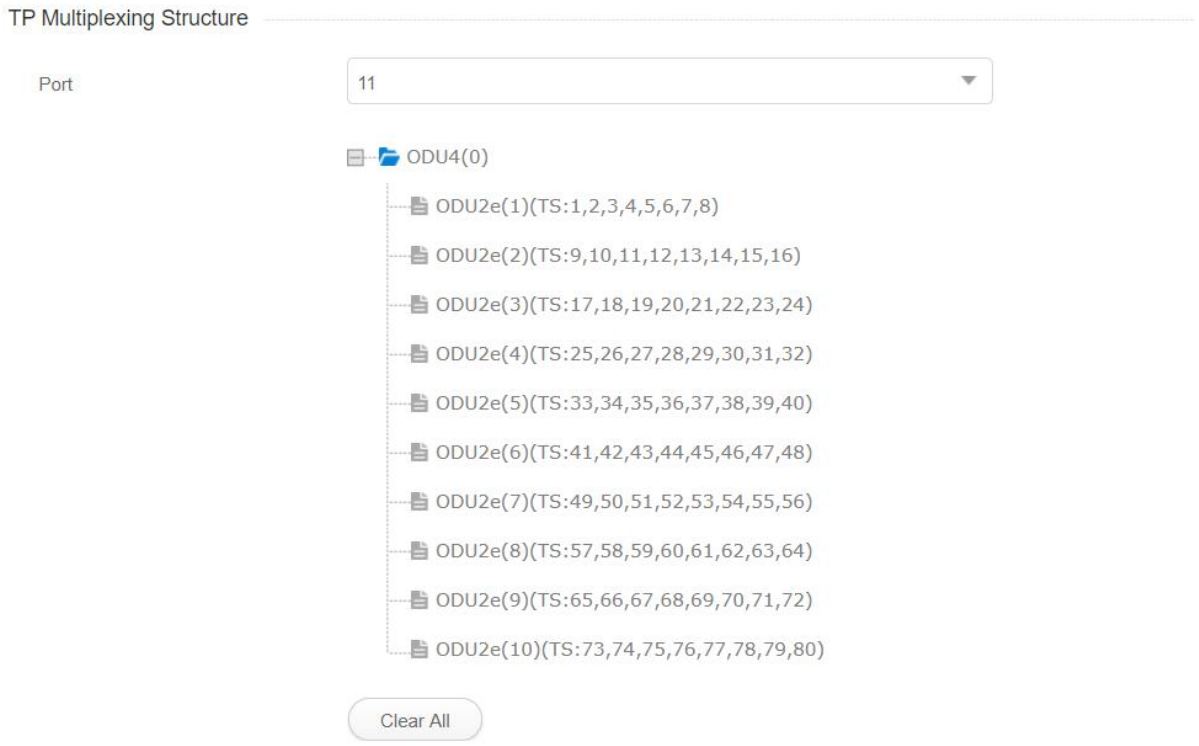



Figure5-28 Configuration Result of M6500-MXP10 Demultiplexing 10*ODU2e

#### 5.4.1.3. Cross-Connection Configuration

For example, if we need to create bidirectional cross-connection with protection of port 1 to port 11, the operation is as follows: Select XGE_BMP at the client side and select OCh (OTU4) at the line side, then ODU2e cross-connection is established correspondingly, as shown in the figure below:

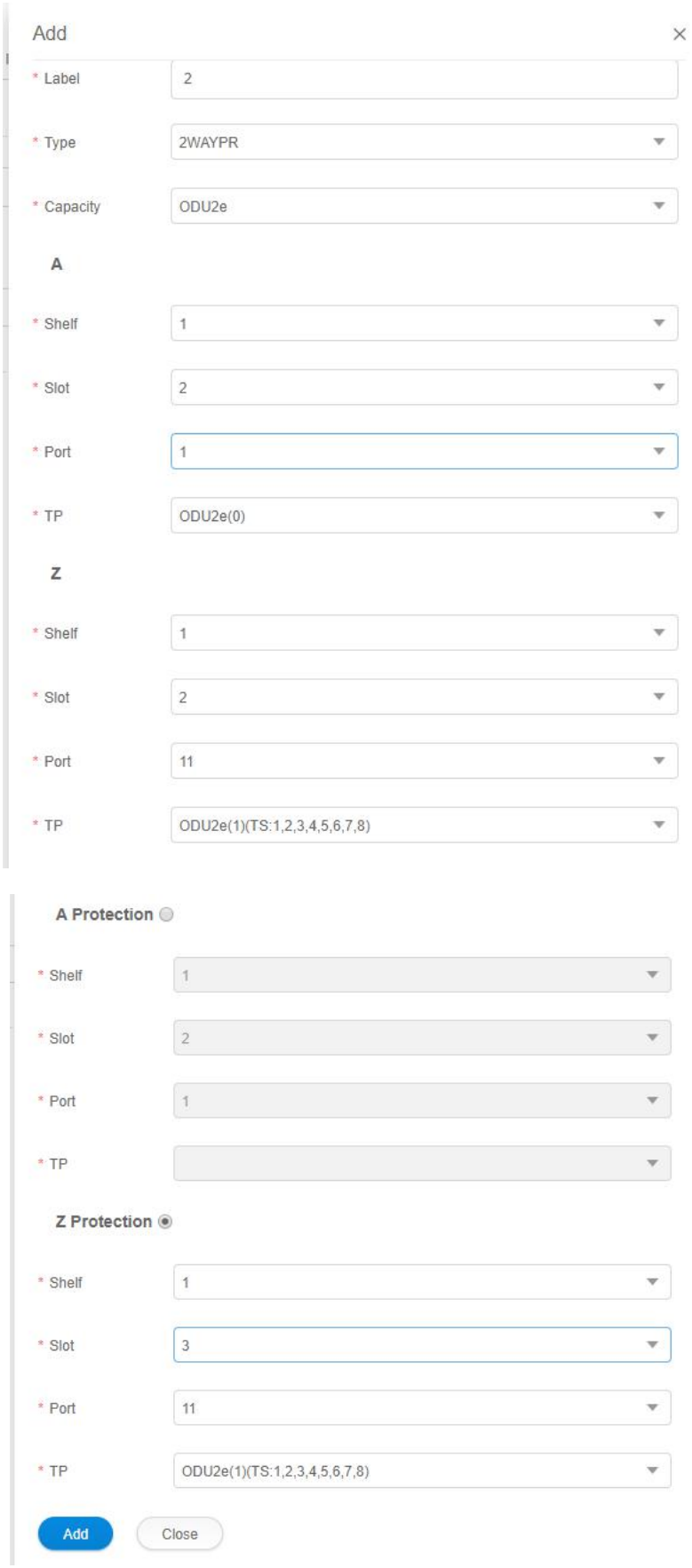



Figure5-29 M6500-MXP10 Bidirectional Cross-Connection with Protection

The following figure shows that the cross-connection is successfully established.

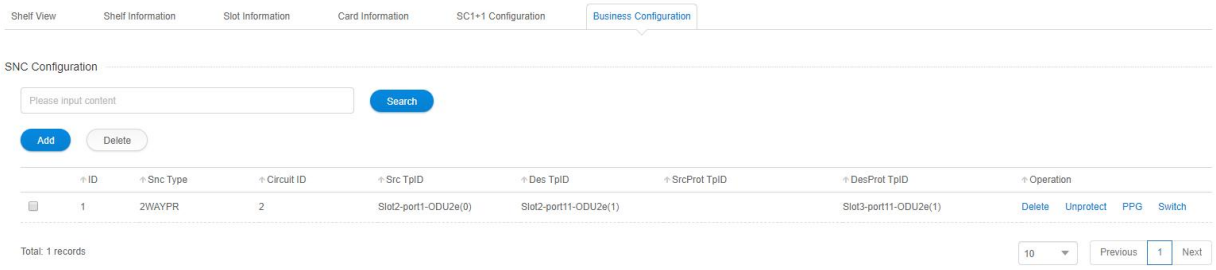



Figure5-30 Successful Establishment of M6500-MXP10 Bidirectional Cross-Connection with Protection

#### 5.4.1.4. FEC Configuration

FEC is only configurable on OUT layer.

- **Line Side Port**

Select NE-Slot 1, click on"*Port11*"and select"*Port Management*", and then select OCh (OTU4) as the port mode. In"*OTU4*" interface under "*Port Configuration*"on the right, select "*FEC type*"to view the configuration. There are in all 7 FEC modes for M6500-MXP10 line side, which are respectively G709FEC/SDFEC1/SDFEC2/SDFEC3/SDFEC1_Non-diff/SDFEC2_Non-diff/SDFEC3_Non-diff. SDFEC2 is the default mode, as shown in the figure
below:

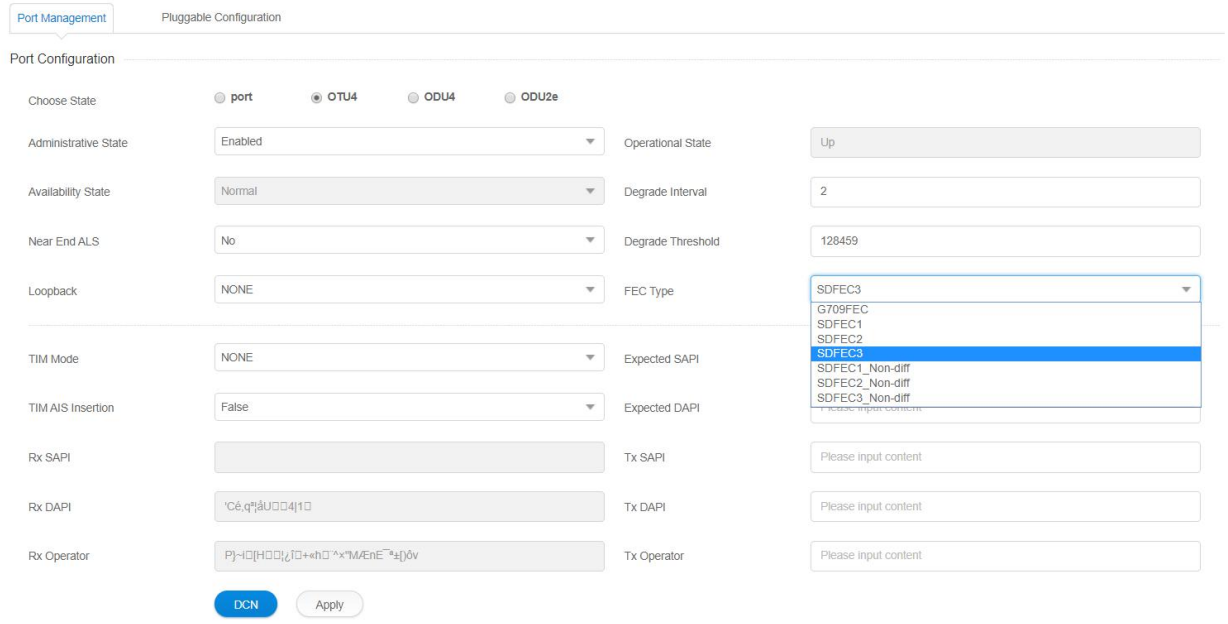



Figure5-31 FEC Configuration of M6500-MXP10 Line Side Port

- **Client Side Port**

Select NE-Slot 2, click on"*Port11*"and select"*Port Management*"on the right, and then select OTU2/OTU2e as the port mode. In"*OTU2/OTU2e*" interface under "*Port Configuration*", select "*FEC type*"to view the configuration. There are in all 4 FEC modes for M6500-MXP10 client side, which are respectively NOFEC/G709FEC/I.4EFEC/I.7EFEC. G709FEC is the default mode, the configuration is as shown in the figure below:

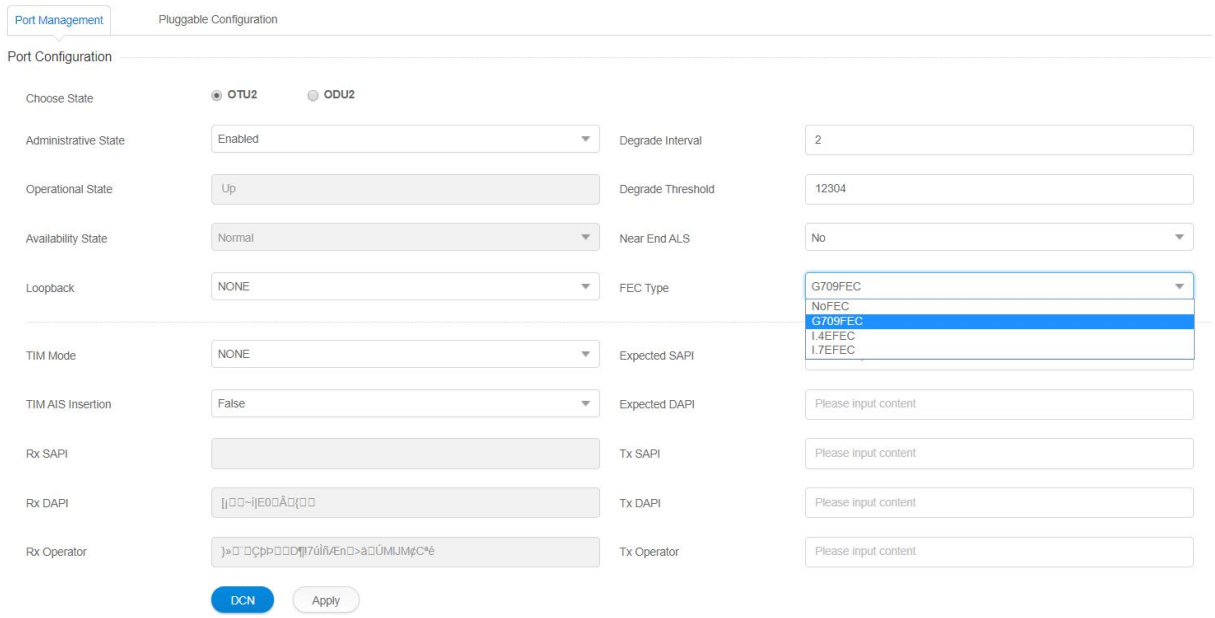



Figure5-32 FEC Configuration of M6500-MXP10 Client Side (OTU2) Port

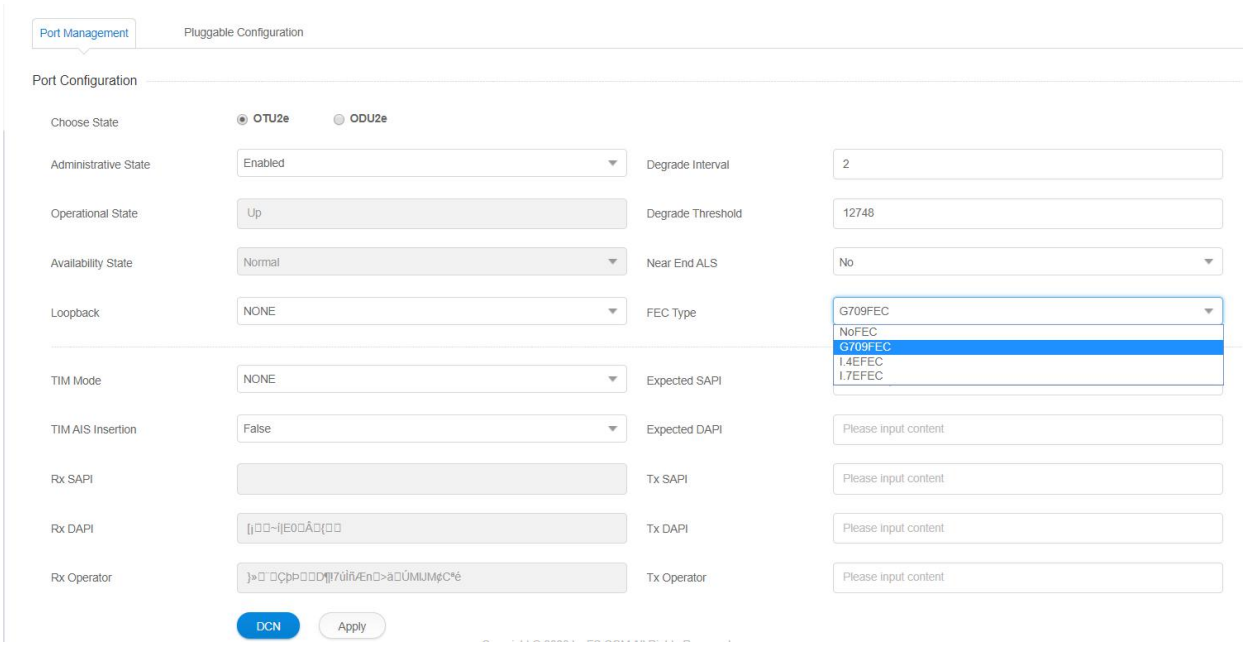



Figure5-33 FEC Configuration of M6500-MXP10 Client Side (OTU2e) Port

## 5.4.2. M6500-TMXP2

The port type of M6500-TMXP2 includes 1 (port 3)*100G line side interface (CFP), 1 (port 1)*100G rate client side interface (QSFP28) or 2 (port 1-2)*40G client side interfaces (QSFP+).

### 5.4.2.1. Service Type

- **Line Side Port**

Select NE-Slot 2, click on“*Port 3*”and select“*Port Management*”on the right, the operation steps are as shown in the figure below:

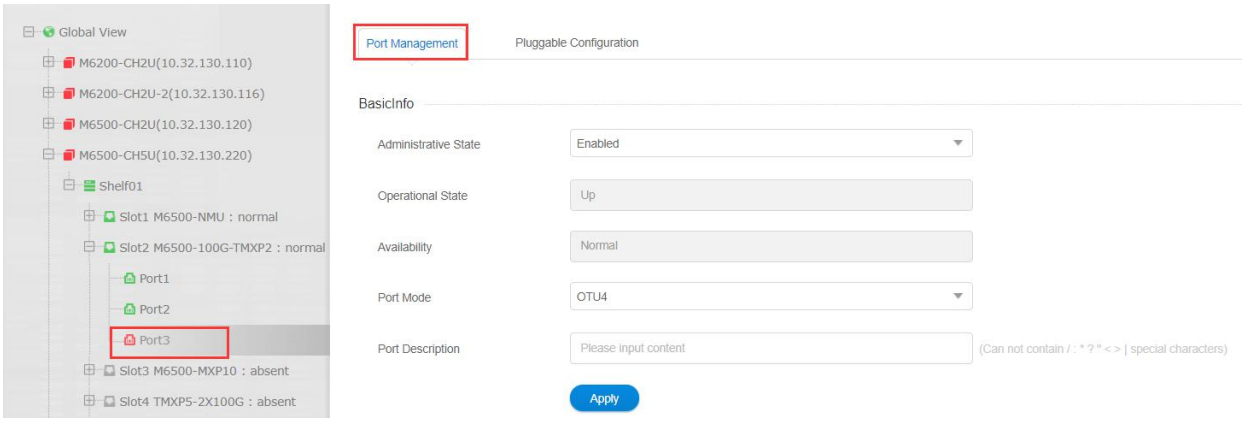



Figure5-34 M6500-TMXP2 Line Side Port Information

The line side port management interface is as shown in the figure below and the service type can be selected in port mode.

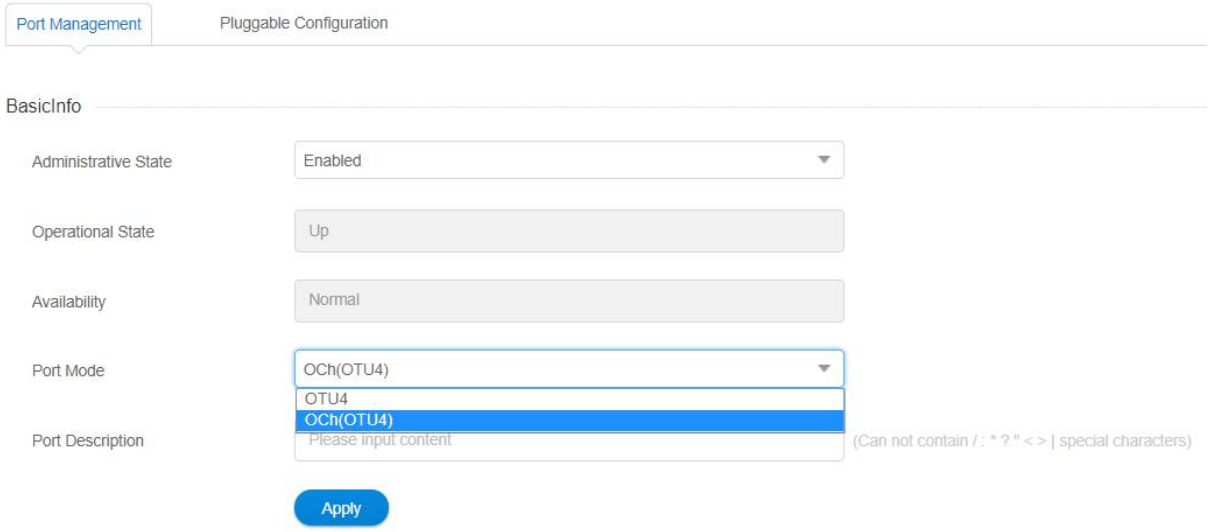



Figure5-35 M6500-TMXP2 Line Side Port Interface

- **Client Side 100G Port**

Select NE-Slot 2, click on"*Port1*"and select"*Port Management*"on the right, the operation steps are as shown in the figure below:

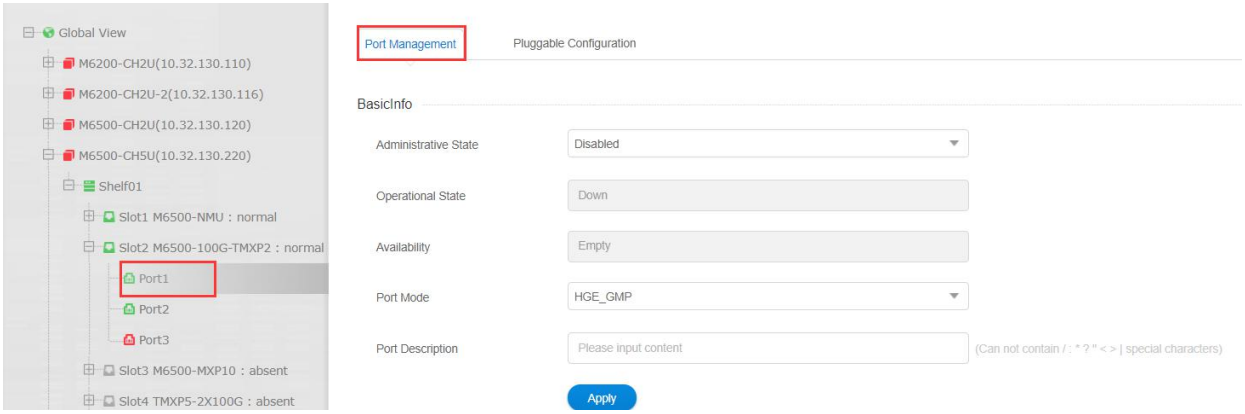



Figure5-36 M6500-TMXP2 Client Side 100G Port Information

The client side port management interface is as shown in the figure below and the service type can be selected in port mode.

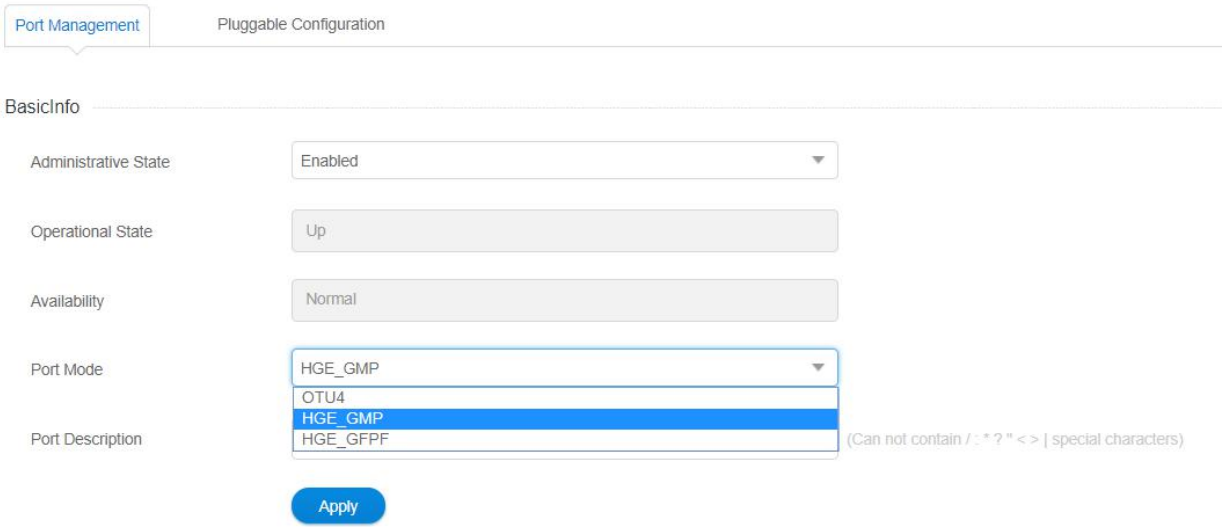



Figure5-37 M6500-TMXP2 Client Side 100G Port Interface

- **Client Side 40G Port**

The current board mode is 100G; you need to change the board mode to 40G mode. Select NE (10.32.130.220)-Slot2, click on "*Slot2*" and select "*Card Mode Configuration*" module on the right, as shown in the figure below:

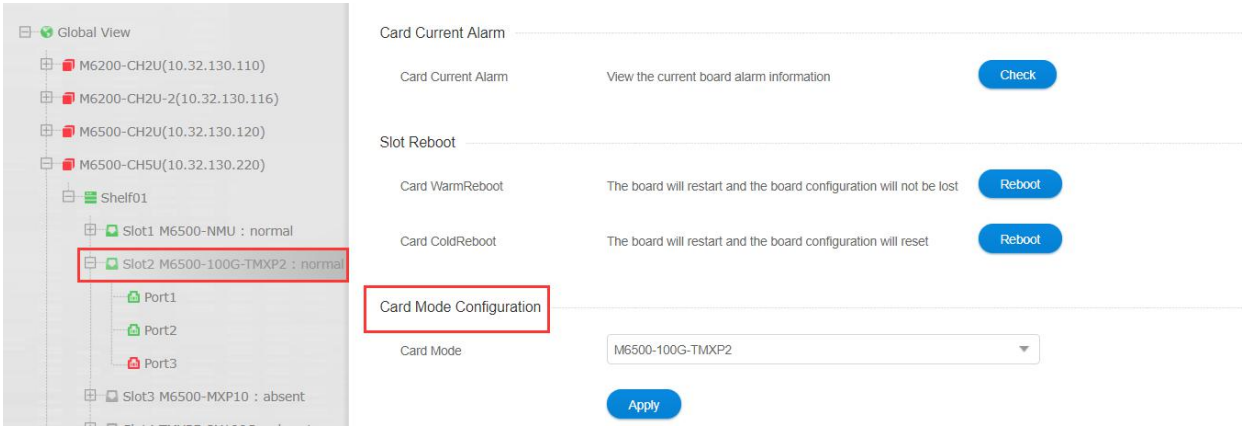



Figure5-38 Operation Steps of M6500-TMXP2 Card Configuration

After the window to select card mode appears, select M6500-40G-TMXP2.

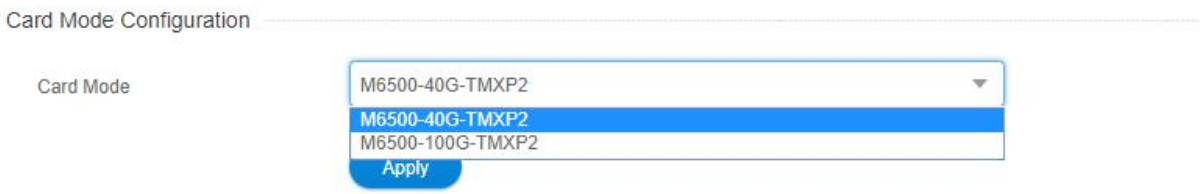



Figure5-39 Selection of M6500-TMXP2 Card Mode

Apply M6500-40G-TMXP2 mode.

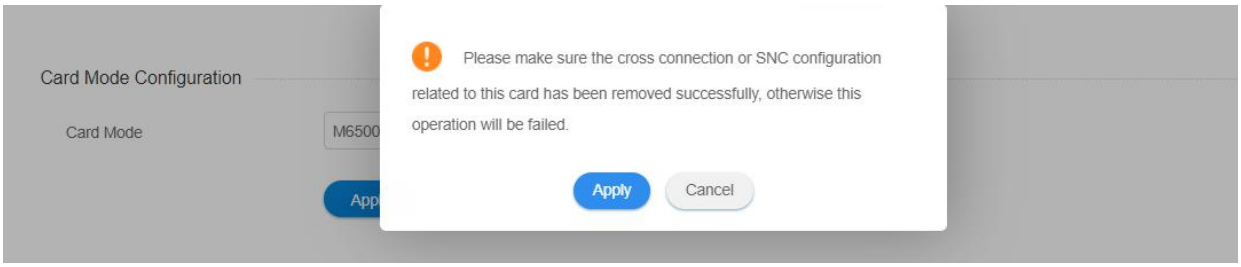



Figure5-40 Apply M6500-TMXP2 Board Mode

After successful application, the board is initialized, as shown in the figure below:

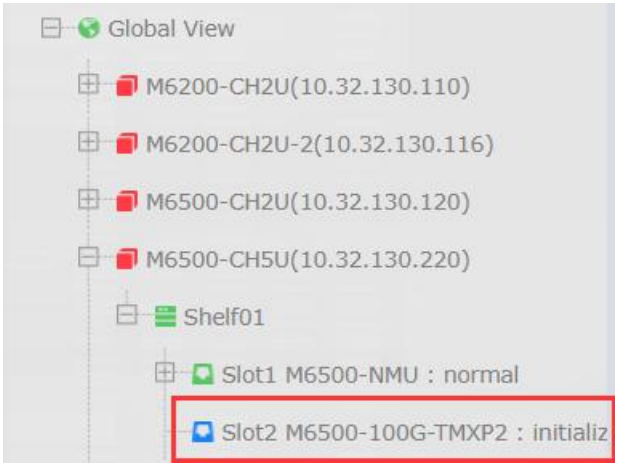



Figure5-41 M6500-TMXP2 Board Initialization

After a moment,NE synchronization is performed. The latest mode of M6500-TMXP2 board is synchronized.The operation steps are as follows: select NE, and click and select " *NE Management*" on the right , then click "*synchronization* " button on the right side of the NE synchronization module, the interface is as shown in the figure below:

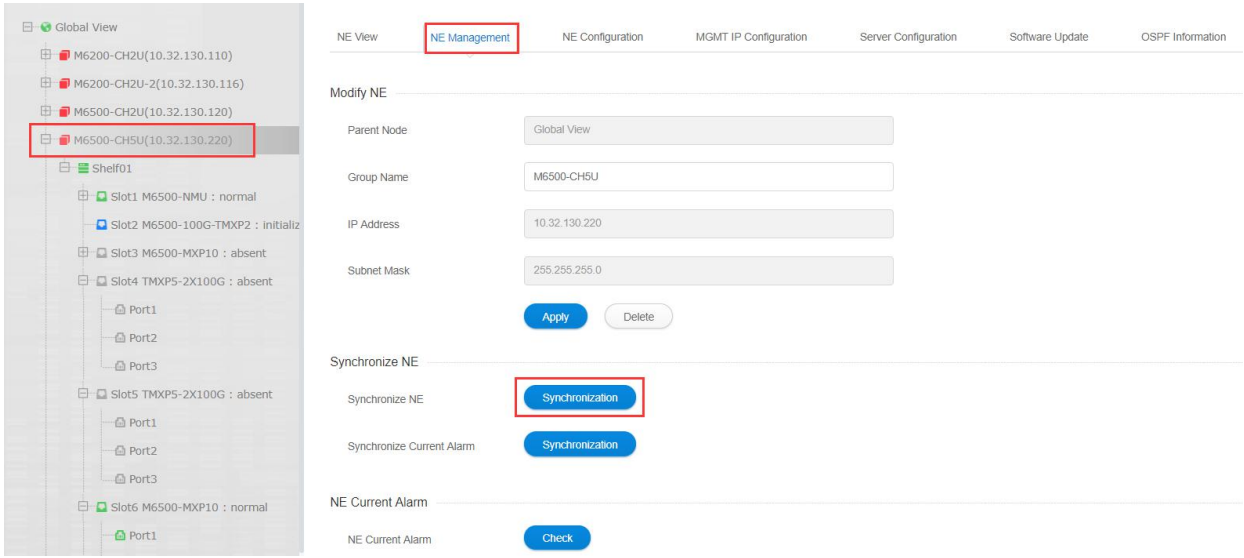



Figure5-42 NE Synchronization

After successful synchronization, it is successfully switched to the M6500-40G-TMXP2 board mode, as shown in the figure below:

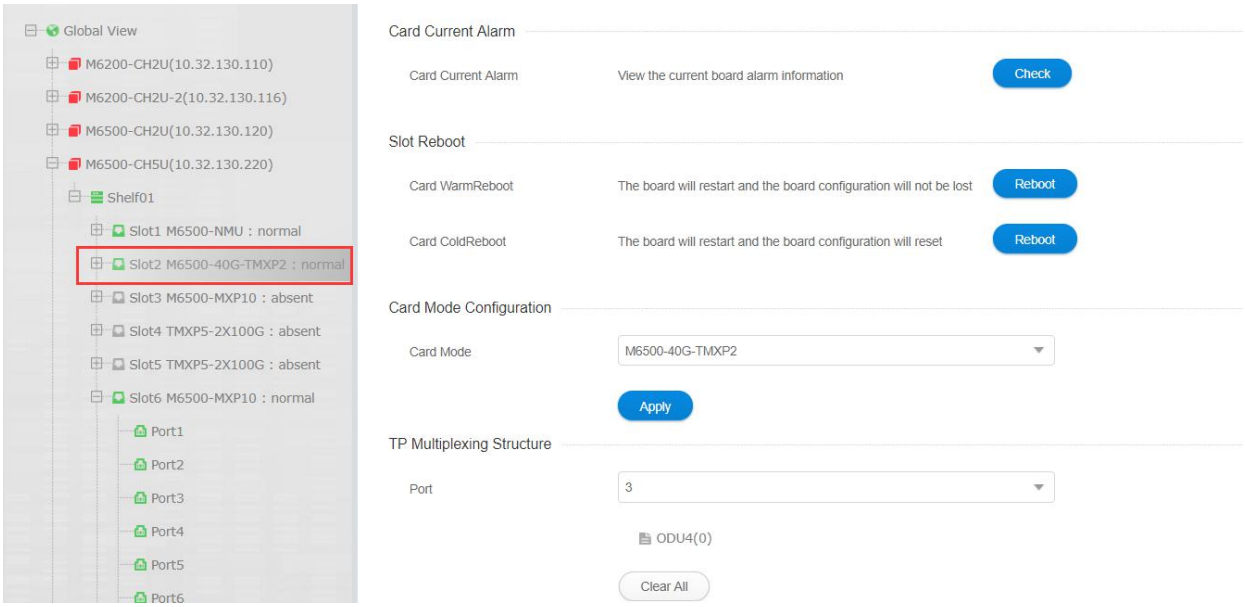



Figure5-43 Successful Switch of the Board Mode

At this time, 40G client side port mode can be selected: select NE-Slot 2, click on"*Port1*"and select"*Port Management*"on the right, the interface is as shown in the figure below:

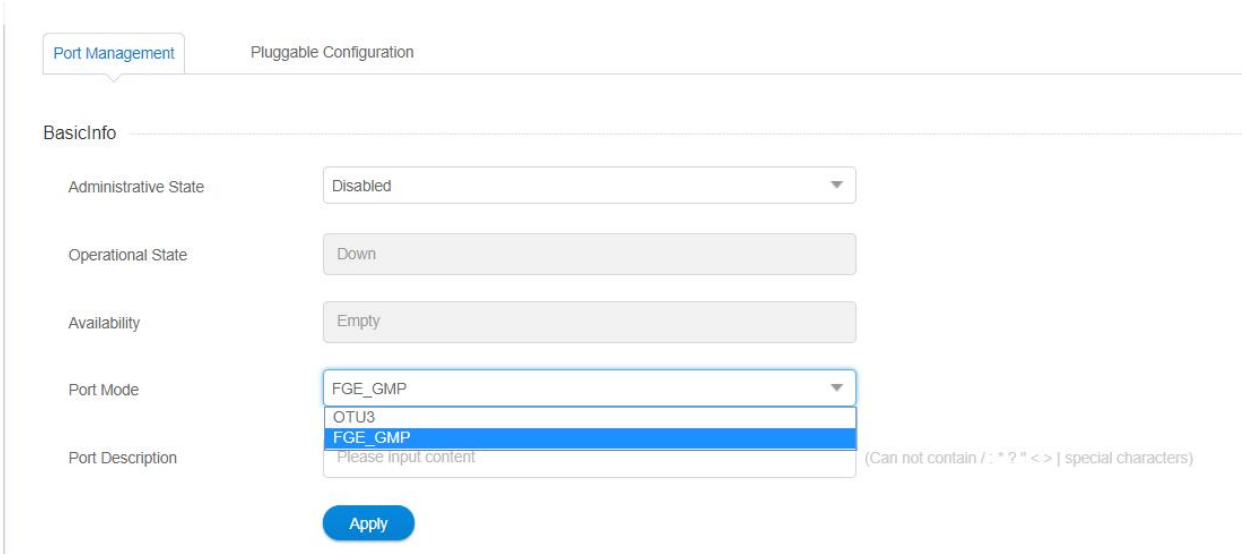



Figure5-44 M6500-TMXP2 Client Side 40G Port Interface

### 5.4.2.2. Time Slot Configuration

When the board is in 100G mode, there is no need to configure time slot. When the board is in 40G mode, it needs to configure time slot.

Select NE, click on"*Slot 2*" and select"*TP Multiplexing Structure*"module, the steps are as shown in the figure below:

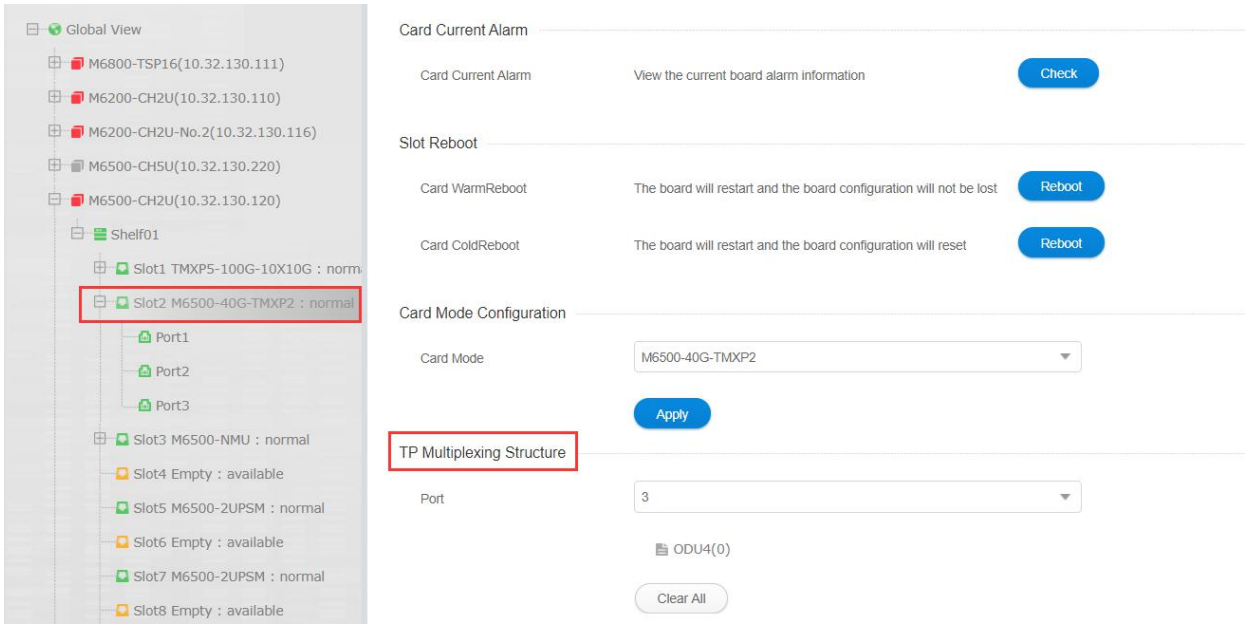



Figure5-45 Operation Steps of M6500-TMXP2 TP Multiplexing

The interface is as shown in the figure below. Select ODU4 to demultiplex to ODU3 (ODU2&ODU2e are unavailable).


Figure5-46 M6500-TMXP2 Demultiplexing Configuration Interface

ODU4 can be demultiplexed to 2*ODU3 and 31 time slots are configured for each ODU3.

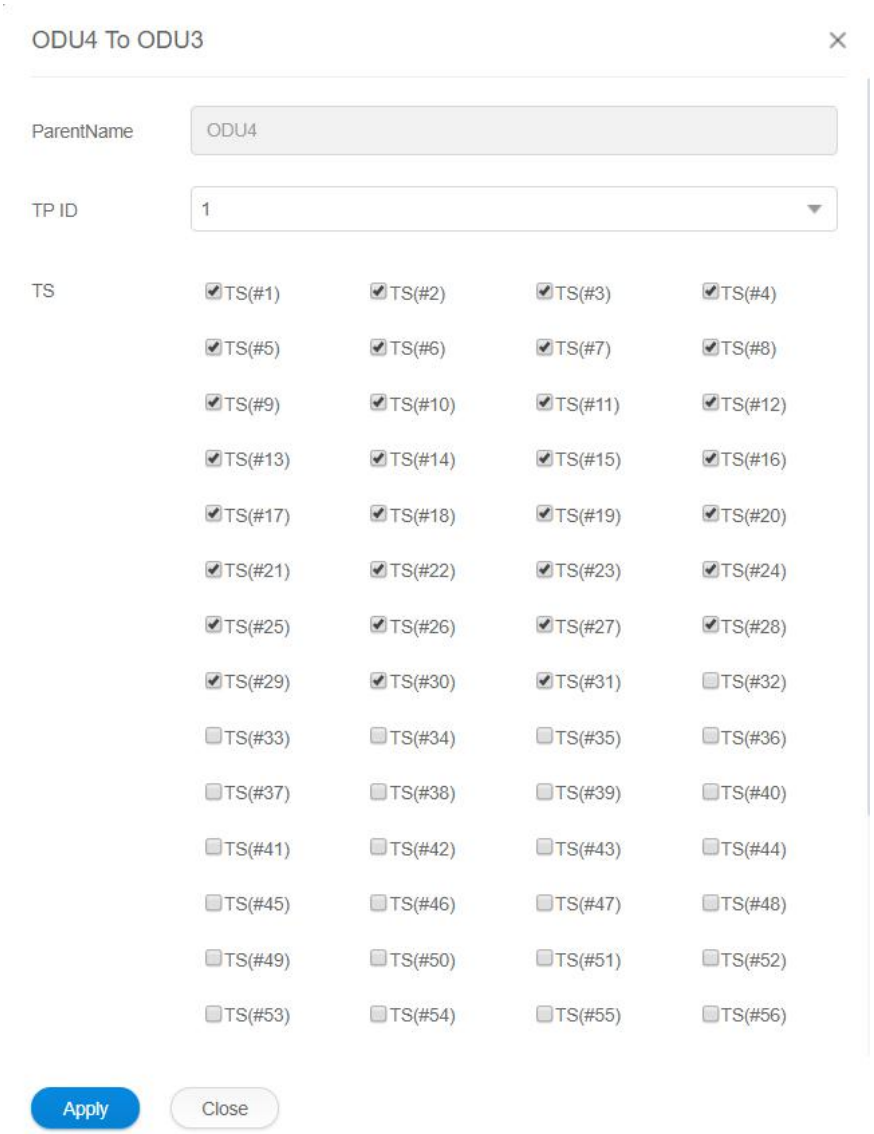



Figure5-47 Time Slot Configuration of M6500-TMXP2 Demultiplex ODU3

When it is fully configured with 2*ODU3, the interface is as shown in the figure below:

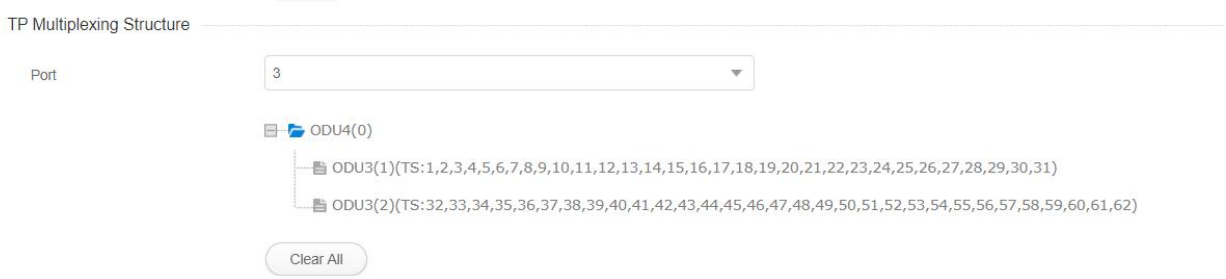



Figure5-48 Configuration Result of M6500-TMXP2 Demultiplexing 2*ODU3

#### 5.4.2.3. Cross-Connection Configuration

For example, if we need to create bidirectional cross-connection without protection of port 1 to port 3, the operation is as follows: Select HGE_GMP at the client side and select OCh (OTU4) at the line side, then ODU4 cross-connections established correspondingly, as shown in the figure below:

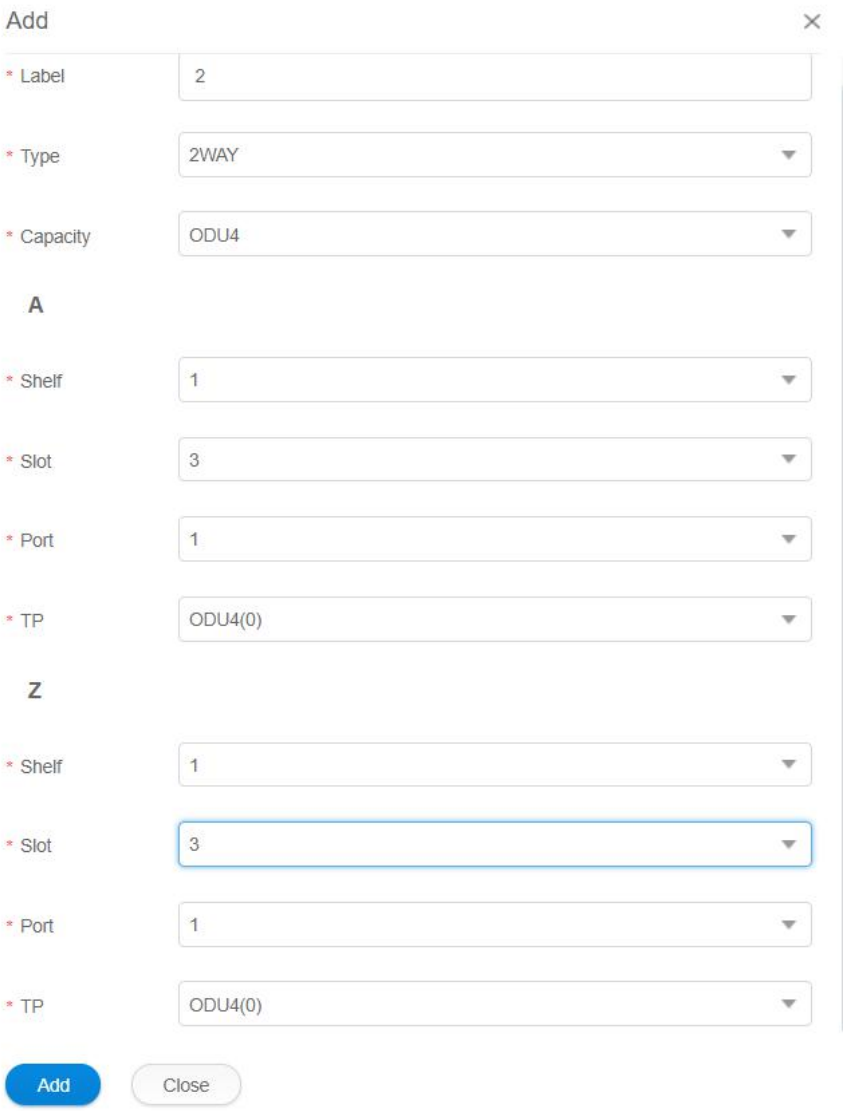



Figure5-49 M6500-TMXP2 Bidirectional Cross-Connection without Protection

The following figure shows that the cross-connection is successfully established.

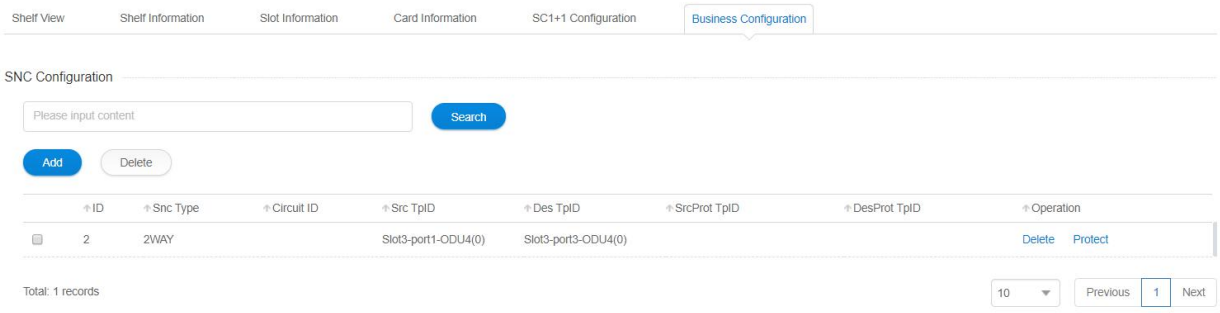



Figure5-50 Successful Establishment of M6500-TMXP2 Bidirectional Cross-Connection without Protection

### 5.4.2.4. FEC Configuration

FEC is only configurable on OUT layer.

- **Line Side Port**

Select NE-Slot 2, click on "*Port 3*"and select"*Port Management*"on the right, and then select OCh (OTU4) as the port mode. In"*OTU4*"interface under"*Port Configuration*", select "*FEC type*"to view the configuration. There are in all 7 FEC modes for TMXP2 line side, which are respectively G709FEC/SDFEC1/SDFEC2/SDFEC3/SDFEC1_Non-diff/SDFEC2_Non-diff/SDFEC3_Non-diff. SDFEC3 is the default mode, as shown in the figure below:

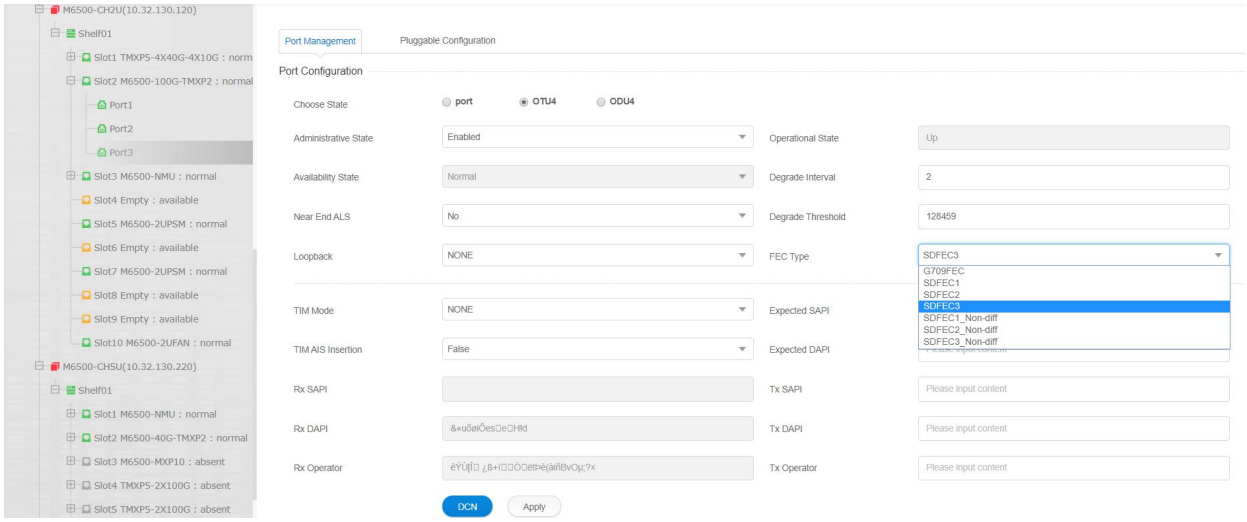



Figure5-51 FEC Configuration of M6500-TMXP2 Line Side Port

- **Client Side 100G Port**

Select NE-Slot 2, click on "*Port1*"and select"*Port Management*"on the right", and then select OTU4 as the port mode. In"*OTU4*" interface under"*Port Configuration*", select "*FEC type*"to view the configuration. There is only one default FEC mode for 100G client side, which is G709FEC, as shown in the figure below:

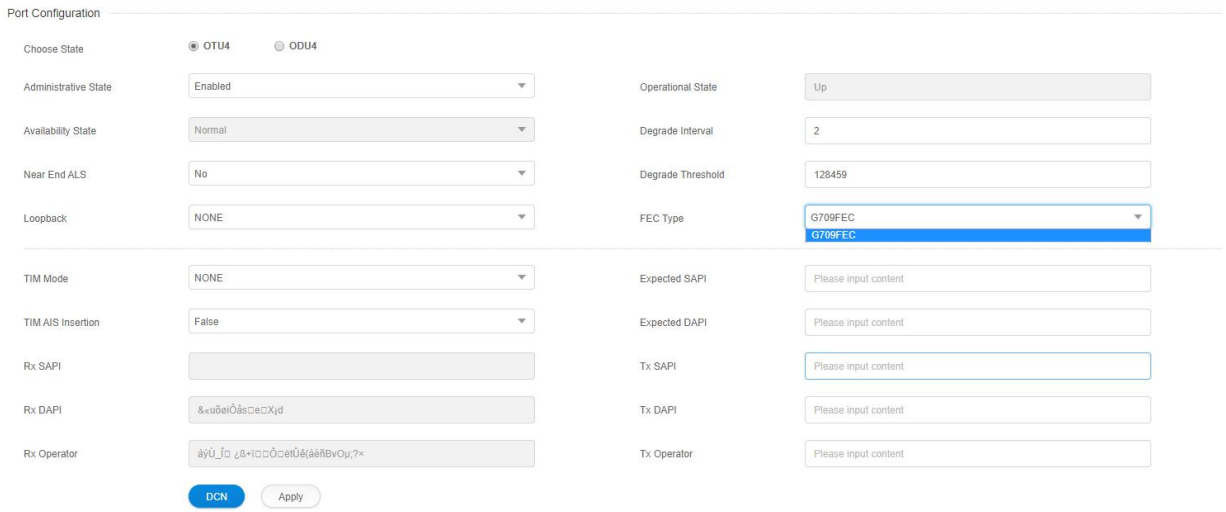



Figure5-52 FEC Configuration of M6500-TMXP2 Client Side 100G Port

- **Client Side 40G Port**

Select NE-Slot 2, click on"*Port1*"and select"*Port Management*"on the right, and then select OTU3 as the port mode. In"*OTU3*" interface under "*Port Configuration*", select "*FEC type*"to view the configuration. There are in all 4 FEC modes for the client side 40G, which are respectively No FEC/G709FEC/I.4EFEC/I.7EFEC. G709FEC is the default mode, the configuration is as shown in the figure below:

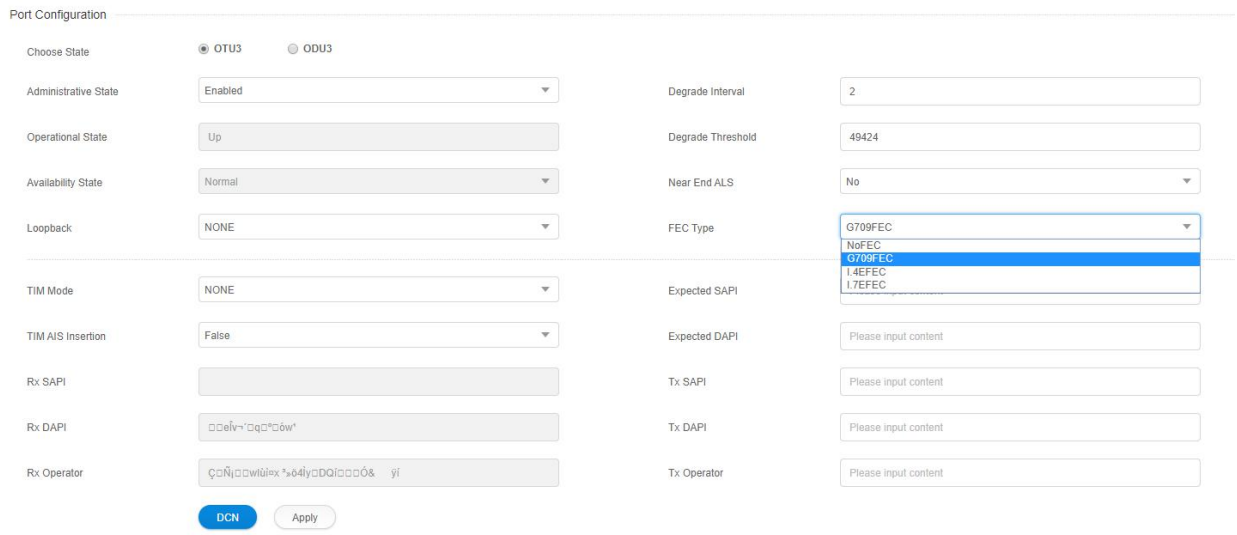



Figure5-53 FEC Configuration of M6500-TMXP2 Client Side 40G

## 5.4.3. M6500-TMXP5

M6500-TMXP5 port types are divided into 1 (port 1) 200G/100G line side interface (CFP2),

2 (ports 2-3) 100G client interface (QSFP28),

1 (port 3) 100G client interface (QSFP28) ) and 2 (ports 5-6) 40G client-side interfaces (QSFP+),

1 (port 3) 100G client-side interfaces (QSFP28) and 3 (ports 4-6) 10G client-side interfaces (QSFP+),

4 (Ports 2-5) 40G client-side ports (QSFP+) and 1 (port 6) 10G client-side ports (QSFP+)

5 (ports 2-6) 10G client-side ports (QSFP+).

### 5.4.3.1. Service Type

- **Line side port**

Select the NE-Slot1,click on "*Port1*" and select "*Port Configuration*" on the right. The operation steps are shown in the figure below.

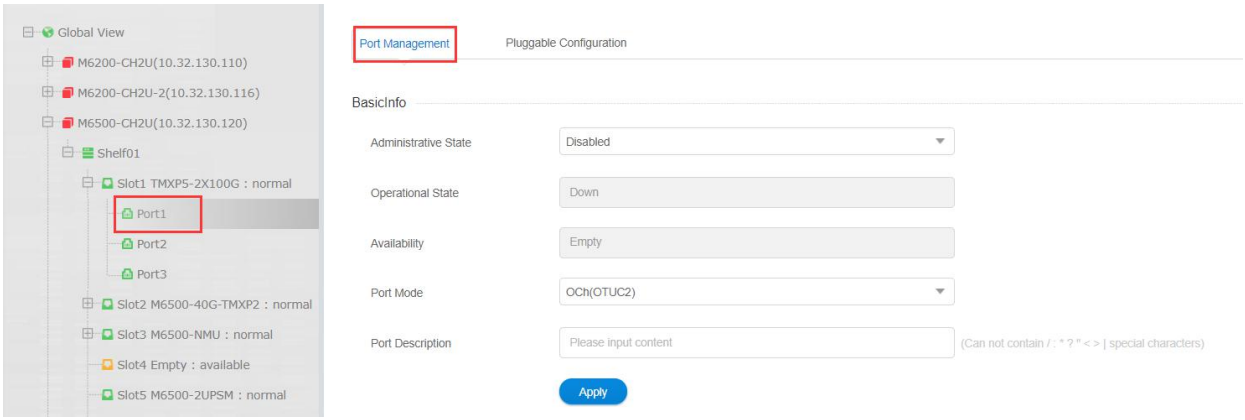



Figure5-54 M6500-TMXP5 line side port information operation steps

Open the line side port management as below figure, and can choose the service type in port mode.

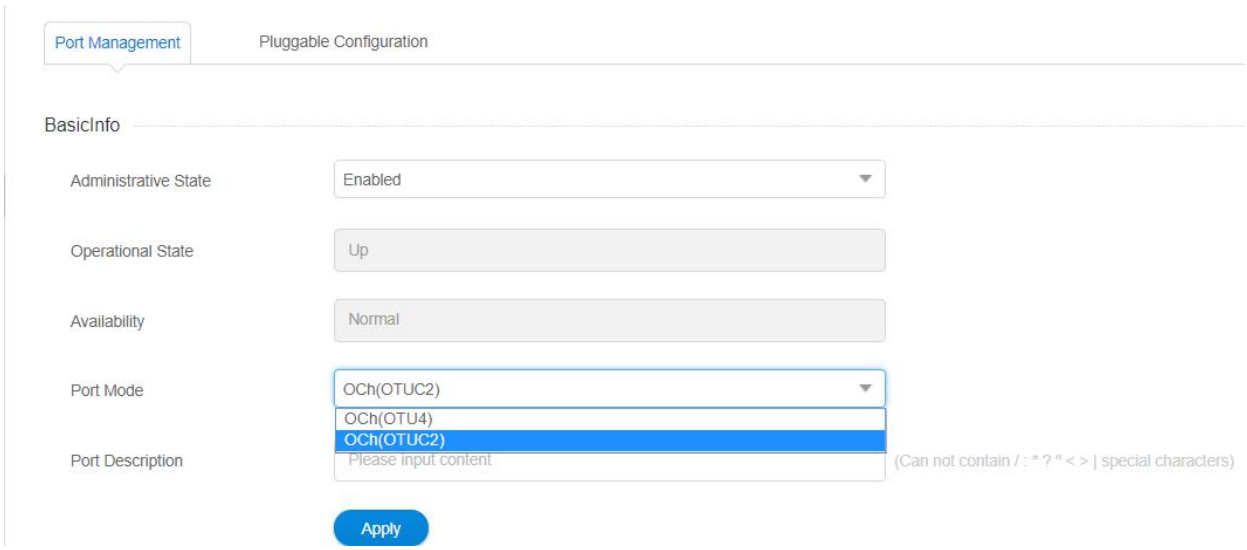



Figure5-55 M6500-TMXP5 Line side port interface

- **Client side port**

M6500-TMXP5 client-side ports are divided into 100G, 40G, and 10G. According to different board modes, different client-side ports are displayed.

Select the NE-Slot 1, click on "*Slot 1*" and select "*Card Mode Configuration*" module on the right, the steps are shown in the figure below.

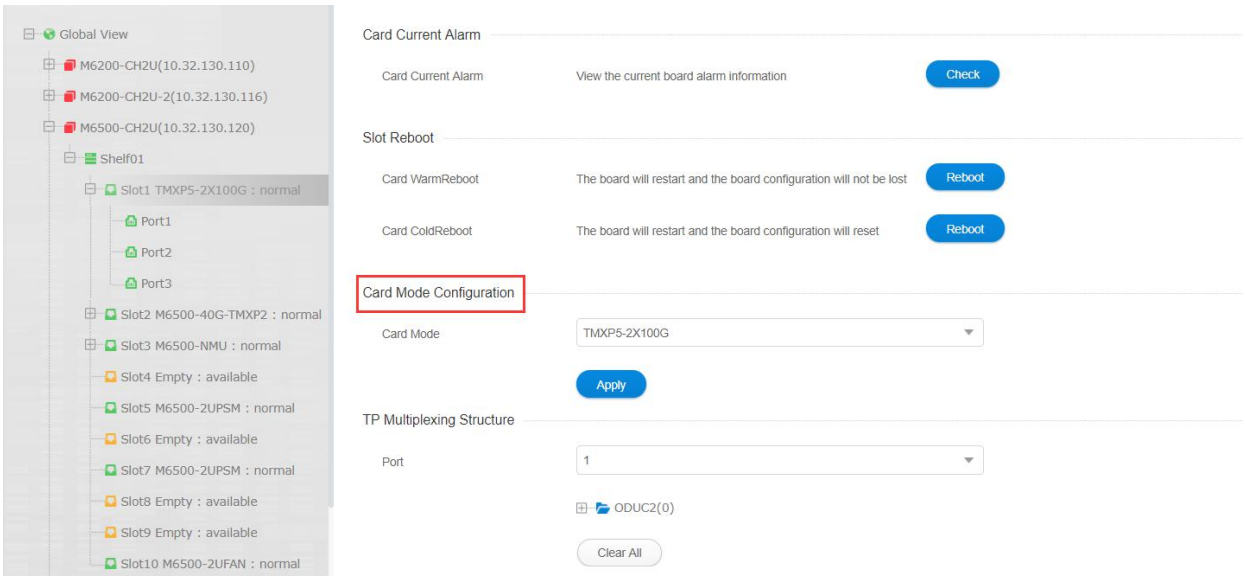



Figure5-56 M6500-TMXP5 Board configuration operation steps

After selection, the card mode selection window appears.

The client side supports 100G and can choose TMXP5-2X100G, TMXP5-100G-10X10G, TMXP5-100G-2X40G;

The client side supports 40G and can choose TMXP5_4X40G-4X10G, TMXP5-100G-2X40G;

The client side supports 10G can choose TMXP5-20X10G, TMXP5-100G-10X10G, TMXP5_4X40G-4X10G.

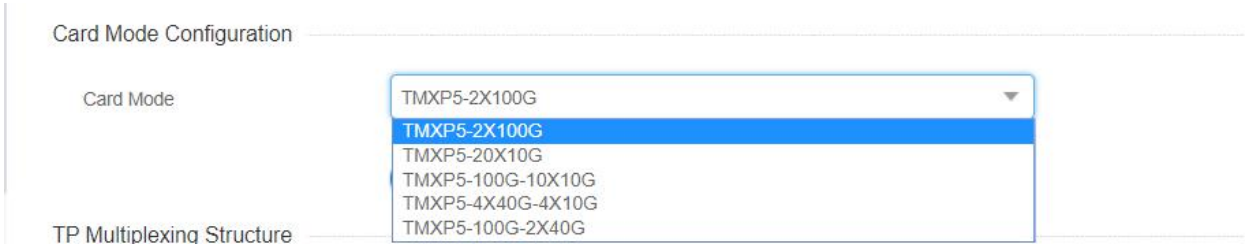



Figure5-57 M6500-TMXP5 Card mode selection

Apply TMXP5_4X40G-4X10GMode.

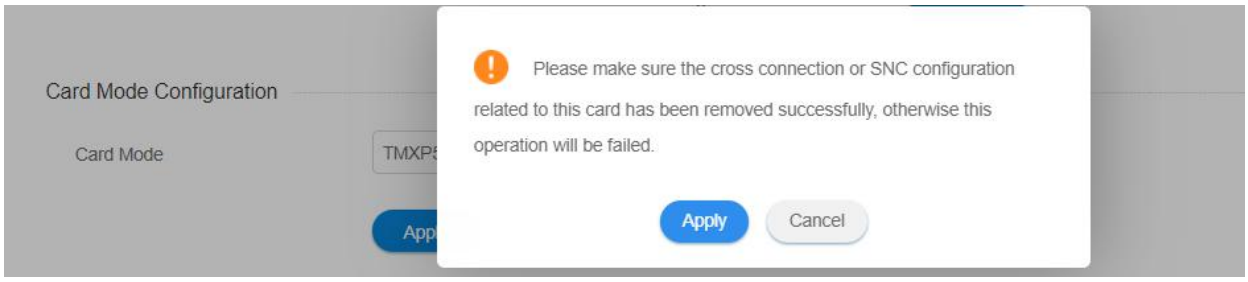



Figure5-58 M6500-TMXP5 Board mode apply

After apply successfully, the board will be in initialization mode as shown below:


Figure5-59 M6500-TMXP5 Board initialization

After a while, perform NE synchronization and synchronize the latest mode of the M6500-TMXP5 board. The operation steps are as follows: select the NE, click and select " *NE Management*" on the right, then click on "*synchronization* " button on the right side of the NE synchronization module, the interface is shown in the figure below.

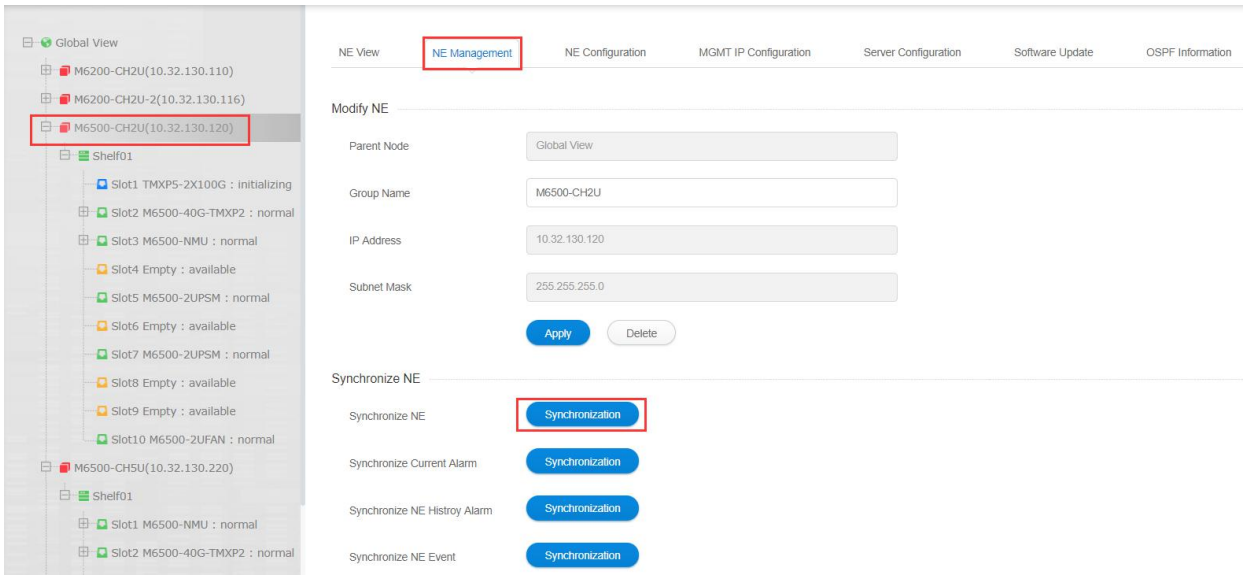



Figure5-60 NE Synchronization

After the synchronization is successful, the TMXP5_4X40G-4X10G board card mode is successfully switched, as shown in the figure below.

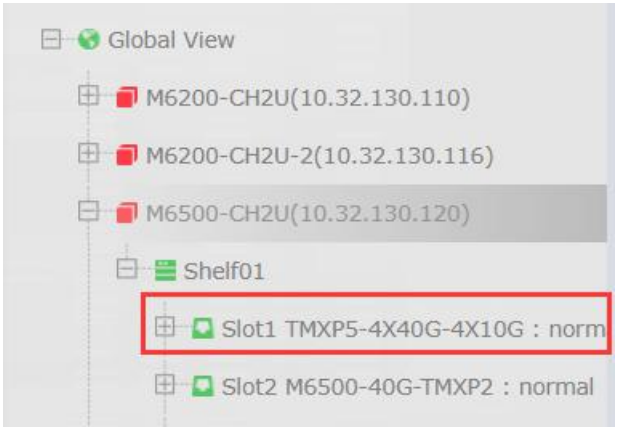



Figure5-61 The board mode switch successfully

- **Client Side 100G**

Select the NE-Slot 1, click on "*Port 3*" and select "*Port Configuration*" on the right. The operation steps are shown in the figure below.

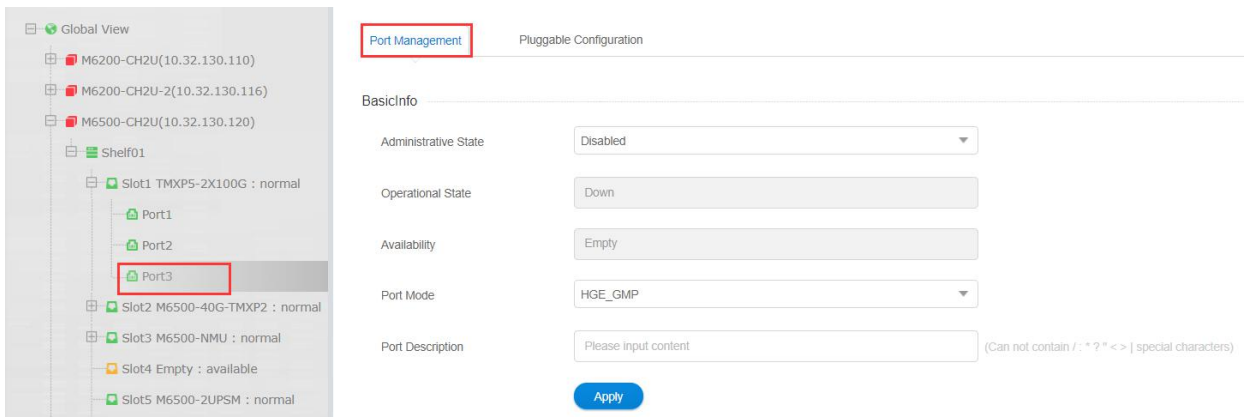



Figure5-62 M6500-TMXP5 Client side 100G port information operation steps

Open the client-side port management interface as shown in the figure below, and you can select the service type in the port mode.

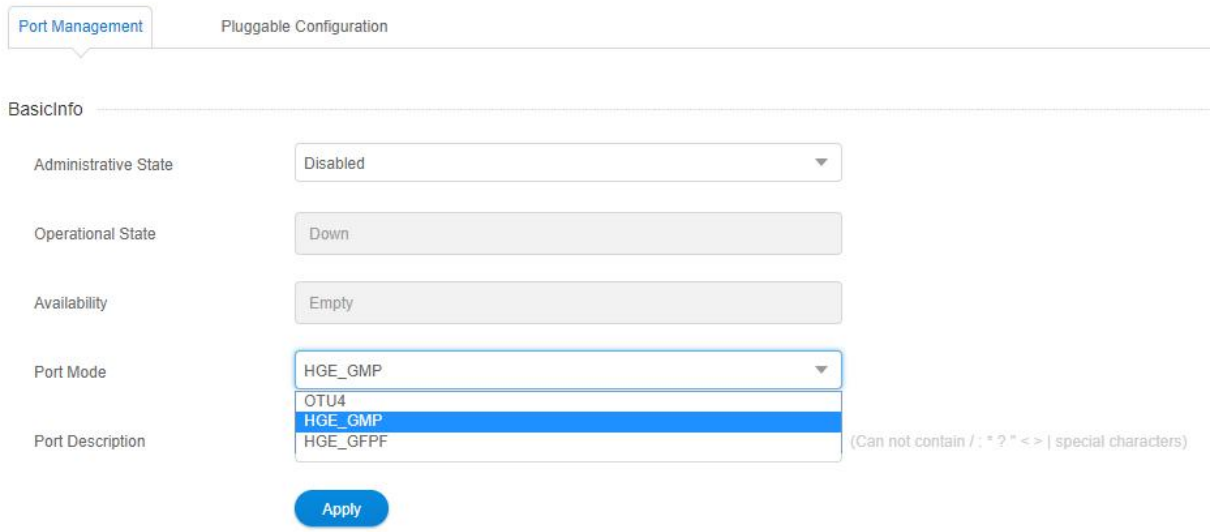



Figure5-63 M6500-TMXP5 Client side 100G port interface

- **Client side 40G port**

First switch the card mode to the corresponding mode. Choose NE--Slot 1, click on "*Port 5* " and choose "*Port management*" on the right , as shown in below:

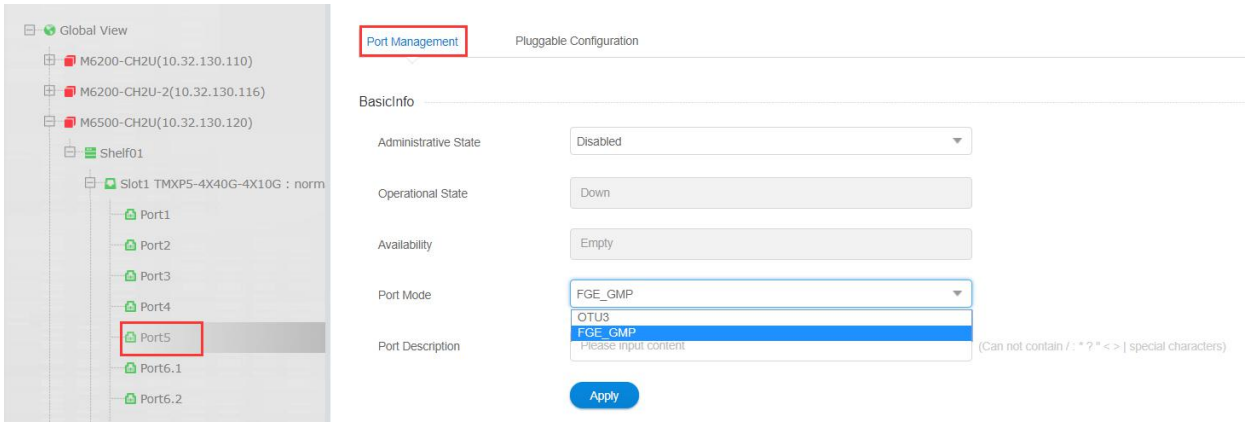



Image5-64 M6500-TMXP5 Client side 40G port interface

- **Client side 10G port**

First switch the card mode to the corresponding mode. Choose NE--Slot 1, click on "*Port 6.1*" choose "*Port management*", as shown in below:

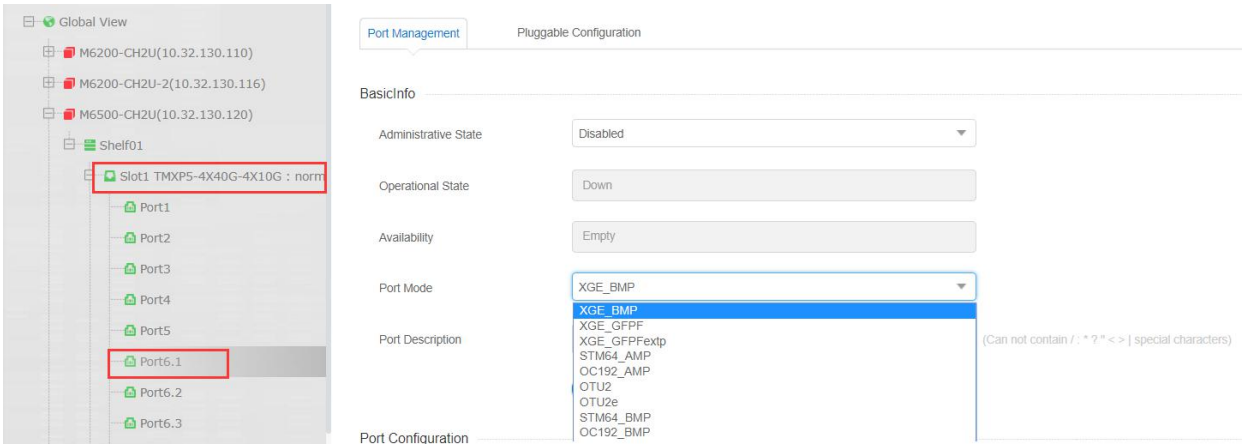



Figure5-65 M6500-TMXP5 Client side 10G port interface

### 5.4.3.2. Time slot configuration

When the board is in the 2X100G mode, there is no need to configure the time slot, and the other board modes all need to configure the time slot.

Take TMXP5-4X40G-4X10G as an example

Select the NE-Slot1 and on the right side there is "*TP Multiplexing Structure*" module, the steps are shown in the figure below.

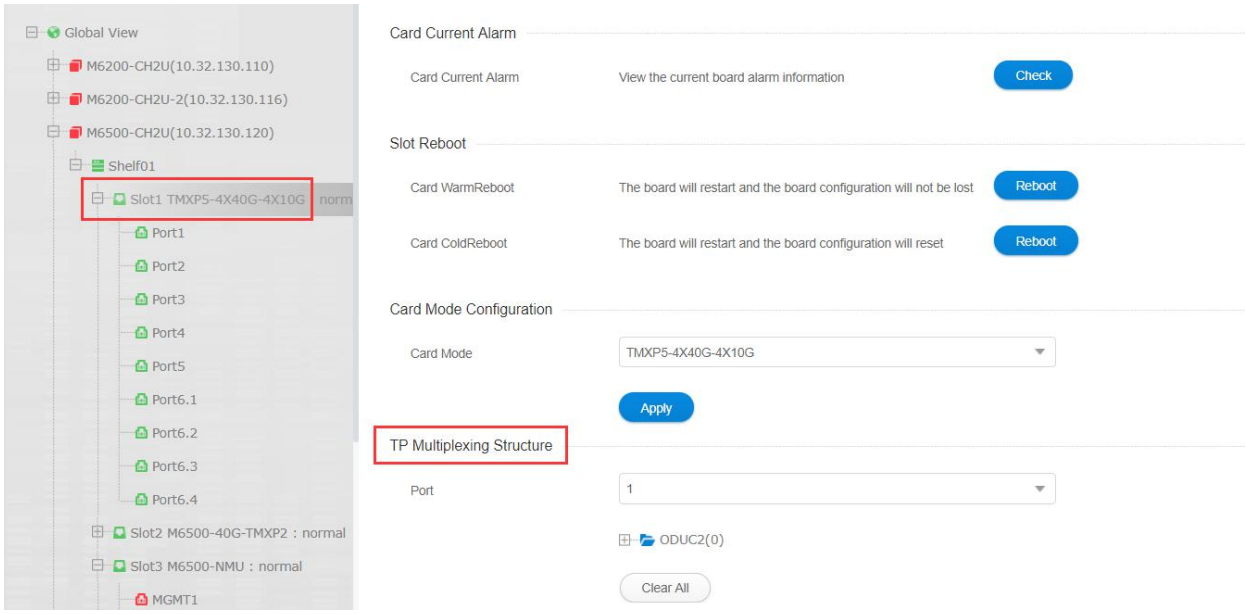



Figure5-66 M6500-TMXP5 TP Multiplexing operation steps

The interface after opening is as follows, select ODU4, it can be demultiplexed into ODU3 and ODU2/ODU2e.


Figure5-67 M6500-TMXP5 Demultiplexing configuration interface

Each ODU4 can be demultiplexed into 2 ODU3 in total, each ODU3 is configured with 31 time slots; and 2 ODU2/2e, each ODU2/2e is configured with 8 time slots.

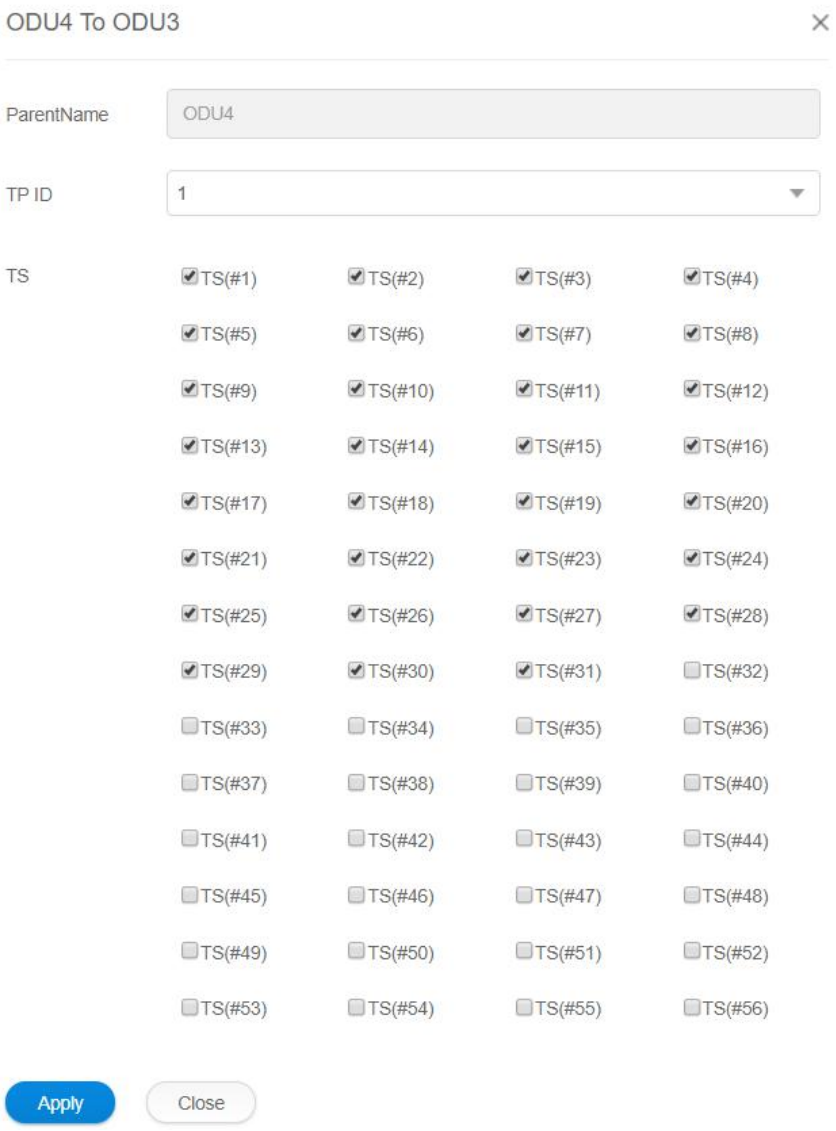



Figure5-68 M6500-TMXP5 Demultiplexing ODU3 time slot configuration

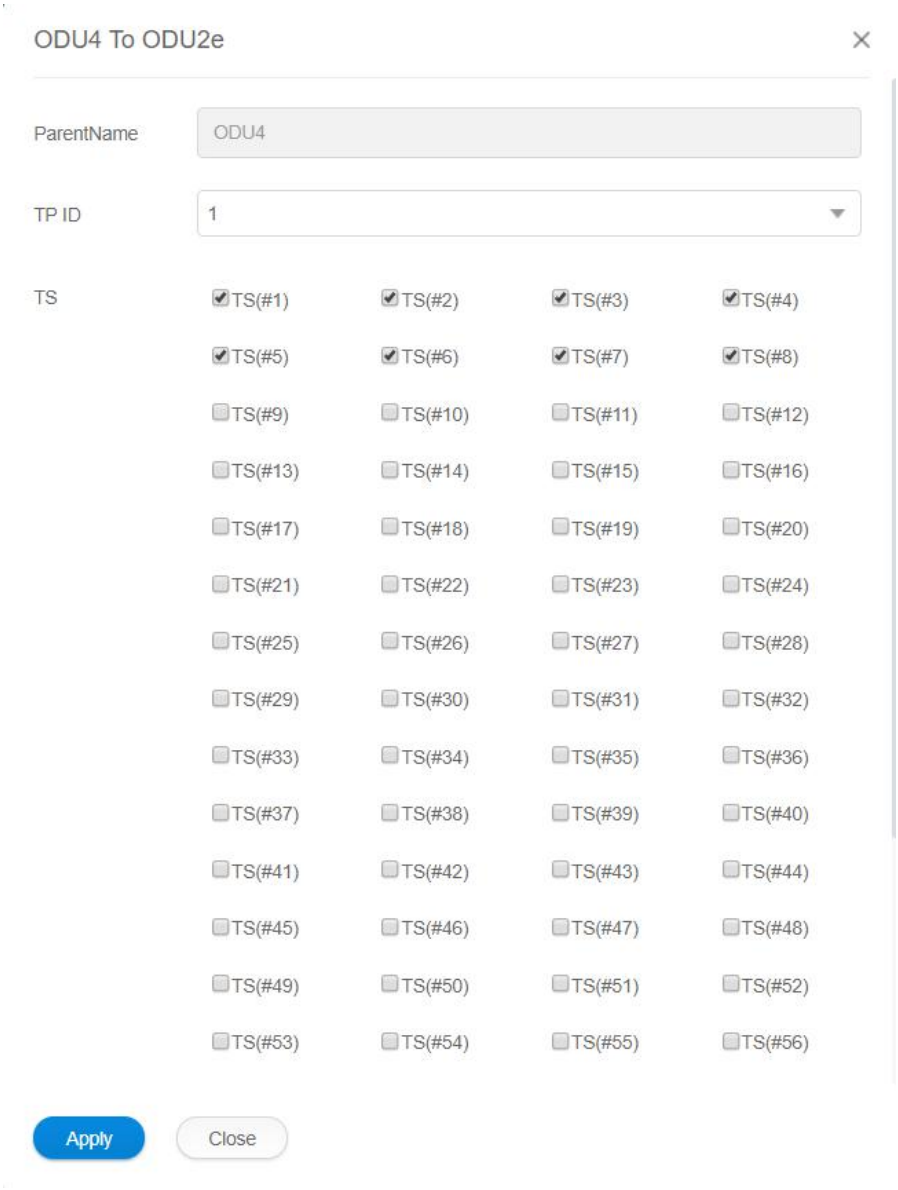



Figure5-69 M6500-TMXP5 Demultiplexing ODU2/2e time slot configuration

Fully configure 2 * ODU3 and 2*ODU2/2e is shown as below figure.

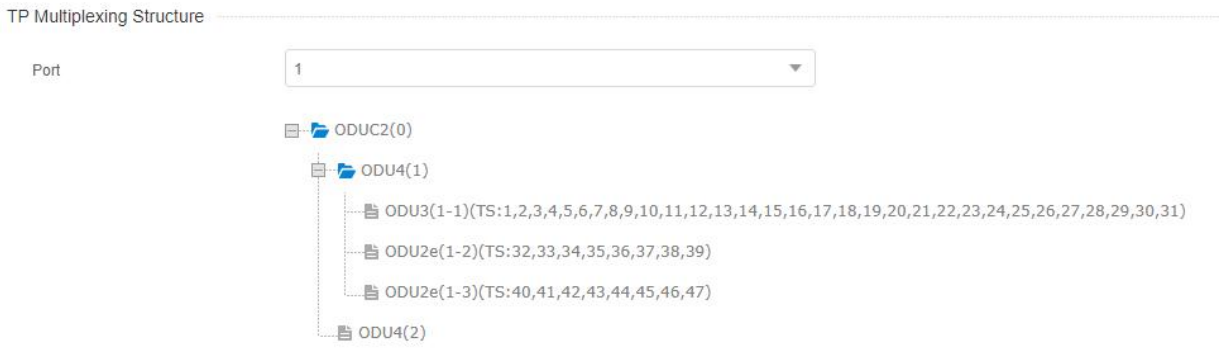



Figure5-70 M6500-TMXP5 demultiplexing 2*ODU3 and ODU2/2e configuration results

#### 5.4.3.3. Cross configuration

Taking the establishment of 40G service as an example, the operation is as follows: select FGE_GMP on the client side and OCh (OTUC2) on the line side, corresponding to the establishment of ODU3 crossover, as shown in the following figure.

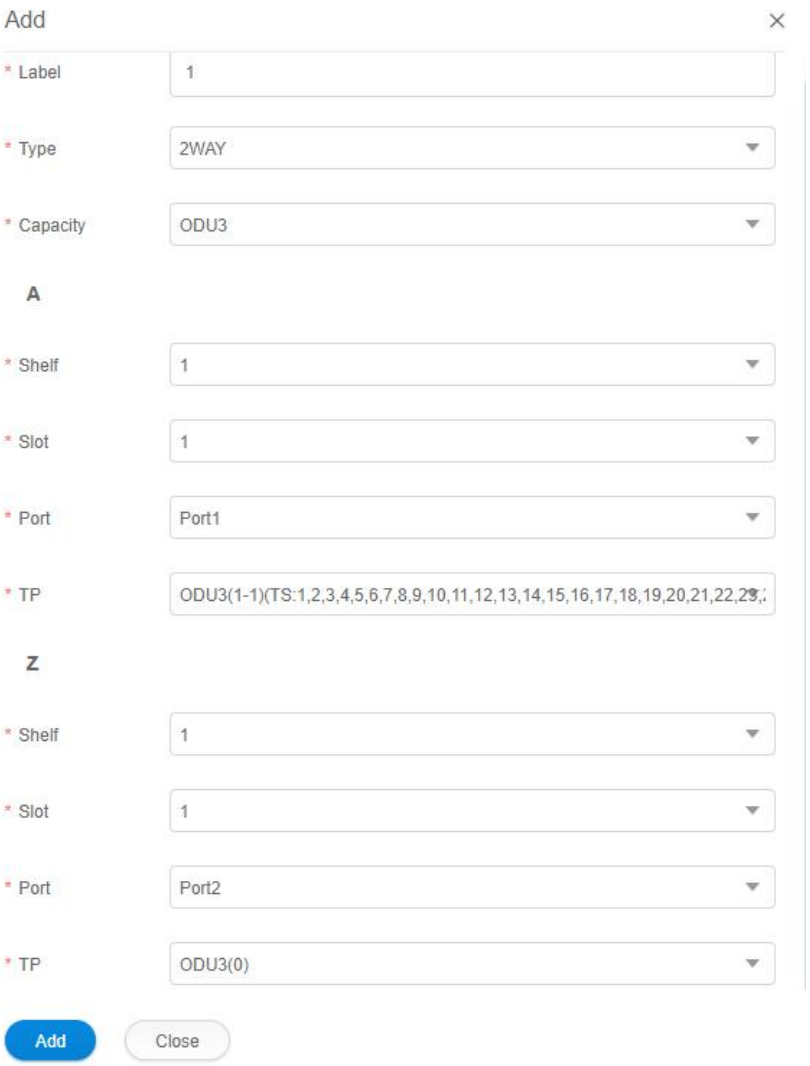



Figure5-71 M6500-TMXP5Two-way cross without protection

The cross establishment is successful as shown in the figure below.

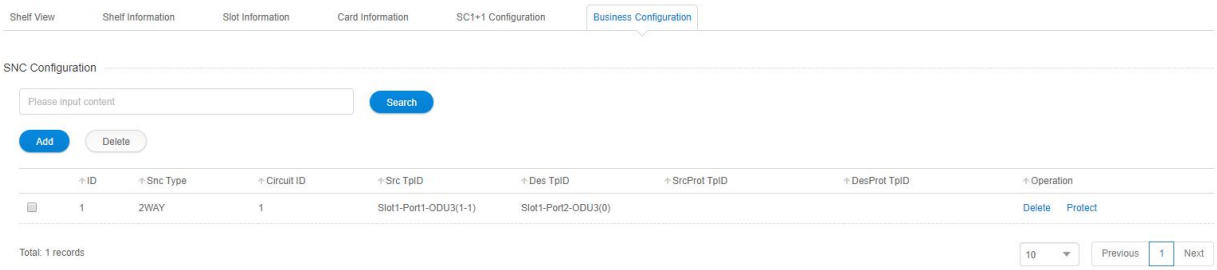



Figure5-72 Two-way without protection cross established successfully

#### 5.4.3.4. FEC Configuration

FEC only can be configured in OTU layer.

- **Line side port**

Select NE-Slot 1, click on "*Port1*" and select "*Port Management*" on the right, select OCh (OTUC2) or OCh (OTU4) as the port mode, select "*OTUC2*" or "*OTU4*" under "*Port Configuration*" and " *FEC Type*" option, check the configuration. When the line side is in 2*100G mode, there are a total of 6 FEC modes on the M6500-TMXP5 line side, which are SDFEC1_8QAM/SDFEC2_8QAM/SDFEC3_8QAM/SDFEC1_16QAM/SDFEC2_16QAM/SDFEC3_16QAM, and when the line side is 7 in the default mode, SDFEC3_16QAM is the default mode. The FEC modes are G709FEC/SDFEC1/SDFEC2/SDFEC3/SDFEC1_Non_diff/SDFEC2_Non_diff/SDFEC3_Non_diff, and SDFEC3 is the default mode. As shown below.

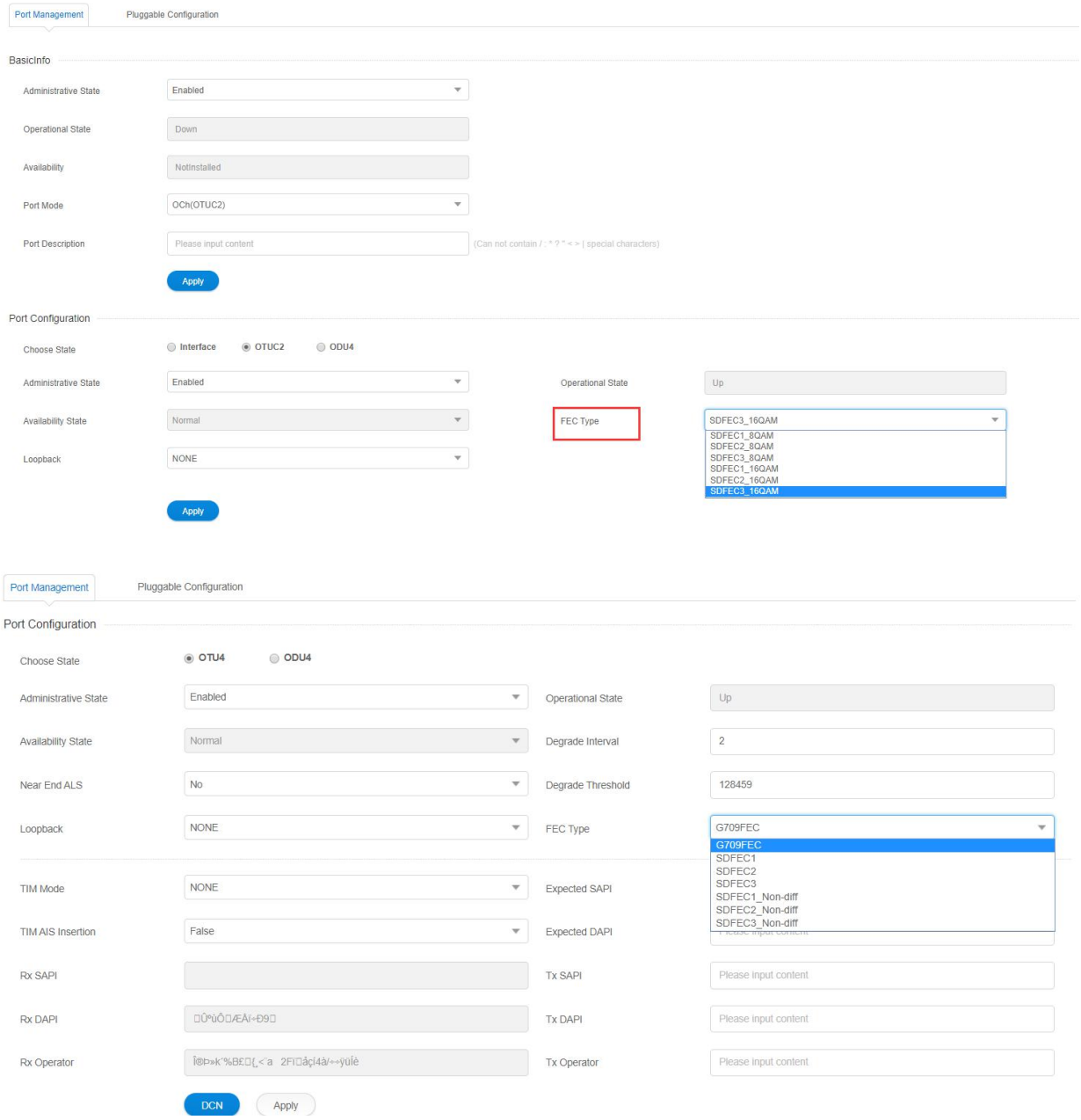



Figure5-73 M6500-TMXP5 Line side port FEC configuration

- **Client Side 100G port**

Select the NE-Slot 1, click on "*Port1*" and select "*Port Management*" on the right, select OTU4 as the port mode, and select the "*FEC Type*" option on the "*OTU4*" interface under "*Port Configuration*" to view the configuration ,

There are 7 types of 100G on the client side, and the default FEC mode is G709 FEC.The configuration is shown below.

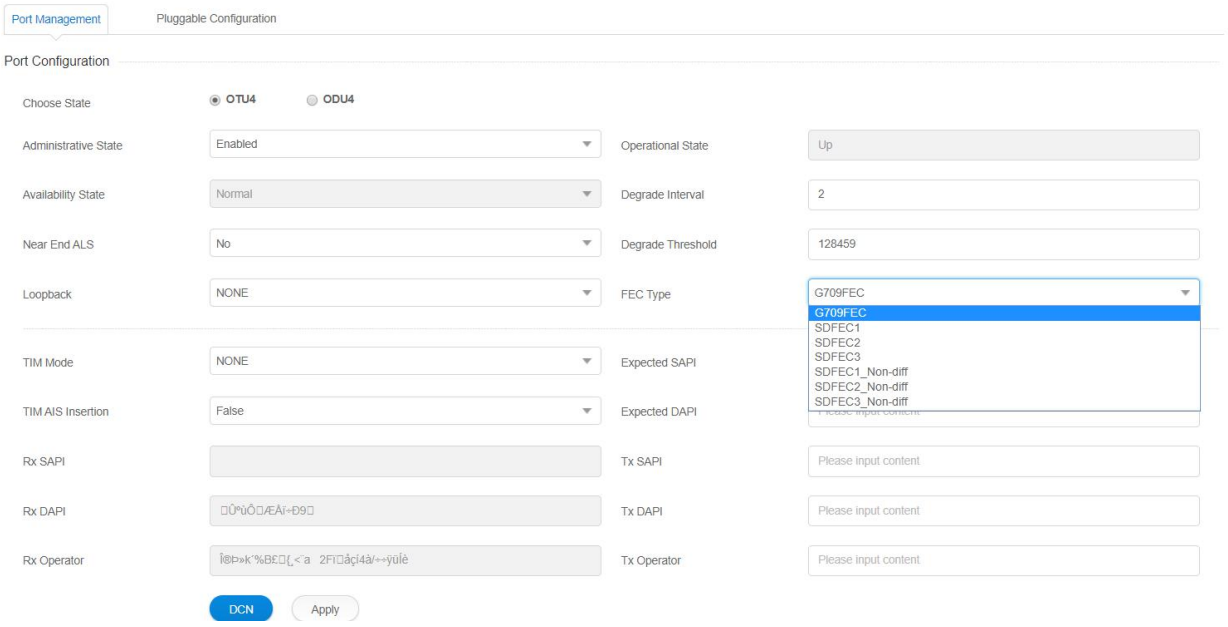



Figure5-74 M6500-TMXP5 Client side 100G Port FEC configuration

- **Client side 40G port**

Select the NE-Slot 1, click on "*Port 2*" and select "*Port Management*" on the right, select OTU3 for the port mode, select the "*FEC Type*" option on the "*OTU3*" interface under "*Port Configuration*", on the client side there are 4 FEC modes for 40G, namely no FEC/G709FEC/I.4EFEC/I.7EFEC, among which G709FEC is the default mode. The configuration is shown below.

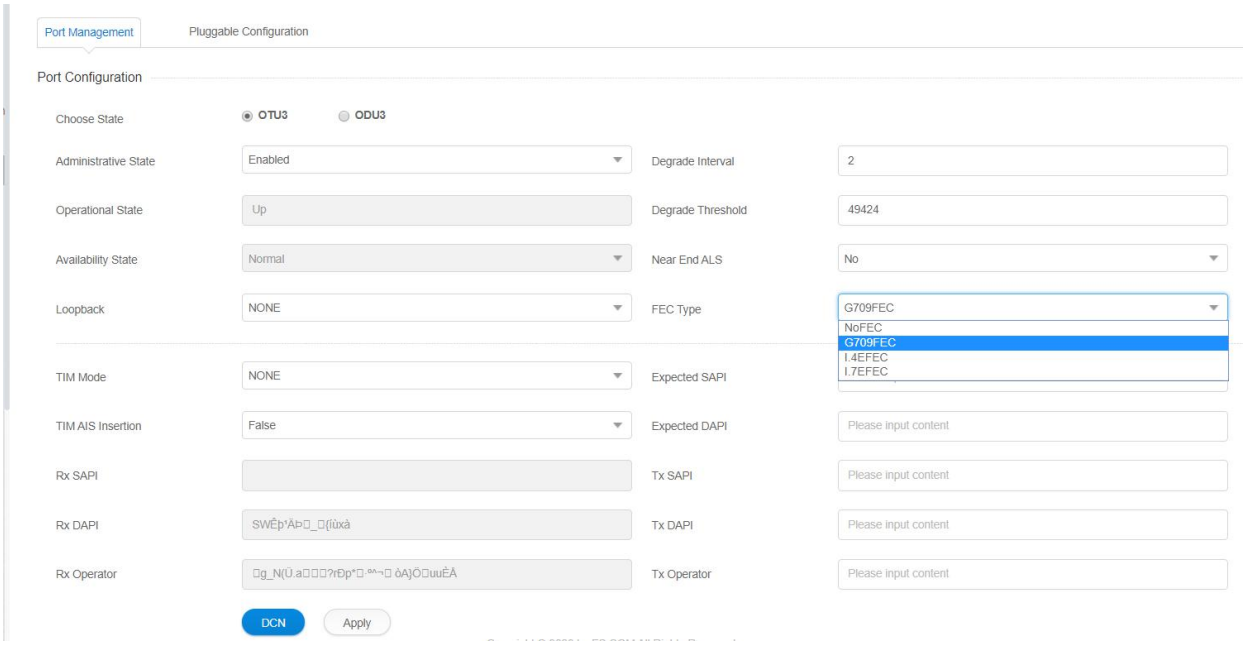



Figure5-75 M6500-TMXP5 Client side 40G port FEC configuration

- **Client side 10G Port**

Select the NE-Slot 1, click on "*Port 6.1*" and select "*Port Management*" on the right, select OTU2 as the port mode, select the "*FEC Type*" option on the "*OTU2*" interface under "*Port Configuration*", on the client side There are 4

FEC modes for 10G, namely no FEC/G709FEC/I.4EFEC/I.7EFEC, among which G709FEC is the default mode. The configuration is shown below.

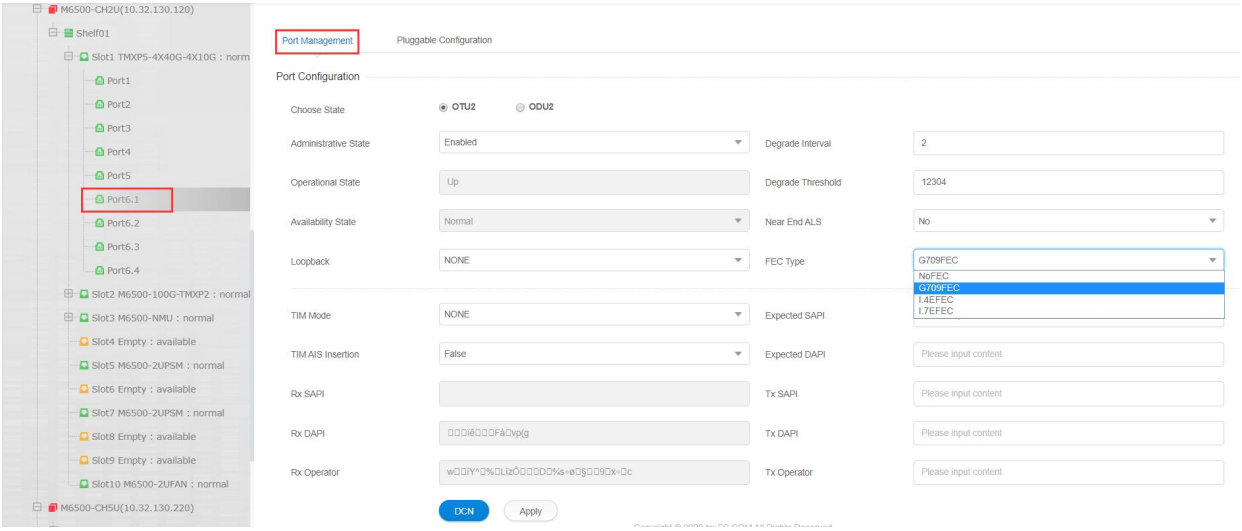



Figure5-76 M6500-TMXP5 Client side 40G Port FEC configuration

# 5.5. Configuration Example

## 5.5.1. Configuration Example of Ring Network Service

Here we take the ring network of Site A, Site B and Site C in M6500-TMXP2 board access 100G service as an example.

Configure the service type of the client side port1 as 100GE_GMP/GFPF, and the mode of the lien side port3 as OTU4 or OCh (OTU4).

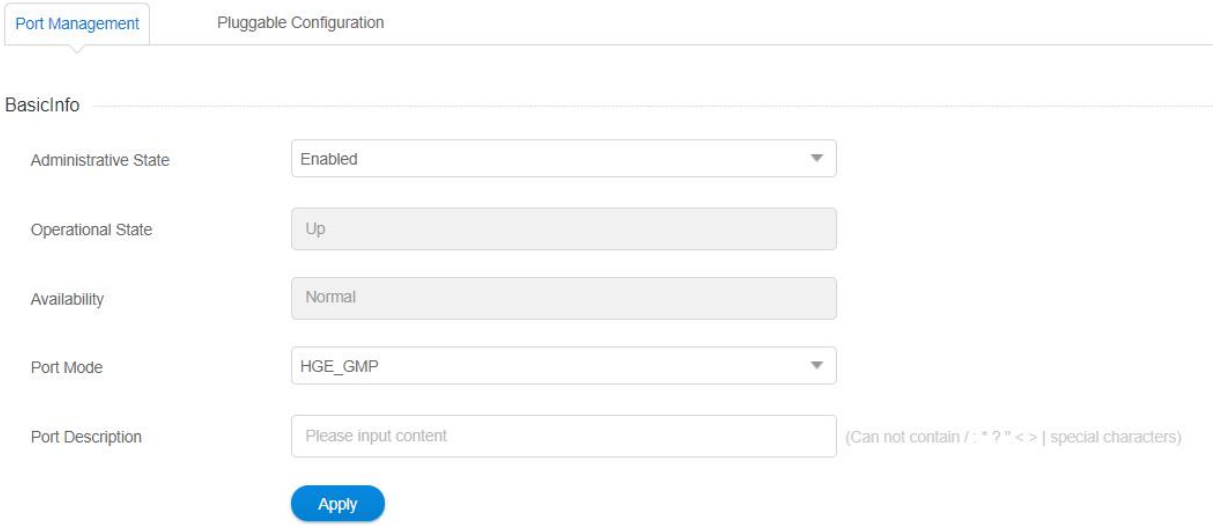



Figure5-77 Configure Client Side Signal Mode

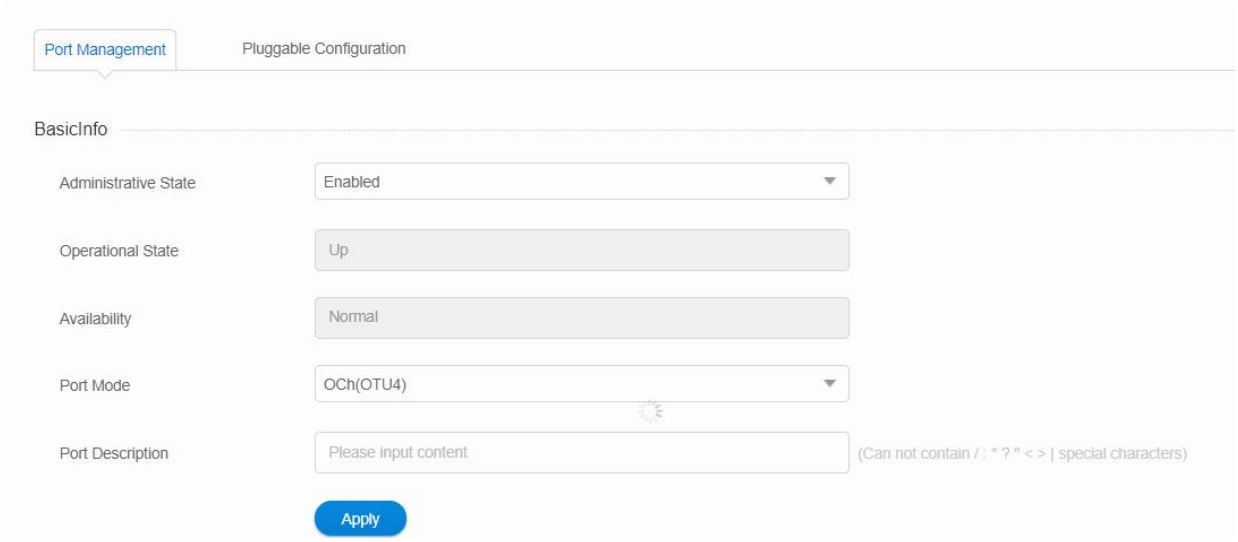
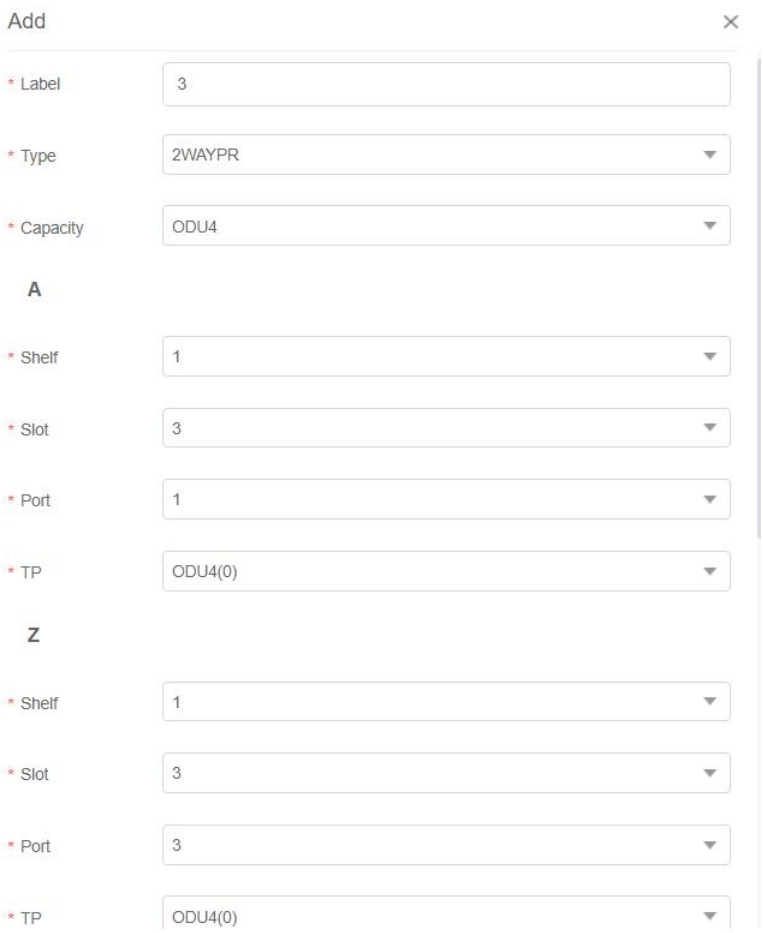



Figure5-78 Configure Line Side Signal Mode

Create cross-board two-way SNC cross-connection for ODU4 of the client side port1 to port3.



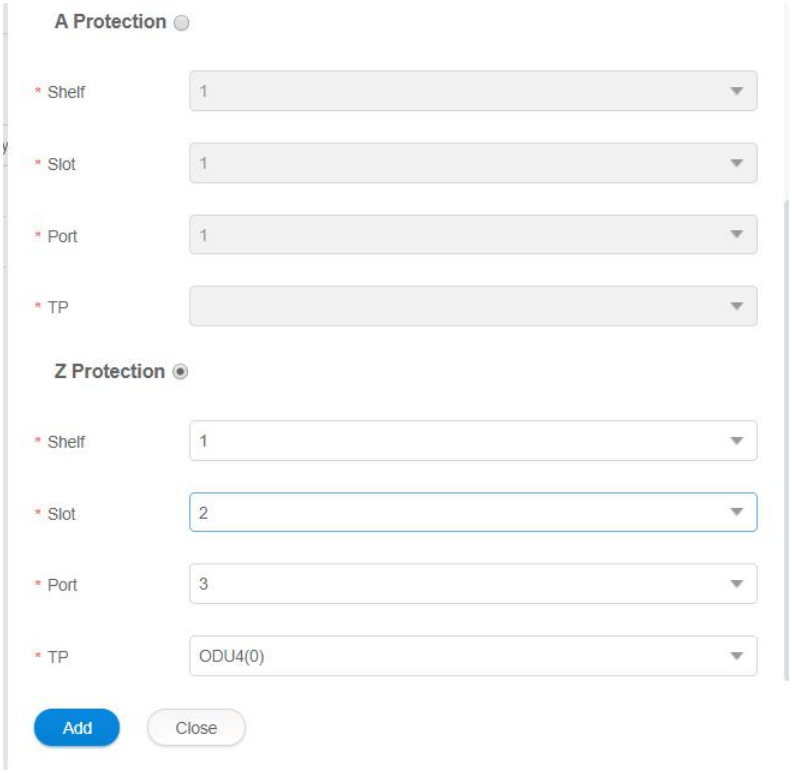



Figure5-79 Create Two-way Cross-Connection of ODU4

Build the environment according to the following diagram.

**Note**

- **Respectively create the two-way SNC cross-connection with protection of port1 to port3 (primary)/port3 (standby) at Site A and Site C.**
- **Ensure that the client side service types including mapping methods of Site A and Site C are the same.**
- **Create two-way cross-connection for ODU4 of port3 to port3 at Site B. Site B acts as the transparent transmission site.**

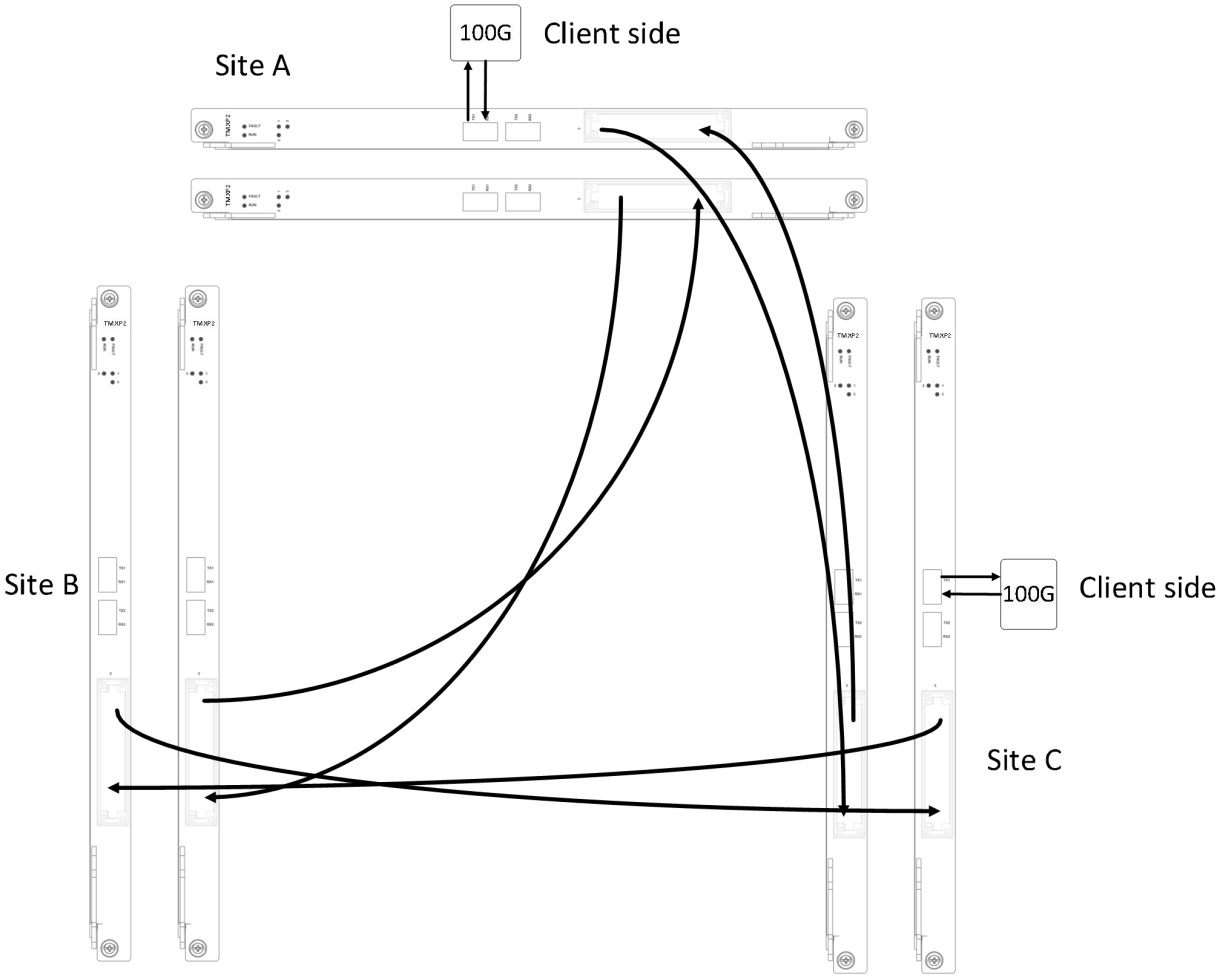



Figure5-80 Site-to-Site Primary and Standby Protection Environment

# 6. Overhead Configuration

## 6.1. Configuration Rules

The G.709 standard defines the overhead function of the OTN frame structure and the network of each layer. M6500adopts a lot of overhead bytes, which provides great convenience for equipment maintenance.

M6500usually configures overhead such as SM, PM, TCMi (i = 1 ~ 6)etc. This chapter describes in detail the configuration methods of various overhead, including: configuration rules, configuration steps and configuration examples.

### 6.1.1. SM, PM & TCMi Overhead Introduction

SM is the segment monitoring overhead byte of OTUk layer. By configuring the SM overhead, the performance and fault monitoring of the electrical regeneration segment can be carried out.

PM is the path monitoring overhead byte of ODUk layer. By configuring the PM overhead, the performance and failure of end-to-end wavelength service channel can be monitored.

The PM monitoring connection of the service should be established between the network elements of the service two ends. The SM monitoring connection of the service should be established between the service network element and the electrical relay network element or between the relay network element and the power. This product has no electrical relay applications, so SM planning and PM planning are usually the same.

### 6.1.2. Overhead Configuration Rules

SM and PM monitoring overhead can be configured on branch interface cards, line interface cardsand optical forwarding cards. The general principles are as follows (priority is determined in sequence):

1. SM must be terminated between the network elements at both ends of the power layer service, and the intermediate network elements can go through the optical layer without overhead monitoring.

2. For non-OTUk/ODUk services, when it is multiplexed or mapped to OTUk/ODUk services, the OTUk/ODUk services must establish PM connections, that is, PM connection enablement and monitoring enablement must be activated.

3. For OTUk services, the network elements connected with PM overhead need to be configured, but PM connection enablement must be prohibited.Monitoring enablement can be configured to "activate" or "inactivate" and it is suggested that it be set to activate. For ODUk services, PM monitoring enablement must be activated because there is no SM.

4. When OTUj / ODUj services are multiplexed and mapped to OTUk / ODUk (j < k) services, the location where configuration monitoring enable "activation" / "inactivation" includes the call port (such as the Client / Port port) and the call ODTUjk port.

### 6.1.3. TTI Configuration Rules

After configuring the connection enablement or monitoring enablement of SM and PM, TTI is also required to be configured. TTI is a path trace marker that exists in PM and SM overhead bytes to test whether the corresponding overhead is correctly connected.

TTI includes SAPI and DAPI. SAPI value and DAPI value sent by single card at the opposite end are required to be consistent with SAPI value and DAPI value expected to be received by single card at the local end, and SAPI value and DAPI value sent by single card single card at the local end are consistent with SAPI value and DAPI

value expected to be received at the opposite end. That is to say, the two network elements connected by the overhead should meet the rules as shown in table 6-1:

Table6-1 Overhead Establishment Rules

| NE A | | Set Relationship | NE B | |
|---|---|---|---|---|
| Send TTI | SAPI | = | SAPI | Receive TTI |
| | DAPI | = | DAPI | |
| Receive TTI | SAPI | = | SAPI | Send TTI |
| | DAPI | = | DAPI | |

# 6.2. Configuration Steps

## 6.2.1. SM Configuration Steps

Here we take M6500-MXP10 board as an example to introduce the SM configuration steps:

- Activate the connection and monitoring enablement of SM overhead.

In M Series NMS, the service XGE_GFPF is configured for port 1 of the local end and opposite end of M6500-MXP10 board (Specific service is configured according to actual demand). OTU4 service is configured for port 11 of the local-end and opposite-end board (Specific service is configured according to actual demand). Demultiplex ODU4 to ODU2, configure service cross-connection, connect optical fiber and build the environment.

### Configuration Steps

Click on port 11 at the local end to enter the port management interface of the local end. Click on and enter"*OTU4*"option interface, then set"*Path Trace Mismatch (TIM) Mode*" as"*Source & Destination Access Identifier*"(SAPI&DAPI), and set the status of"*Path Trace Mismatch (TIM) Affects Service*"as"*Yes*". The opposite-end SM overhead configuration method is the same as that of the local end, we will not go into much detail here.

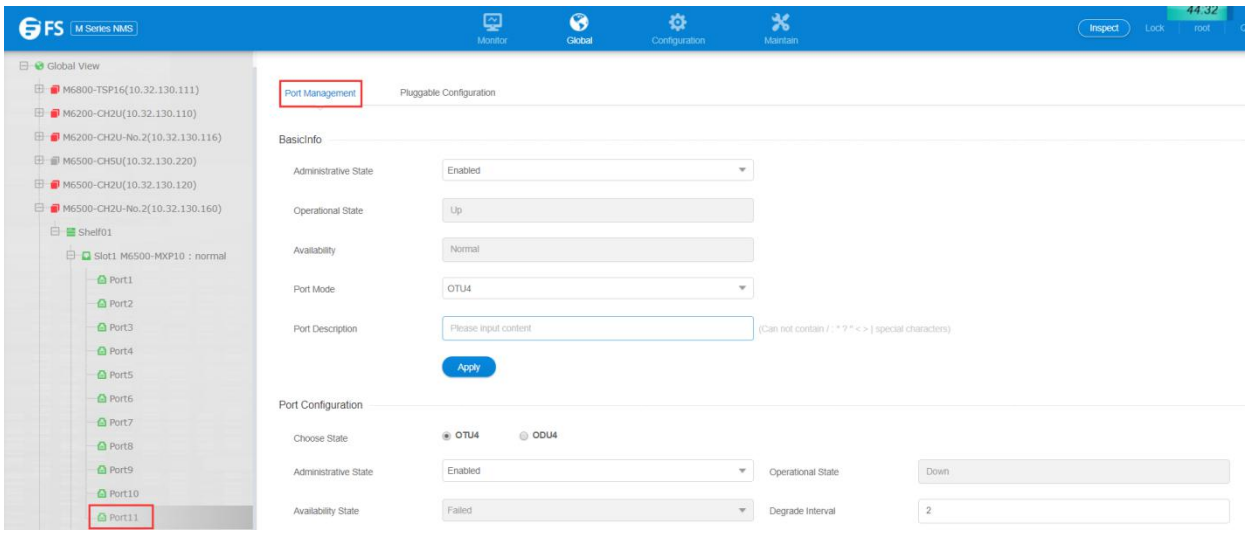



Figure6-1 Enter Port Management Interface

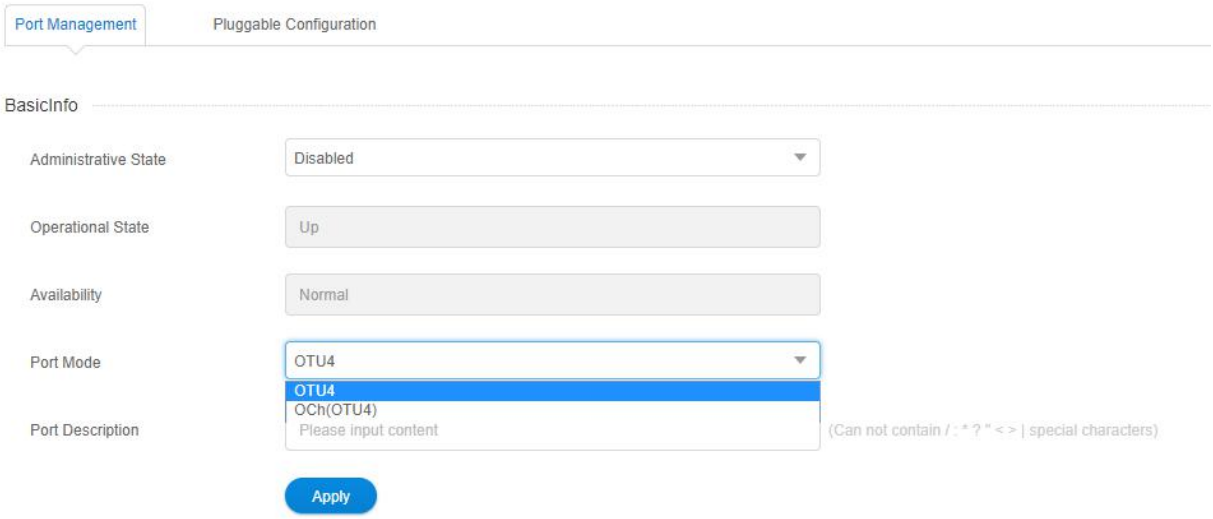



Figure6-2 Select Port Service

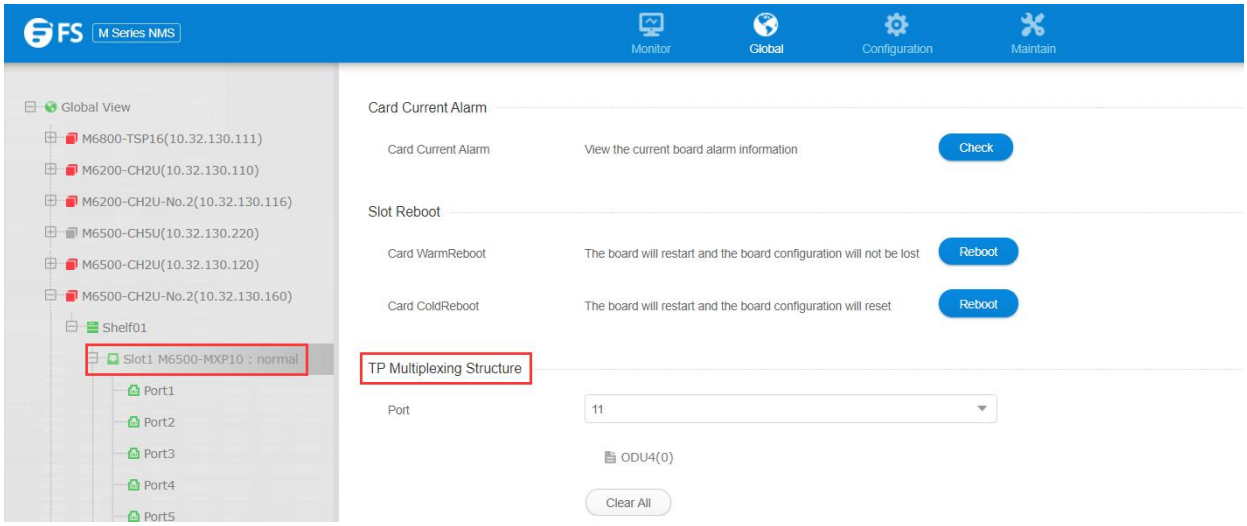



Figure6-3 Enter TP Multiplexing Interface


Figure6-4 TP Multiplexing Configuration Step 1

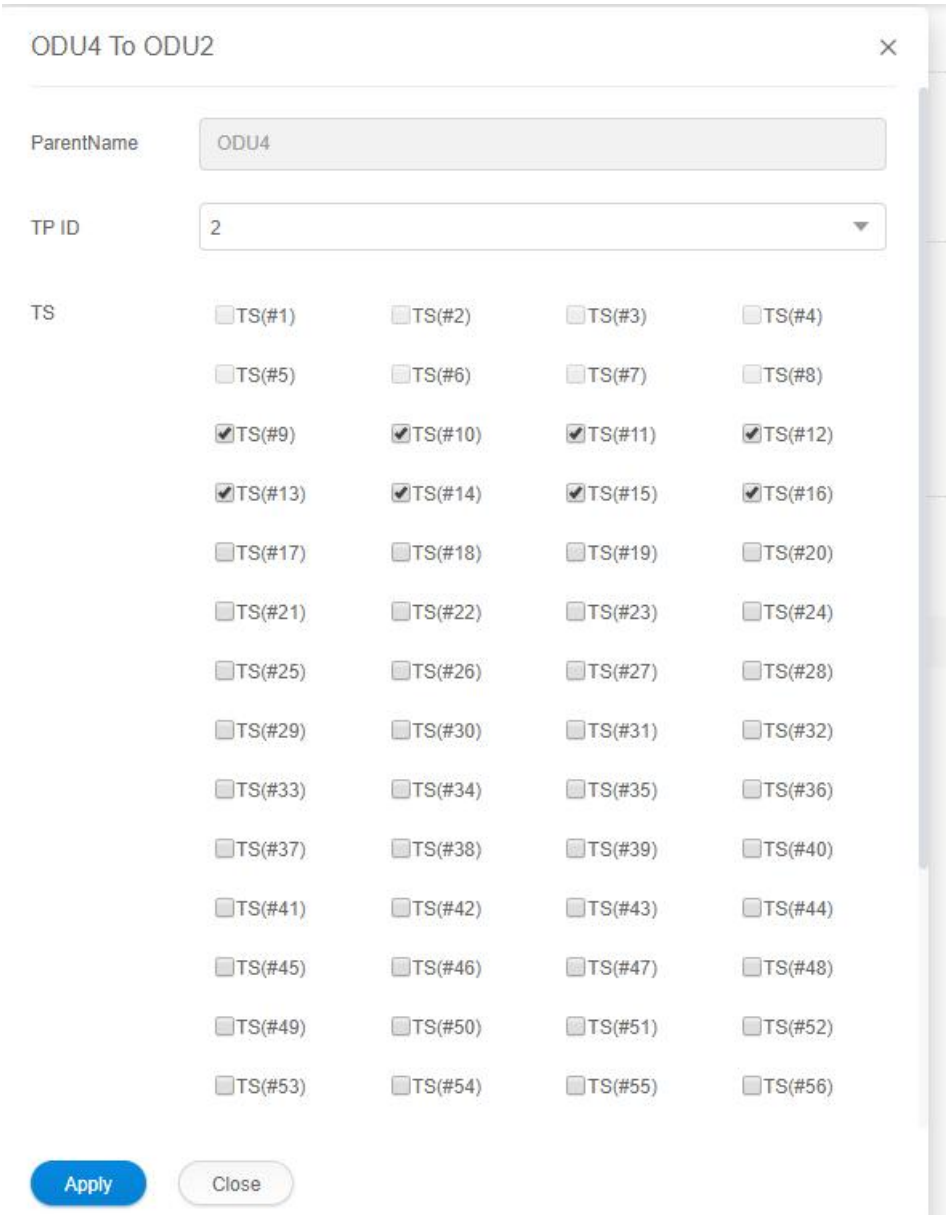



Figure6-5 TP Multiplexing Configuration Step 2

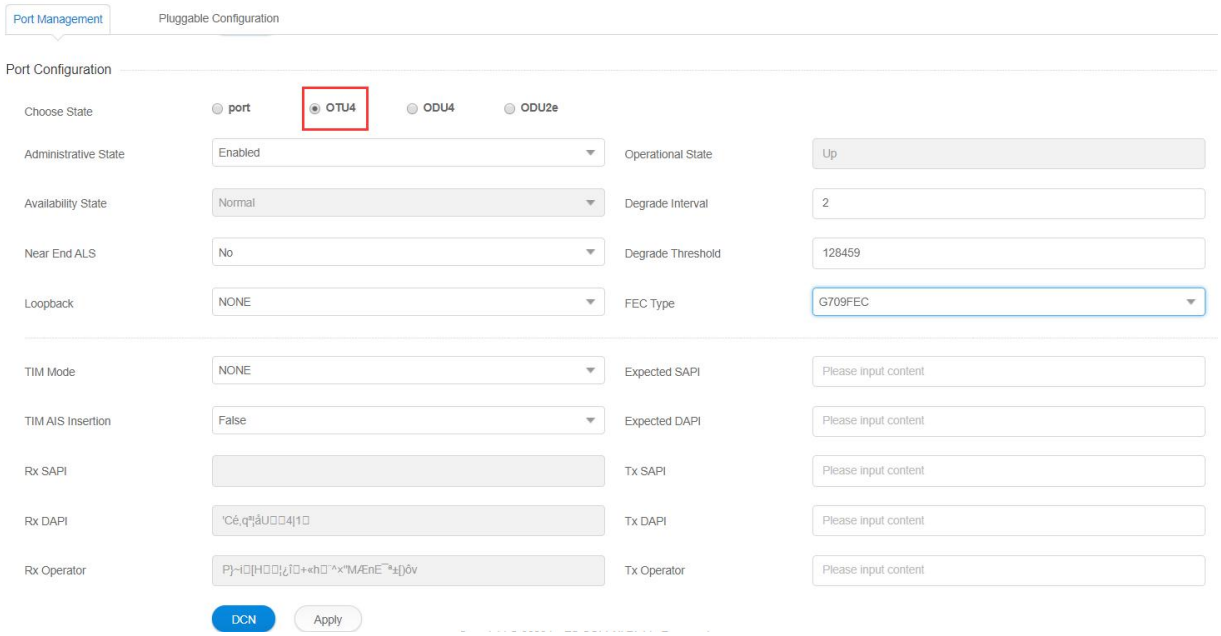



Figure6-6 Click to Enter OTU4 Port Interface

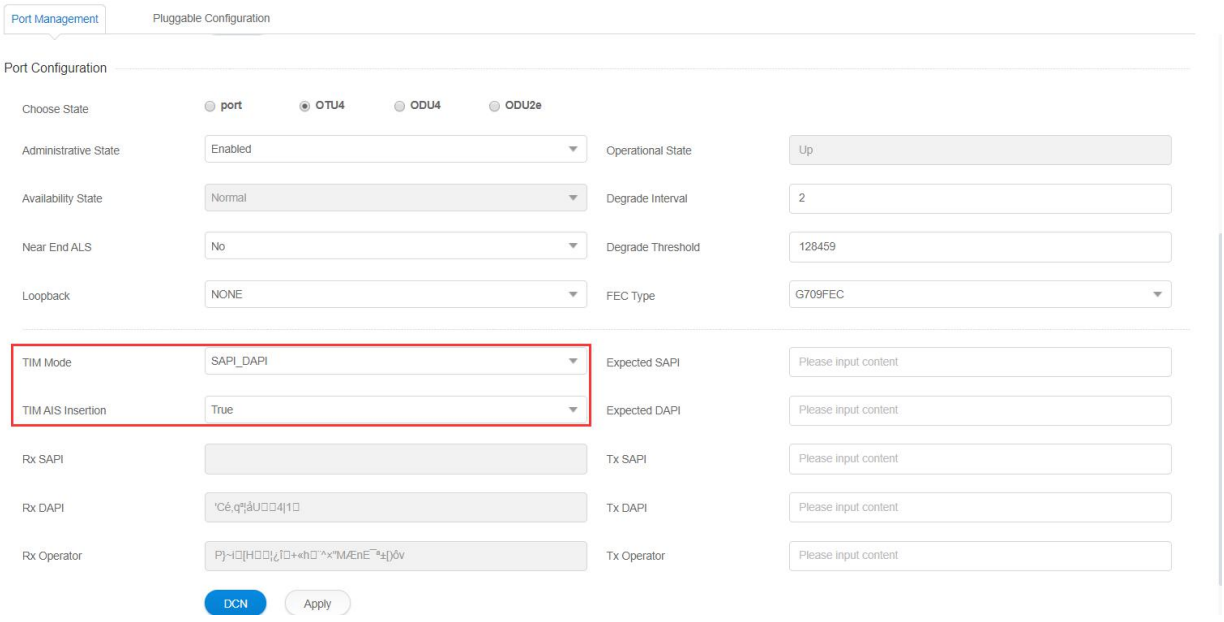



Figure6-7 Set SM Overhead

- TTI Configuration

Enter"*OTU4*" interface of the local and opposite ends to configure"*Send TTI*"and "*Expect to Receive TTI*"of "*SM*"overhead for the corresponding port. The configuration rules are as shown in the table above. Configure the expected and sent source access point identifier (SAPI), the expected and sent destination access point identifier (DAPI). The opposite-end TII configuration method is the same as that of the local end.

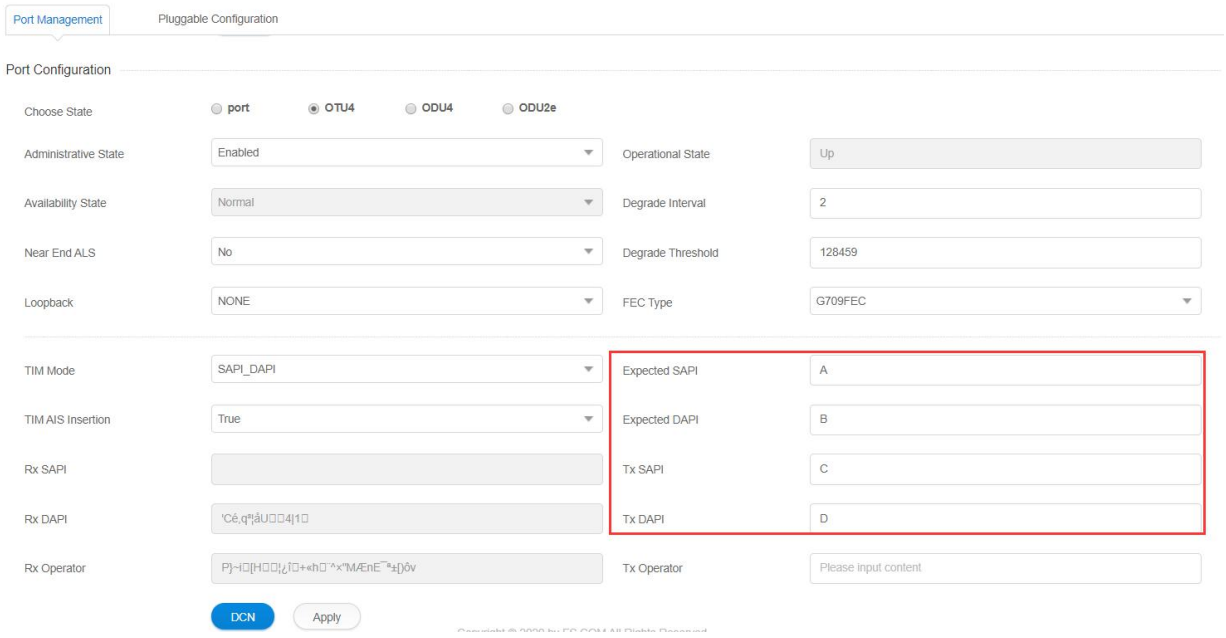



Figure6-8 Configure Local-End TTI

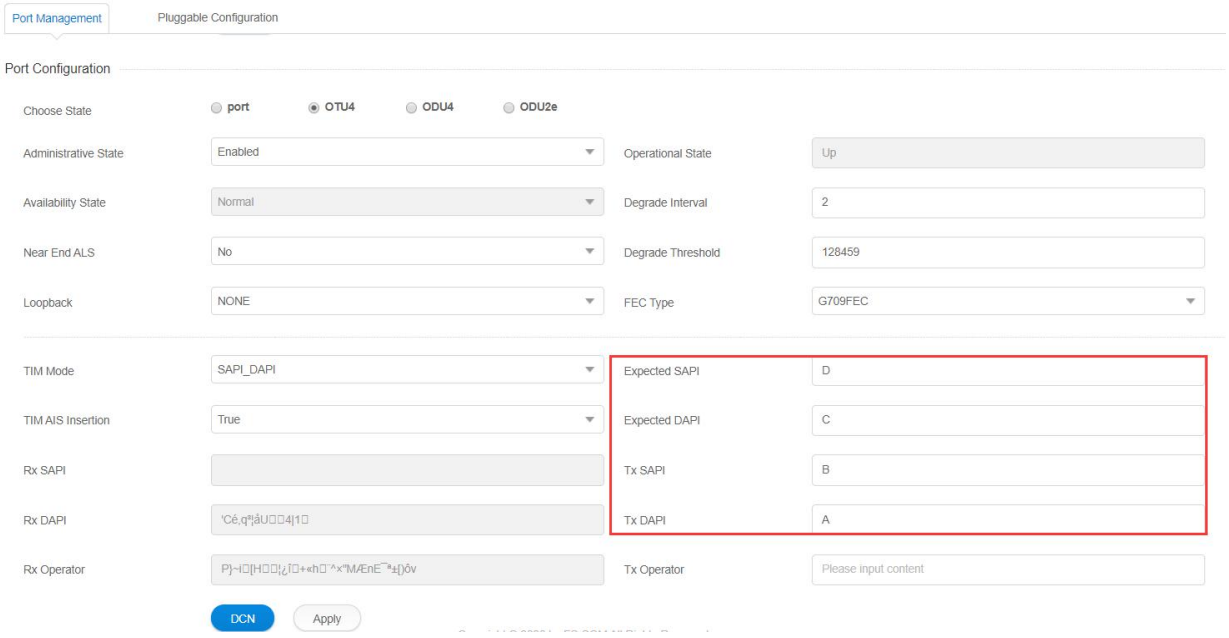



Figure6-9 Configure Opposite-End TTI

**Attention**

**The Source Access Identifier and Destination Access Identifier values in the TTI overhead can be either default or arbitrary strings.**

## 6.2.2. PM Configuration Steps

- Activate the connection and monitoring enablement of PM overhead.

In M Series NMS, the service XGE_BMP is configured for port 1 of the local end and opposite end of M6500-MXP10 board (Specific service is configured according to actual demand). OTU4 service is configured for port 11 of the local-end and opposite-end board (Specific service is configured according to actual demand).

Demultiplex ODU4 to ODU2e, configure service cross-connection, connect optical fiber and build the environment.

For line side Port 11: If the status of ODU layer is“unterminated”, then only expected TTI can be set, but sent TTI cannot be set. It is used as a monitoring function, which checks whether the signal received on the line side is correct.

For client side Port 1: If the status of ODU layer is“client side signal terminated”, then both expected TTI and sent TTI can be set. They are used to test the signal, which tests whether the client side signal sending source and receiving source are correct. The PM overhead configuration of the opposite end is the same as that of the local end. We will not go into too much detail.

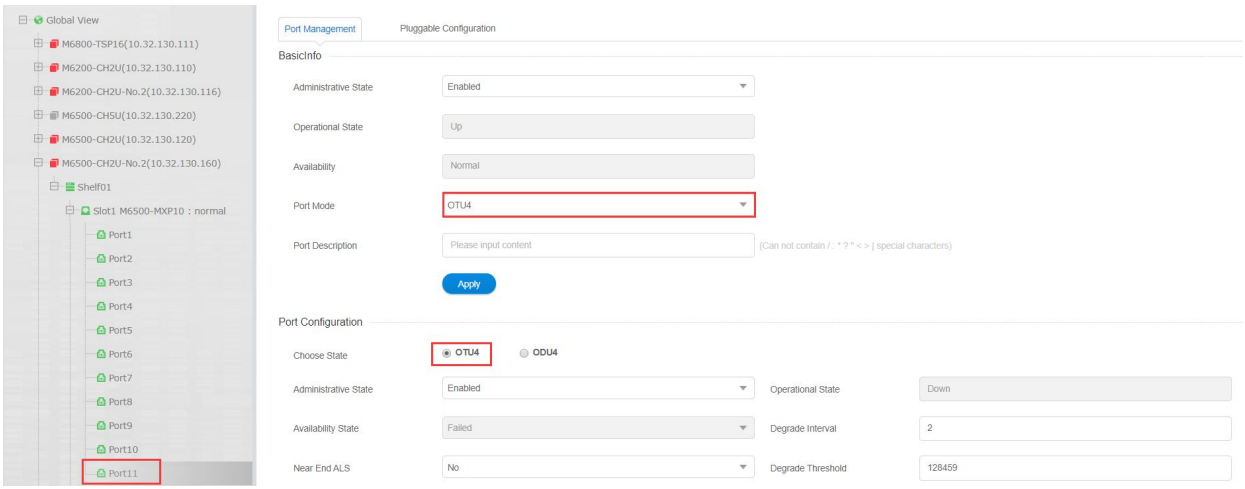



Figure6-10 Enter Line Side Port Management Interface

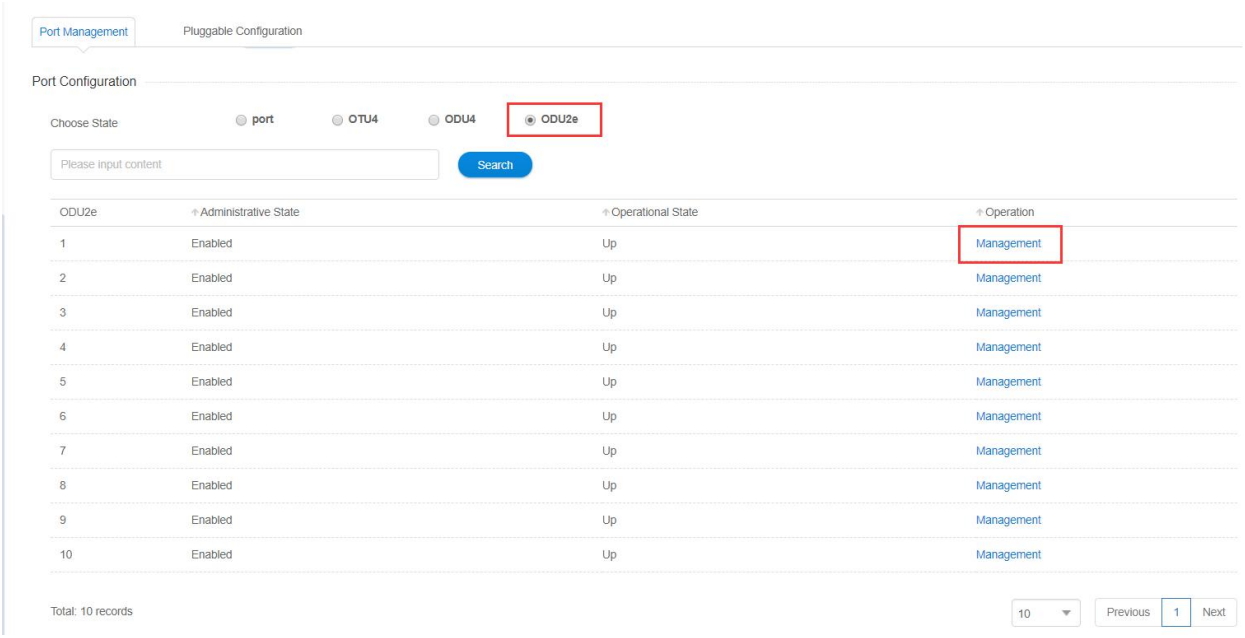



Figure6-11 Enter Line Side ODU2e Management Interface

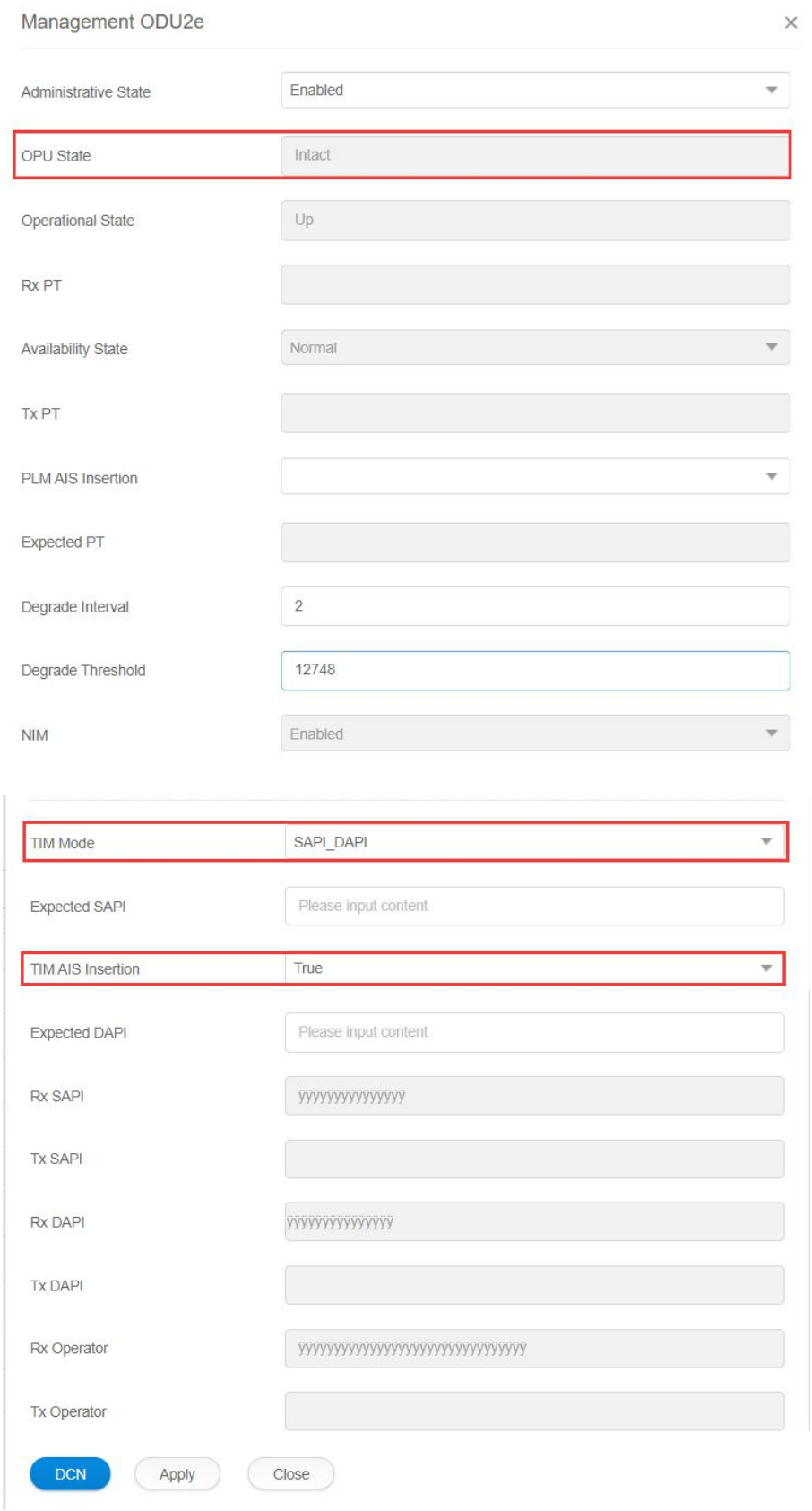



Figure6-12 Set Line Side PM Overhead

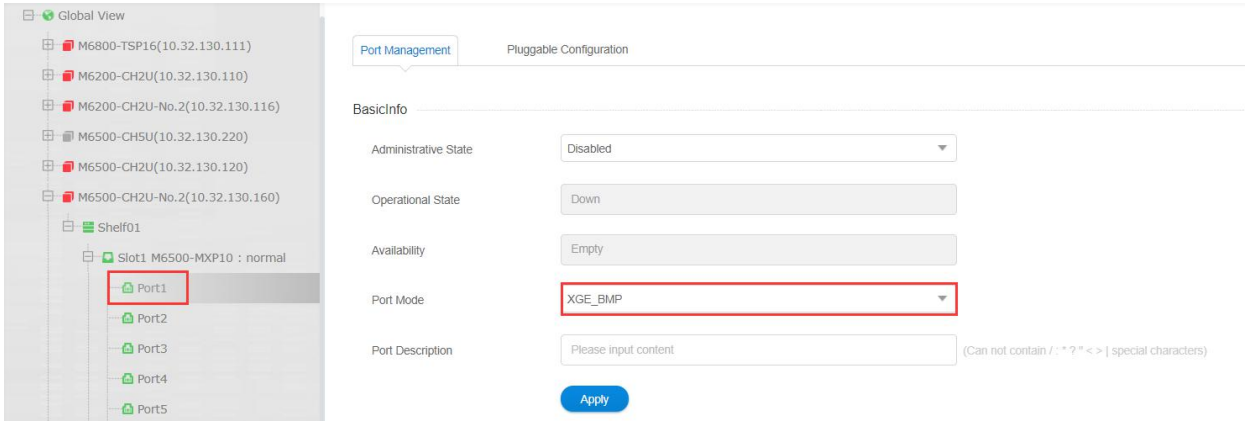



Figure6-13 Enter Client Side Port Management Interface

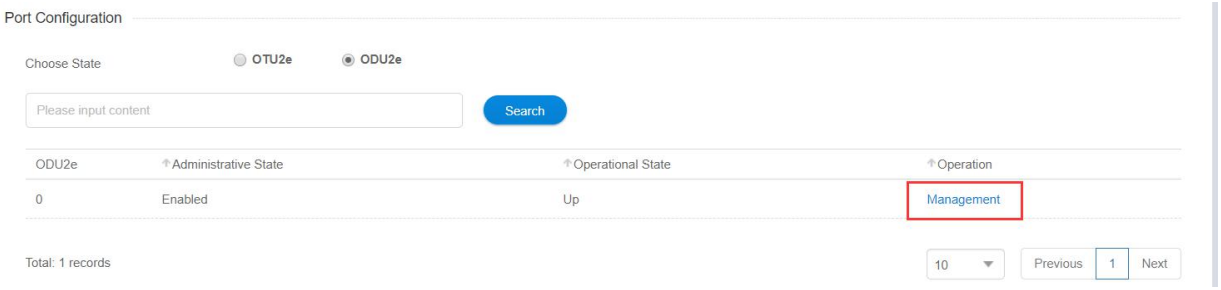
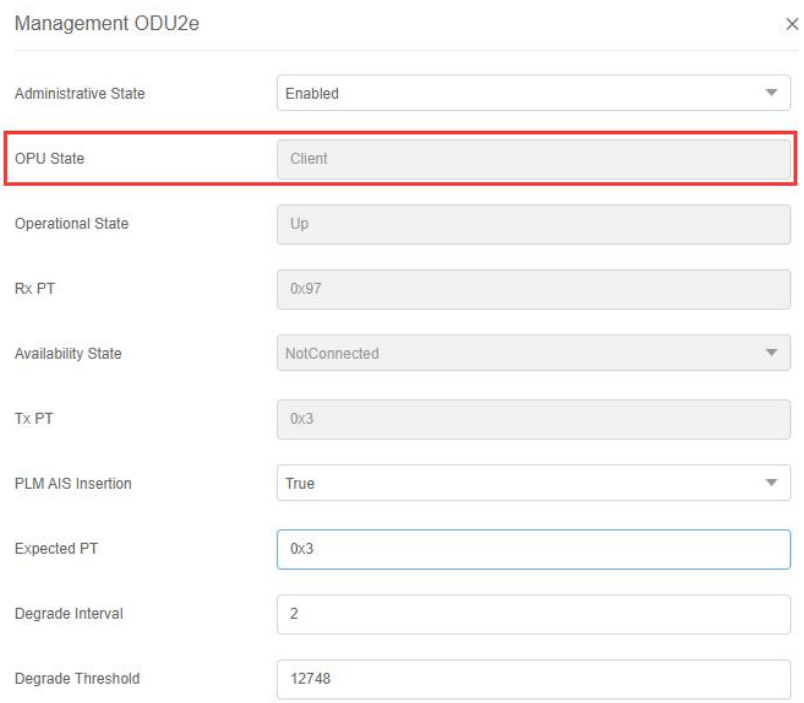



Figure6-14 Enter Client Side ODU2 Management Interface



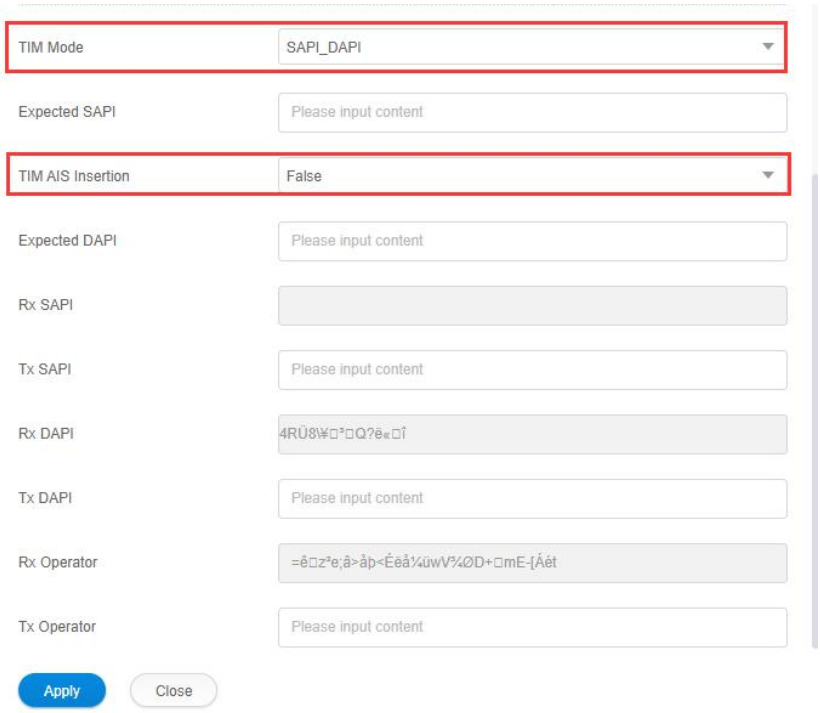



Figure6-15 Set Client Side PM Overhead

- TTI Configuration

Enter“ODU2”/“ODU2e”interface of line side local and opposite ends to configure “Expected Receiving TTI”of “PM” overhead for the corresponding port and to monitor whether the line side receiving signal is correct. Configure the expected source access point identifier (SAPI) and expected destination access point identifier (DAPI) (Here ODU2/ODU2e is prohibited to set sent SAPI and DAPI).

Enter“ODU2”/“ODU2e”interface of the client side local and opposite ends to configure “expected receiving TTI”and“sending TTI”of “PM” overhead for the corresponding port. Configure the expected source access point identifier and sent source access point identifier (SAPI), as well as expected destination access point identifier and sent destination access point identifier (DAPI). The TTI configuration steps of the opposite end are the same as those of the local end. Here we will not go into too much detail.

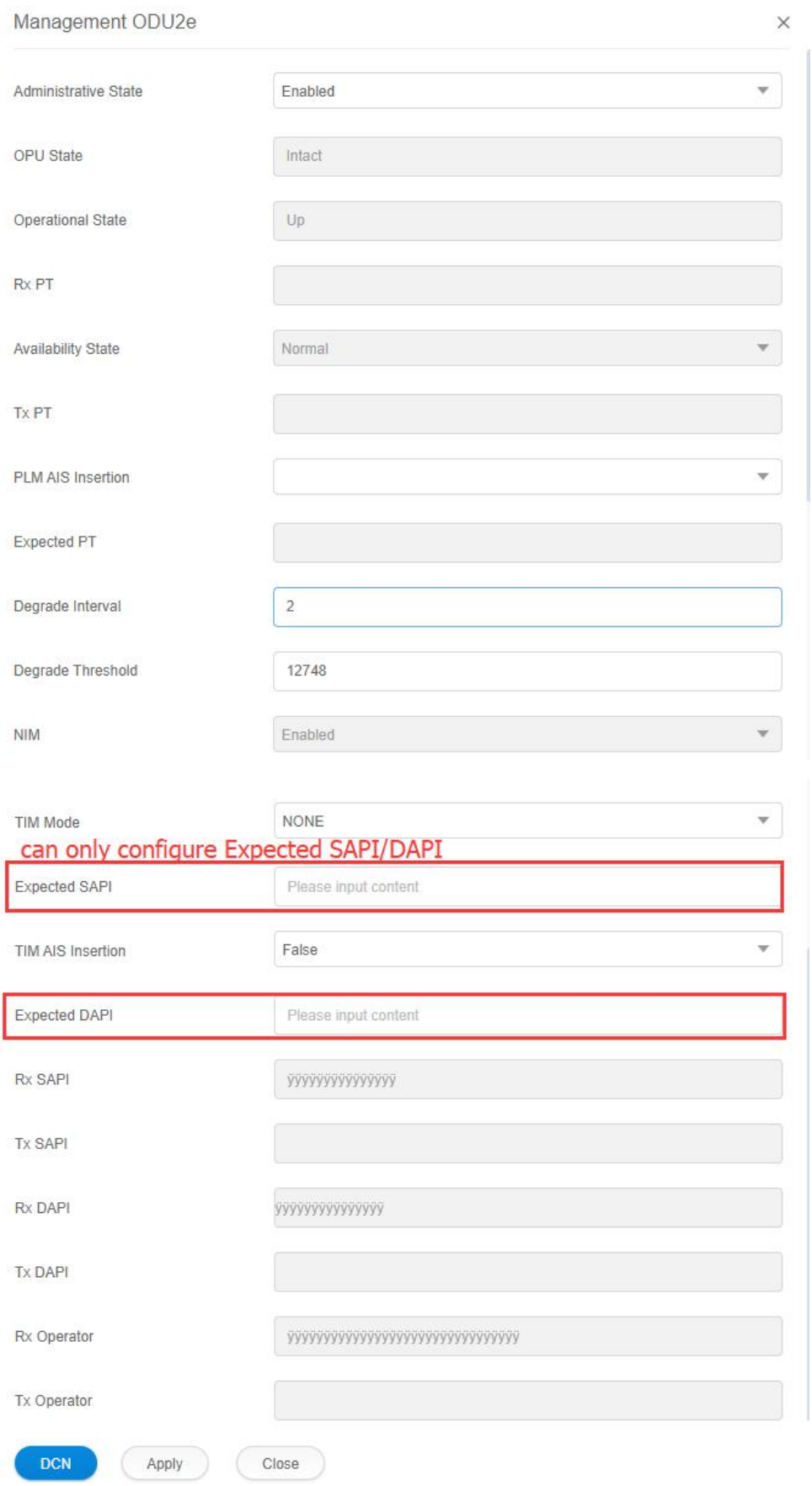



Figure6-16 Configure Line Side Port TTI

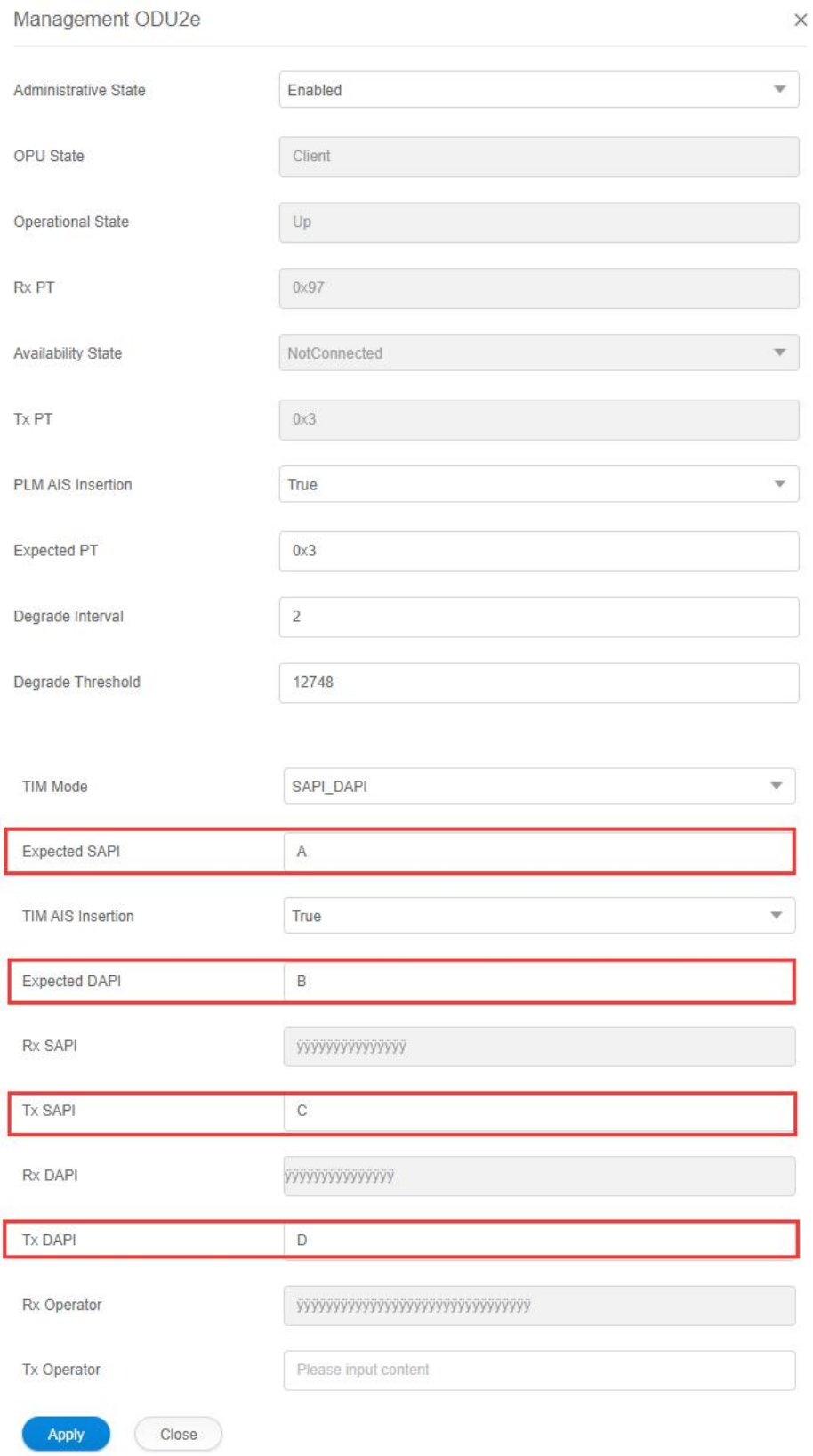



Figure6-17 Configure Client Side Local End Port TTI

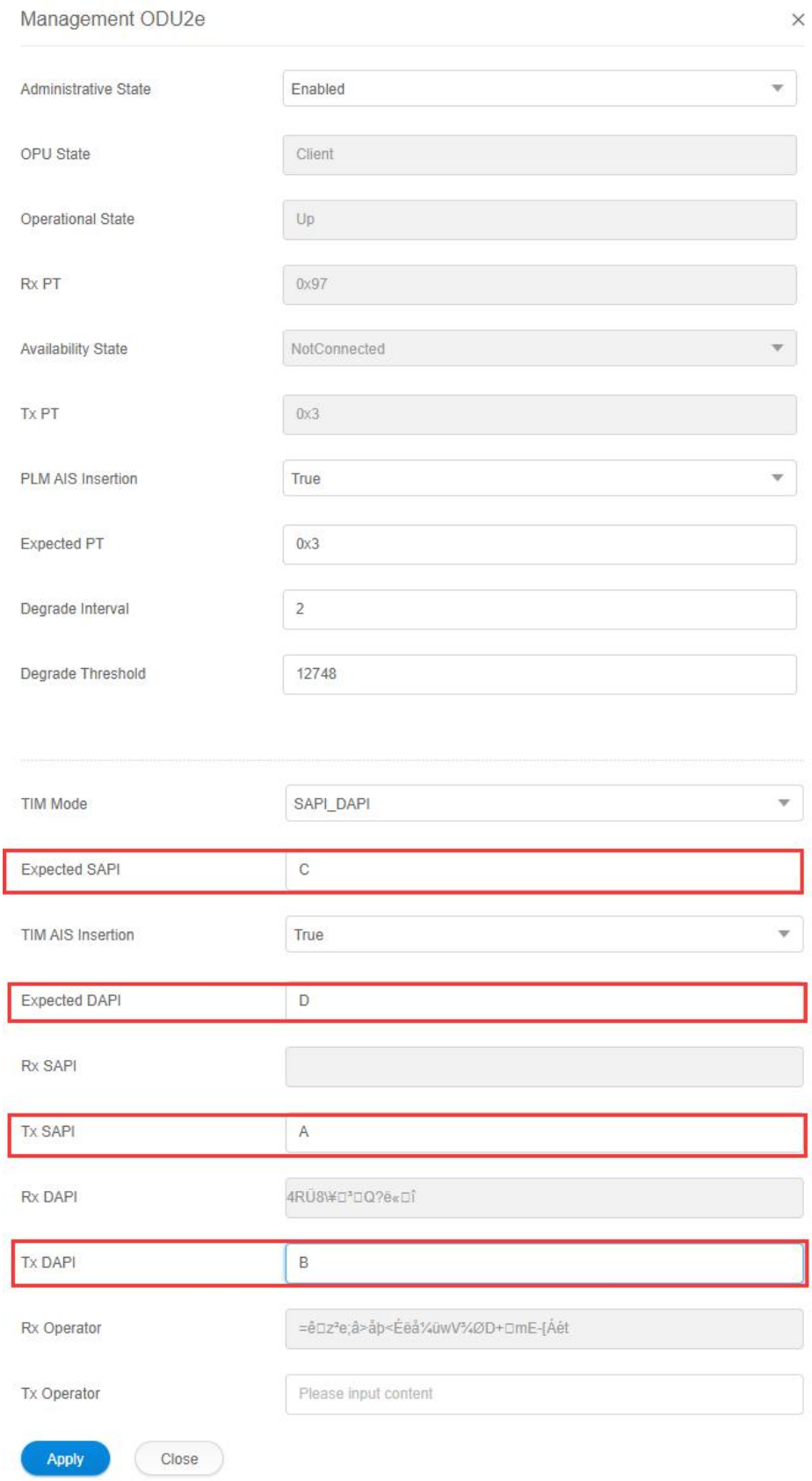



Figure6-18 Configure Client Side Opposite End Port TTI

**Hint**

**The Source Access Identifier and Destination Access Identifier values in the TTI overhead can be either default or arbitrary strings.**

# 6.3. Configuration Examples

Application Environment：

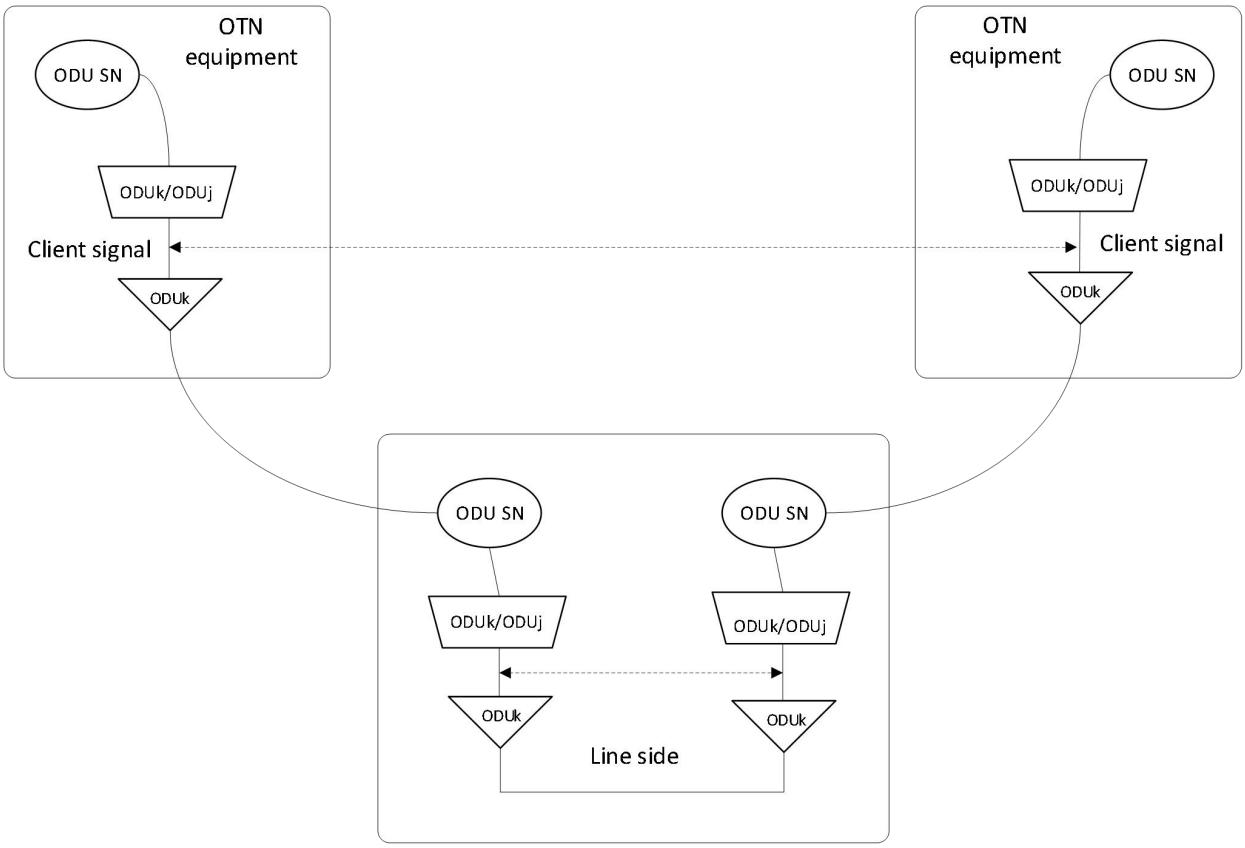



Figure6-19 Application Environment of SM/PM Overhead Configuration

Configuration analysis: The network elements of the local-end and opposite-end client side signals should be configured with the same service, such as XGE_GFPF service (Specific configuration needs to be made according to actual needs). The capacity of the local-end and opposite-end client side signals is ODU2.The OTU2 service is configured on both ends of the line side (configure according to the service type of the client side), and both ends are demultiplexed to ODU2.

According to the SM overhead configuration rules described in 6.1.2, the SM overhead is planned as follows:

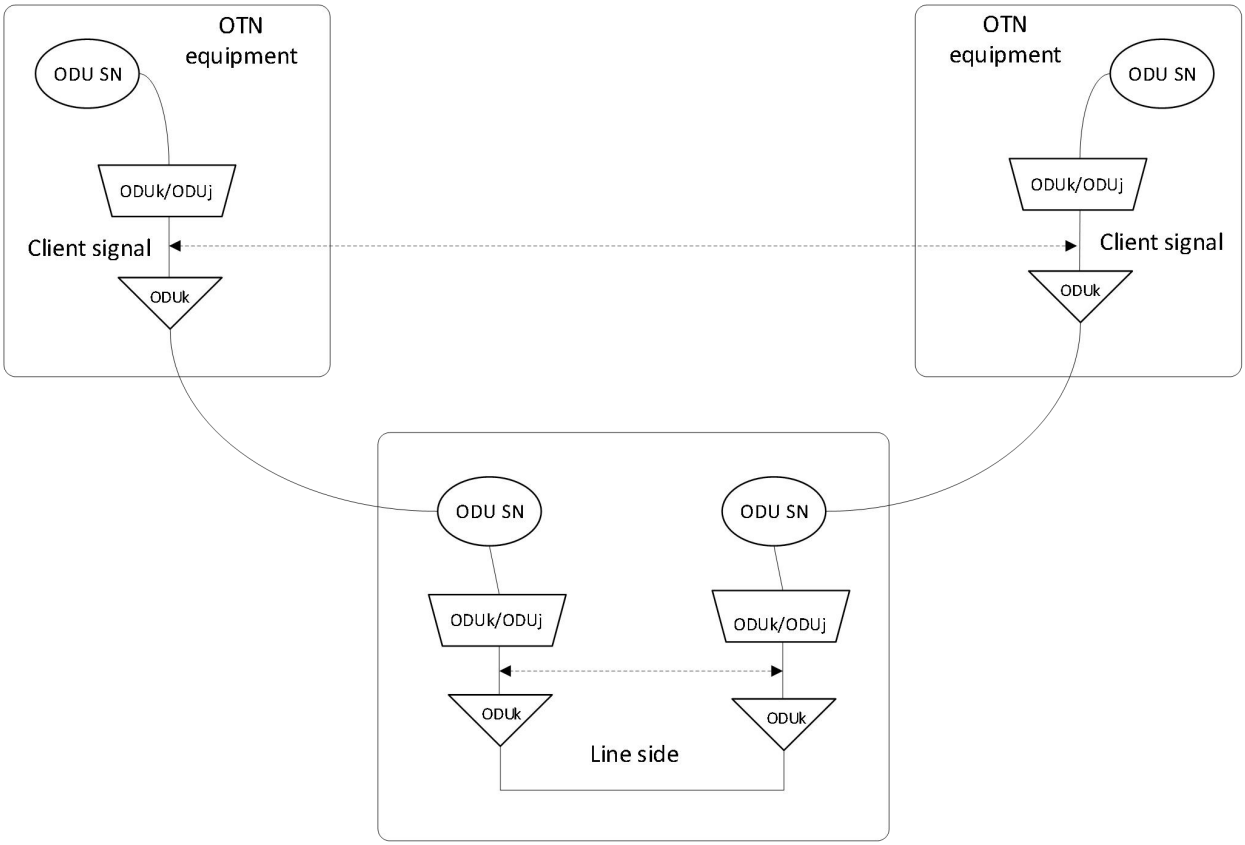



Figure6-20 Schematic Diagram of SM Overhead Configuration

The line side NE of the two ends is OTU2 service (configured according to the service type of the client side). Enable the monitoring function of SM overhead on the OTU2 layer at both ends, and then set the values of sending TTI and expected TTI. For detailed configuration, please see the detailed steps described in 6.2.1. If the values of sending TTI and receiving TTI at both ends conform to the overhead establishment rules listed in Table 6-1, then the line Configuration is correct and the service can be received and dispatched normally.

According to the PM overhead configuration rules described in 6.2.2, the PM overhead is planned as follows:

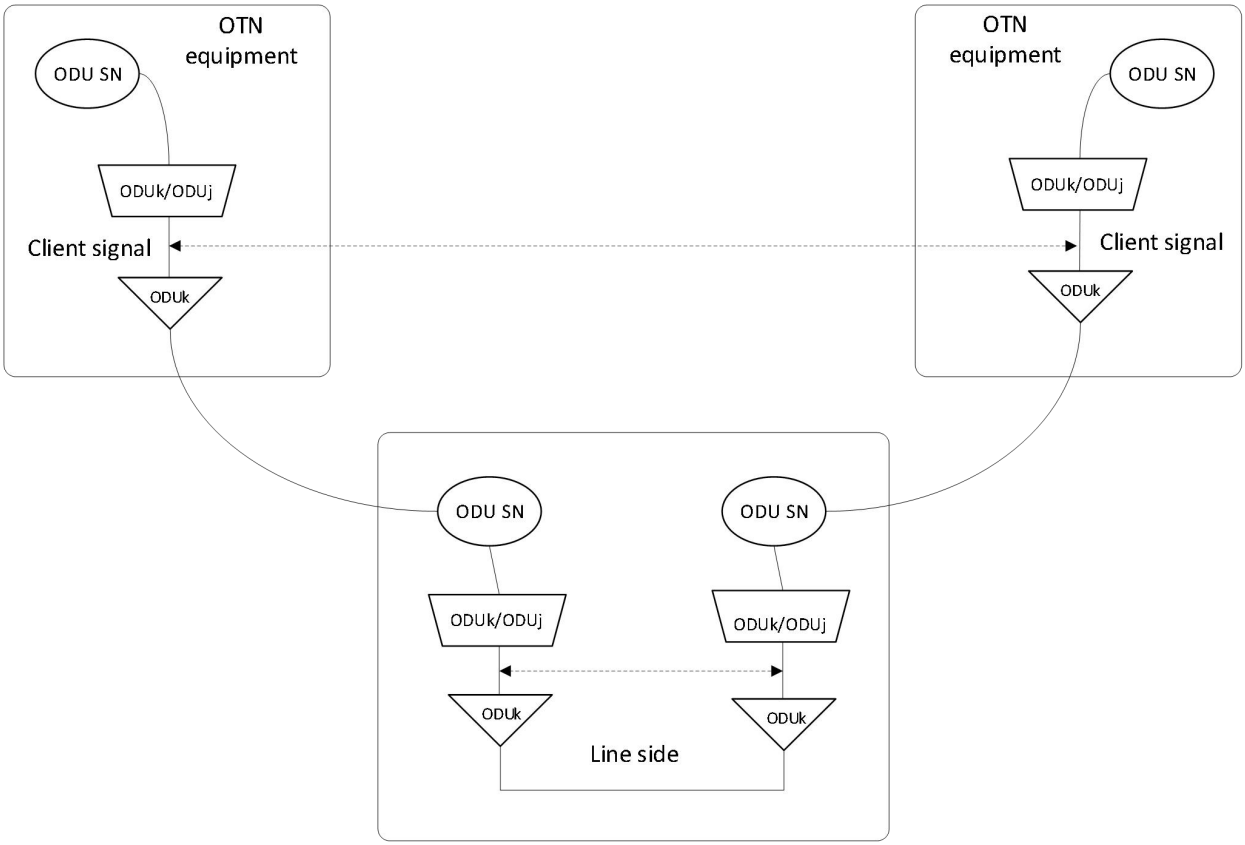



Figure6-21 Schematic Diagram of PM Overhead Configuration

The line side of the NE at the two ends is OTU2 service (configured according to the service type of the client side). After being demultiplexed to ODU2, enable the monitoring function of PM overhead on ODU2 layer at the two ends. Here the status of ODU2 layer is “unterminated”, the value of expected TTI can be set. For detailed configuration, please see detailed steps described in 6.1.3. If the values of expected TTI and receiving TTI of the two ends are the same, then the line configuration is correct and the signal source is correct.

The client side of NE at both ends is XGE_GFPF service (Specific service needs to be configured according to actual demand). Enable the monitoring function of PM overhead of client side port at both ends on ODU2 layer. Here the status of ODU2 layer is “client end signal terminated”. Set the values of sending TTI and expected TTI. For detailed configuration, please see the detailed steps described in 6.1.3. If the values of the sending TTI and receiving TTI of the two ends conform to the overhead establishment rules in Table 6-1, then the line configuration is correct and the service can be normally sent and received.

After the configuration is completed, when fault occurs to the service of the monitoring segment corresponding to SM and PM, the NMS system will report the alarm and performance instructions corresponding to SM and PM, such as TIM, BDI, AIS and SD etc. The fault can be quickly and accurately located according to these alarms and performances.

# 7. SNC Protection Configuration

## 7.1. Introduction of SNC Protection

SNC protection is also called subnet connection protection. Its function is when the signal on the client side fails in the working channel (signal failure, signal degradation), the service can automatically switch to the protection channel and continue to work normally.

The following figure shows the service environment of SNC protection. SNC protection service is configured for the devices at both ends. One is the working channel and the other is the protection channel. When the signal of the working channel is deteriorated or the signal is invalid, the protection channel is working normally at the same time. The service will switch automatically from the working channel to the protection channel. The switch time is less than 50ms, so the service interruption can not be perceived and the service can run normally.

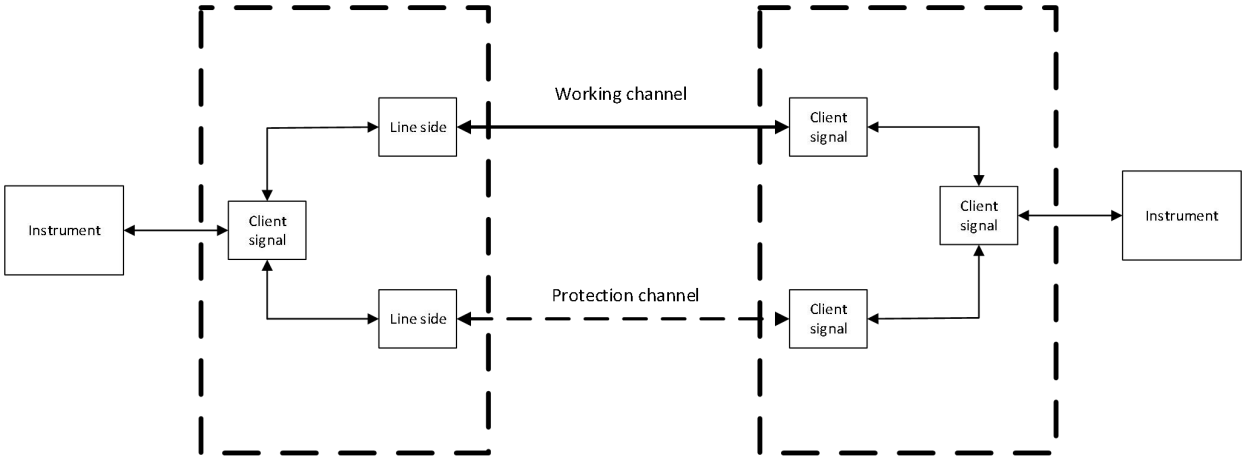



Figure7-1 Schematic Diagram of SNC Protection Service Environment

## 7.2. Configuration Steps

Configuration Prerequisite: After the normal start-up of the equipment board, arrange the optical module and optical fiber, connect the instrument and build the service environment.

Table7-1 SNC Configuration Process

| Stage | Configuration Method |
|---|---|
| Configure Service Type | Select client side service and line side type |
| | Enable client side port |
| | Enable line side port |
| | Line side signal is demultiplexed to low order ODU layer so as to match line side rate and client side rate. |
| Configure Service Cross-Connection with Protection | Select SNC cross-connection type—bidirectional with protection or unidirectional with protection |
| | Select the service capacity, that is, the corresponding ODU time slot. |
| | Select SNC protection mode—Site A protection or Site Z protection. |

| | |
|---|---|
| | Create SNC cross-connection with protection. |
| | Select SNC protection type--SNC/I or SNC/N. |
| Reply Wait Settings | Set reply mode—Reply Mode or Non-reply Mode.<br>If it is set as “non-reply mode”, it indicates that after the service is reversed to the secondary channel, even if the primary channel recovers to normal, the service will still work on the secondary channel until failure occurs to the secondary channel.<br>If it is set as “reply mode”, it needs to simultaneously set the reply waiting time. It indicates that after the service is reversed to the secondary channel, if the primary channel recovers to normal, the service will immediately return to the primary channel or recover to the primary channel after the reply waiting time.<br>The settings for the two ends of the protection equipment should keep consistent. |
| Protection Switching Command Settings | Manually select the issuing external command. |
| Delete Protection Settings | Manually delete the protection channel/working channel. |

## 7.3. Configuration Example

The SNC service types supported by various Shelf and boards are listed in the following table.

Table7-2 Supported SNC Service Type Table

| Shelf Type | Board Type | Supported SNC Service Type |
|---|---|---|
| M6500-CH5U | M6500_MXP10 | 10G service board SNC protection<br>10G service cross board SNC protection |
| | M6500-100G-TMXP2 | 100G service cross board SNC protection |
| | M6500-40G-TMXP2 | 40G service cross board SNC protection |
| M6500-CH2U | M6500_MXP10 | 10G service board SNC protection<br>10G service cross board SNC protection |
| | M6500-100G-TMXP2 | 100G service cross board SNC protection |

The demultiplexing capacity corresponding to the service type is shown in the following table:

Table7-3 TP Multiplexing Capacity Table of SNC Service

| Service Rate | Service Type | Capacity Type |
|---|---|---|
| 1.25G Service | GE_TTT | ODU0 |
| | FE_CBR | |
| | STM1_GMP/OC3_GMP | |
| | STM4_GMP/OC12_GMP | |
| 2.5G Service | STM16_AMP/OC48_AMP | ODU1 |

| | | |
|---|---|---|
| | STM16_BMP/OC48_BMP | |
| 10G Service | XGE_BMP | ODU2e |
| | XGE_GFPF | ODU2 |
| | XGE_GFPFextp | |
| | STM64_AMP/OC48_AMP | |
| | STM64_BMP/OC48_BMP | |
| | OTU2 | |
| | OTU2e | ODU2e |
| 40G Service | FGE_GMP | ODU3 |
| | OTU3 | |
| 100G Service | HGE_GMP | ODU4 |
| | HGE_GFPF | |
| | OTU4 | |

Here we take the 10G service cross board protection of M6500-MXP10 board as an example to introduce the configuration process of SNC services.

1. Insert a M6500-MXP10 board in M6500 and open the NMS interface to add the NE after the normal start-up of the board.

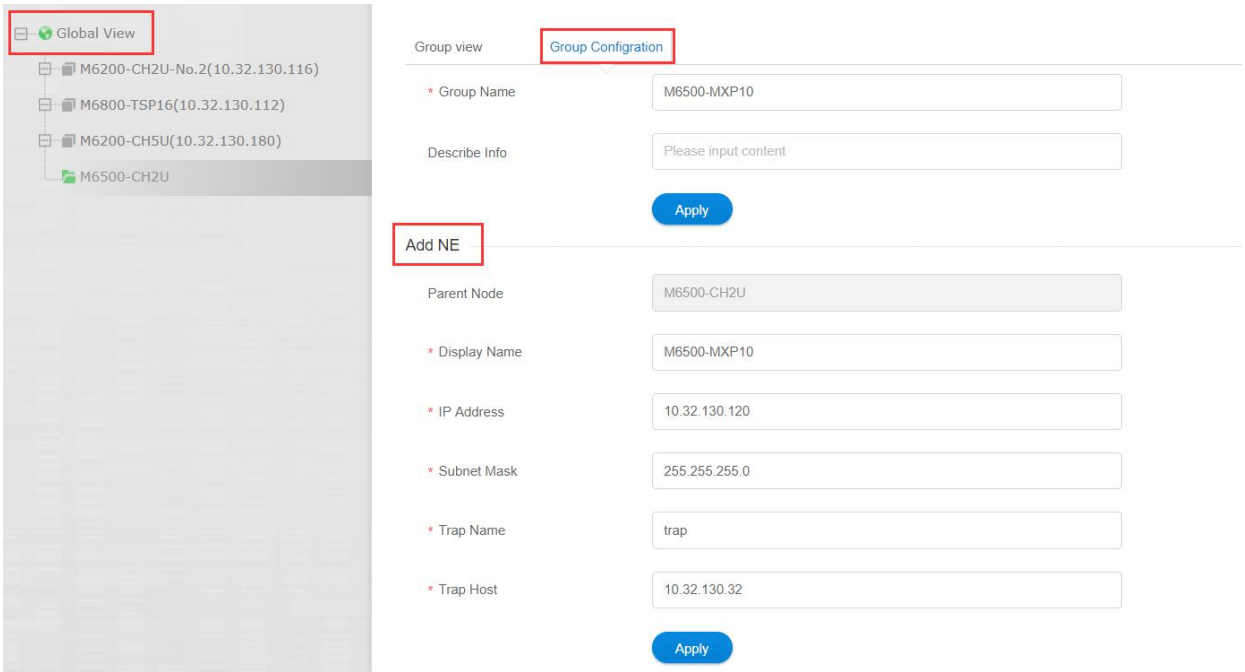



Figure7-2 Add NE

Select a client side port (Port 1-10), (here we take Port 1 of Slot 1 as the client side signal port), then click on the port and select "*Port Management*"on the right.

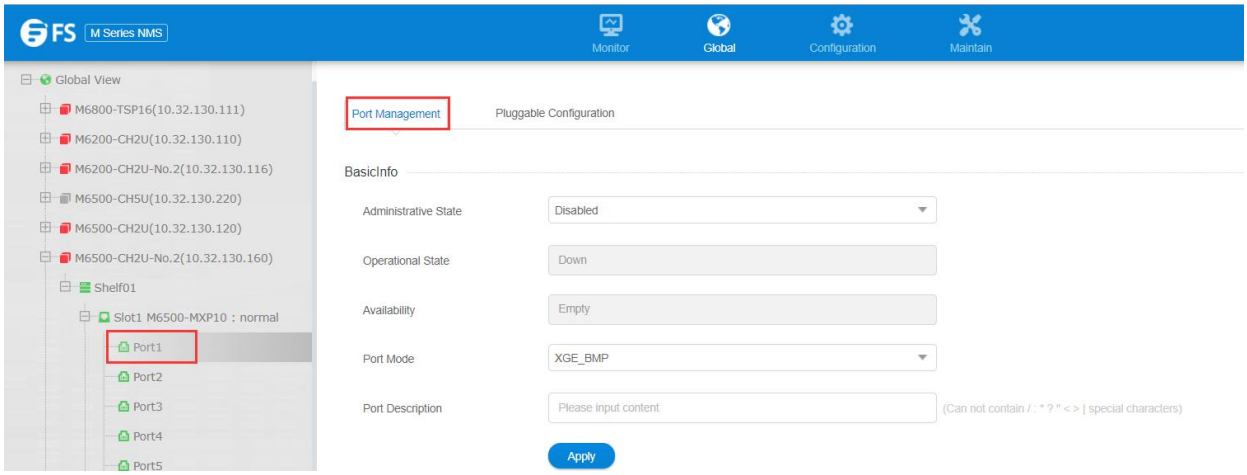



Figure7-3 Select Client Side Port

Select the service type you need and enable the port, then click on "*Apply*".

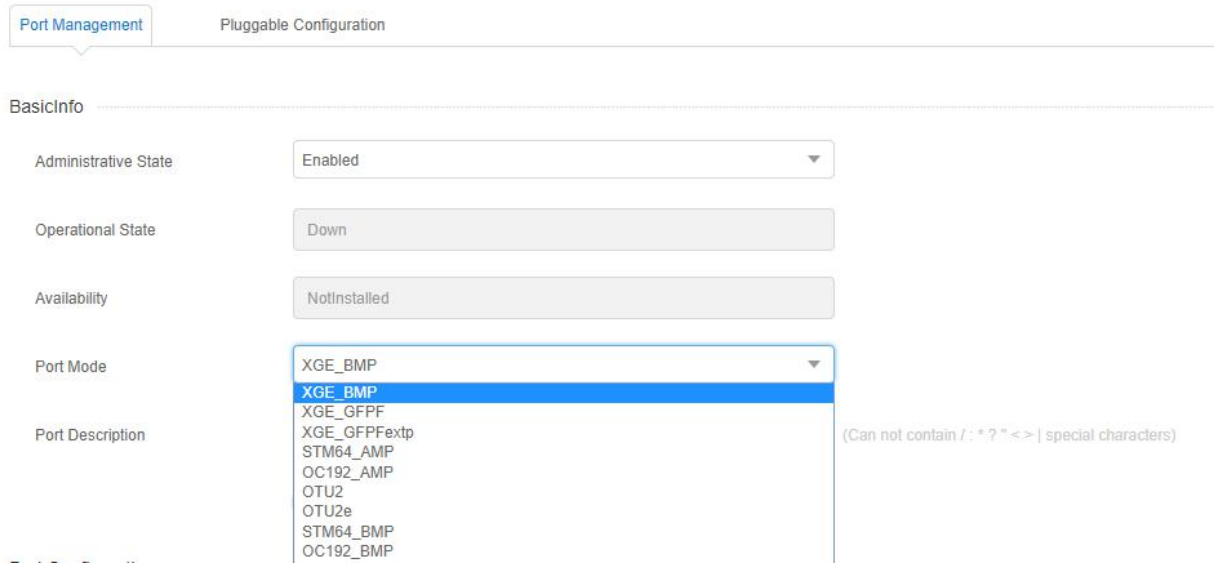



Figure7-4 Configure Client Side Service

2. Here we take Port 11 of Slot 1 and Port 11 of pair Slot 17 as the line side port.Click on the port and select"*Port Management*"on the right. Then select the needed service type according to the optical module type of the line side, enable the port and click on"*Apply*".

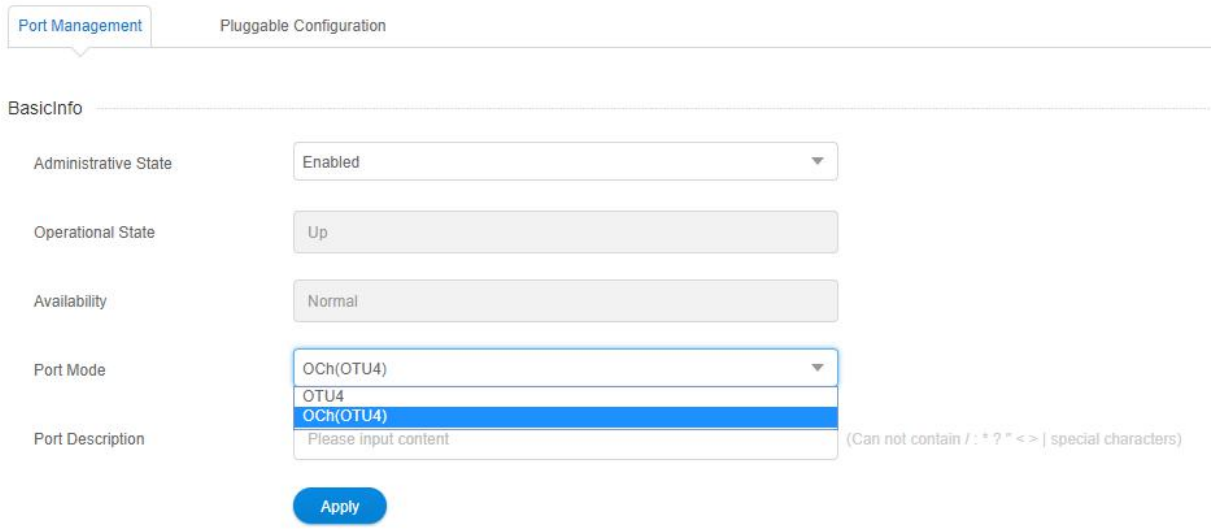



Figure7-5 Configure Line Side Service

3. Click on the service board and select"*TP Multiplexing Structure*".

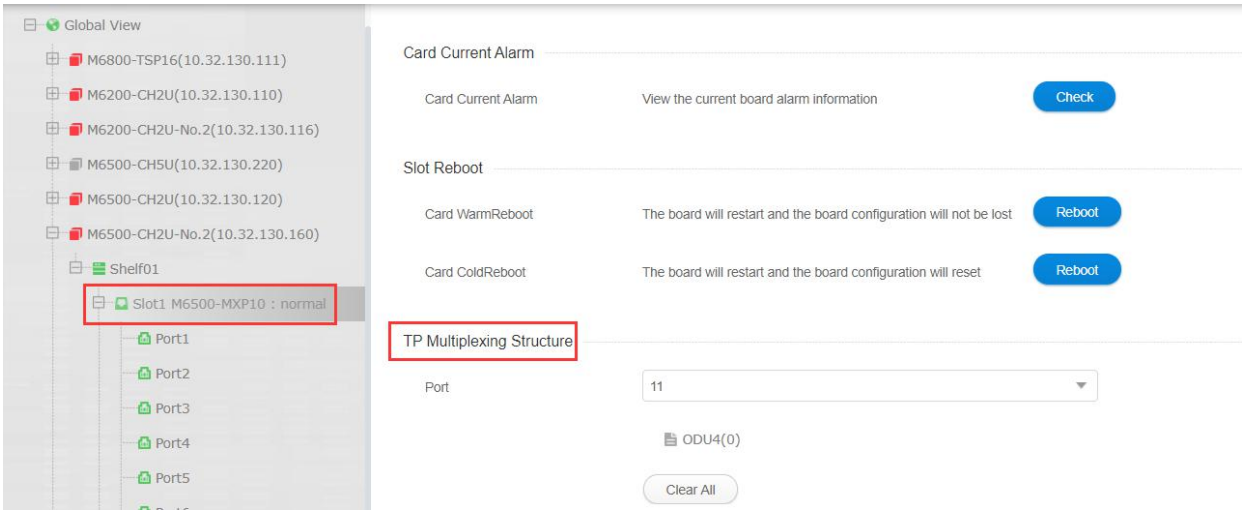



Figure7-6 TP Multiplexing Structure

Select the appropriate time slot to demultiplex to the low order ODU layer, so as to make the line side rate and the client side rate match.

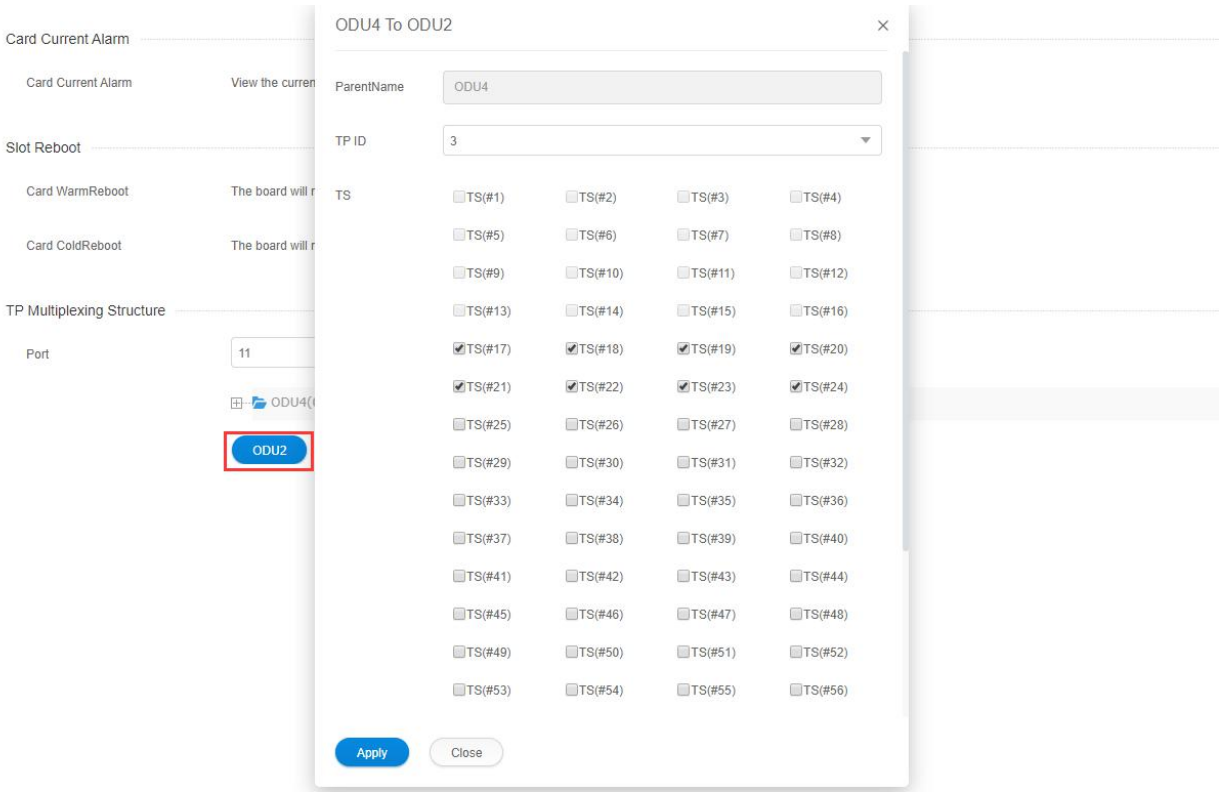



Figure7-7 Select Time Slot Demultiplexing

4. Select SNC cross-connection type--"*bidirectional with protection*"or"*unidirectional with protection*".

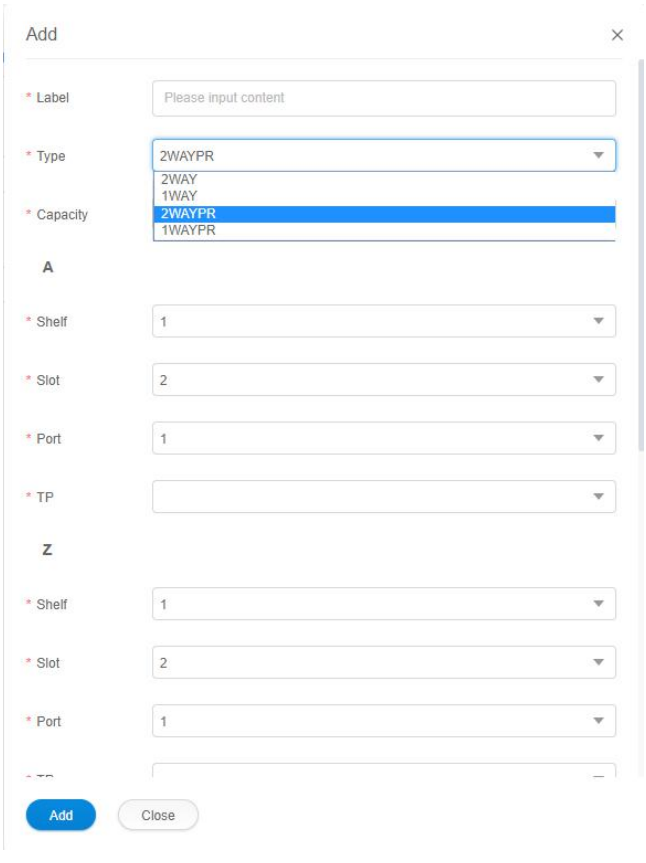


Figure7-8 Select Cross-Connection Type

5. Select the service capacity, that is, the corresponding ODU time slot.

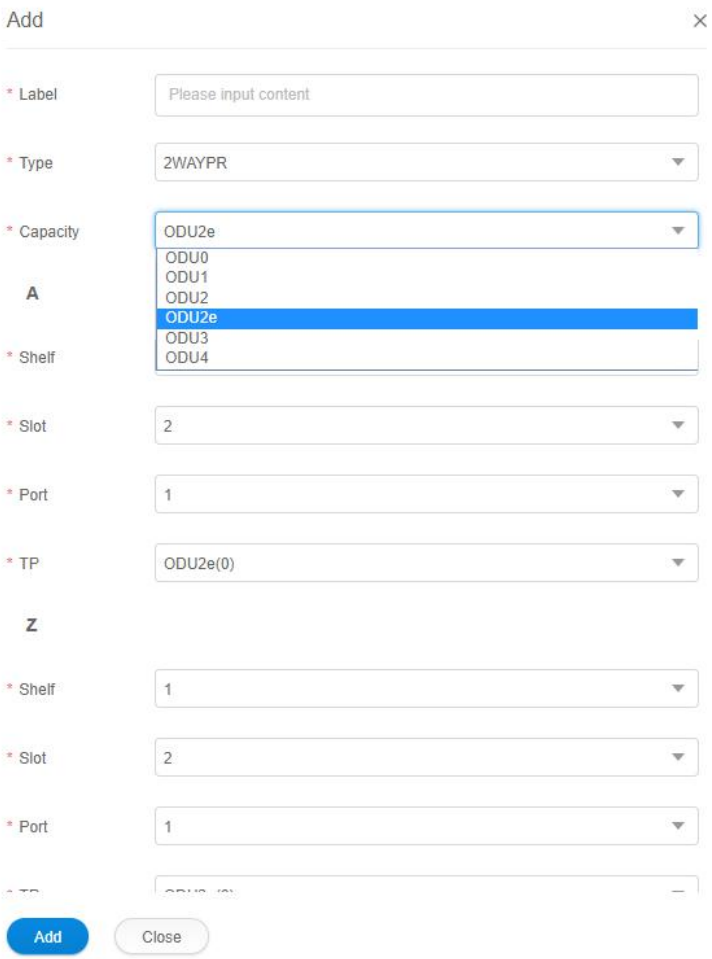



Figure7-9 Select Service Capacity

6. Select SNC protection mode—Site A protection or Site Z protection.

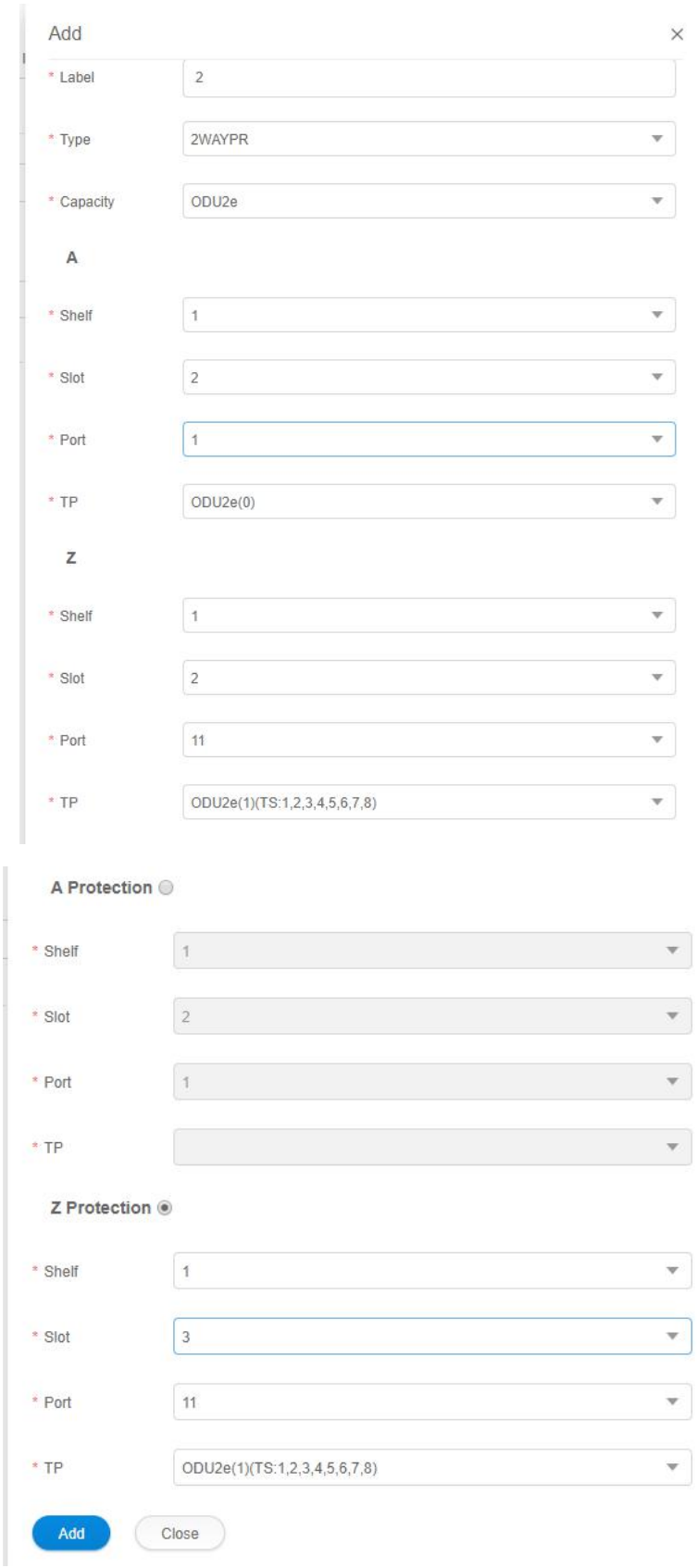



Figure7-10 Select Protection Mode

7. Select client side port number and line side port number. The tag name can be empty. Create the cross-connection of SNC protection service, then click on"*PPG*"option of the created SNC cross-connection with protection.

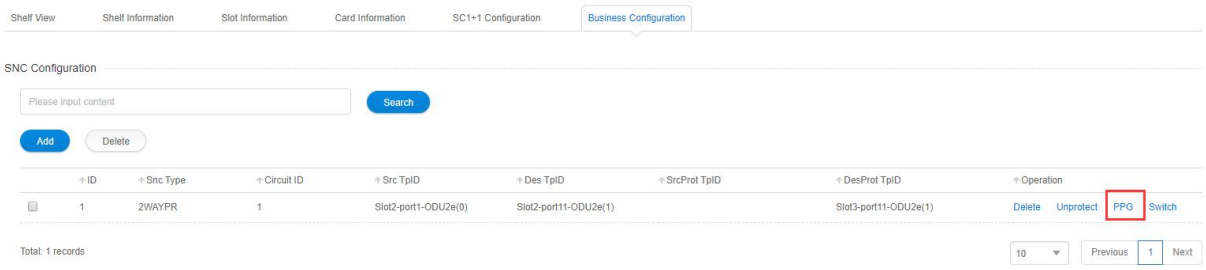



Figure7-11 Click Protection Group

Select the protection type--"*SNC/I*"or"*SNC/N*".

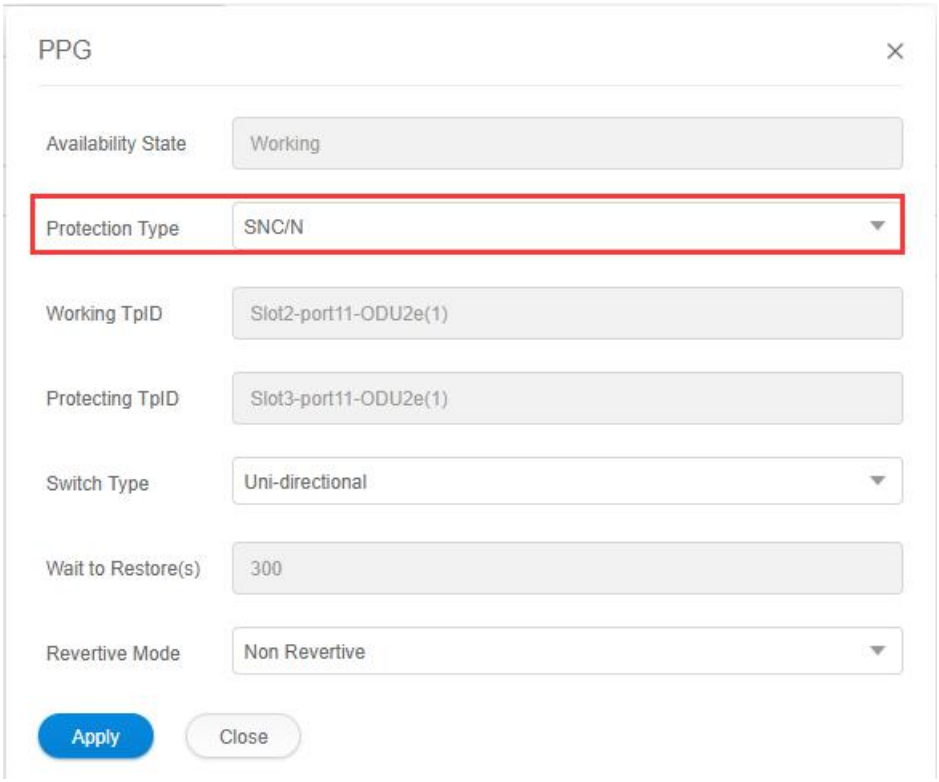



Figure7-12 Select Protection Type

8. Reply wait settings—select"*Revertive*"or"*Non Revertive*". If"*Revertive*"mode is selected, the reply waiting time needs to be entered.

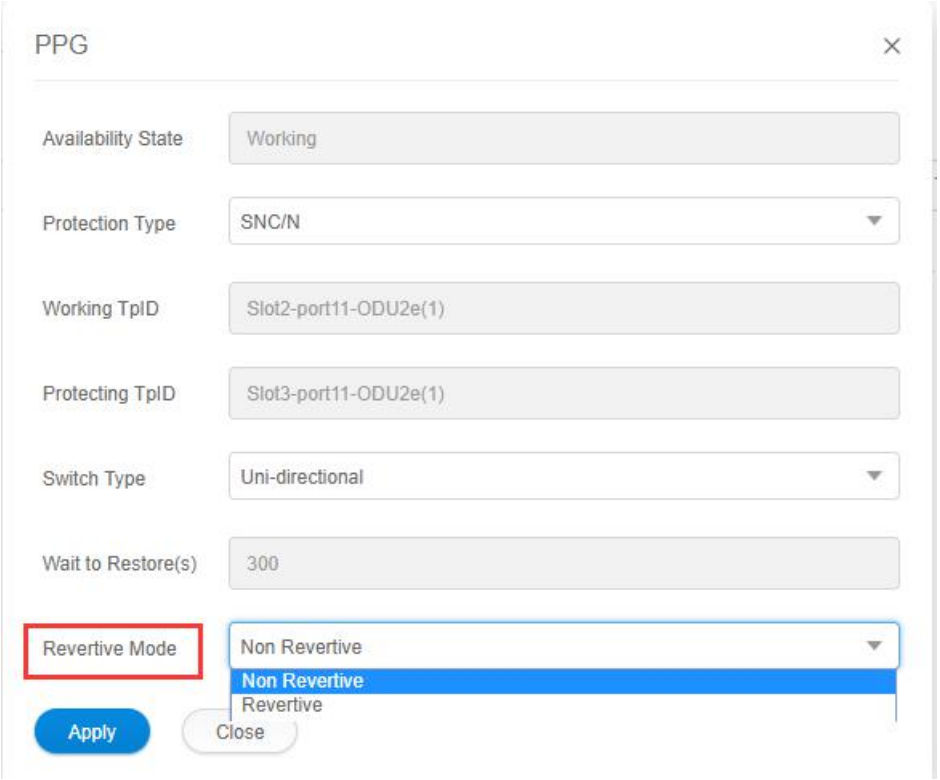



Figure7-13 Reply Wait Settings

9. Click on"*Switch*"option of the created SNC protection cross-connection.

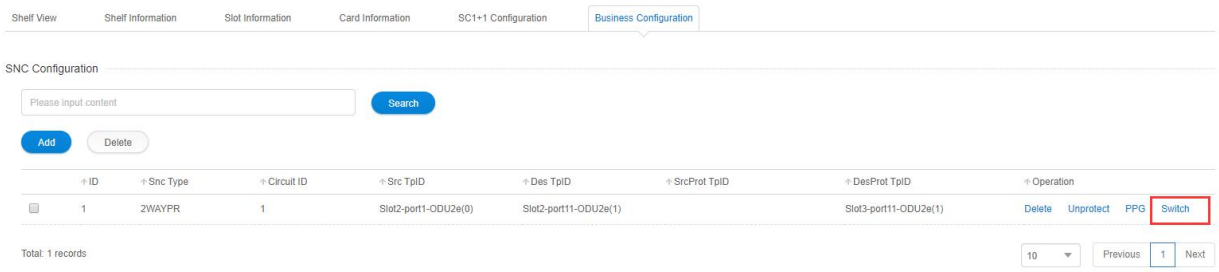



Figure7-14 Protection Switching Settings

Manually select to issue protection switching command. The command priority is clear>lock protection switching>force switch to working channel>force switch to protection channel>manually switch to working channel>manually switch to protection channel>practice.

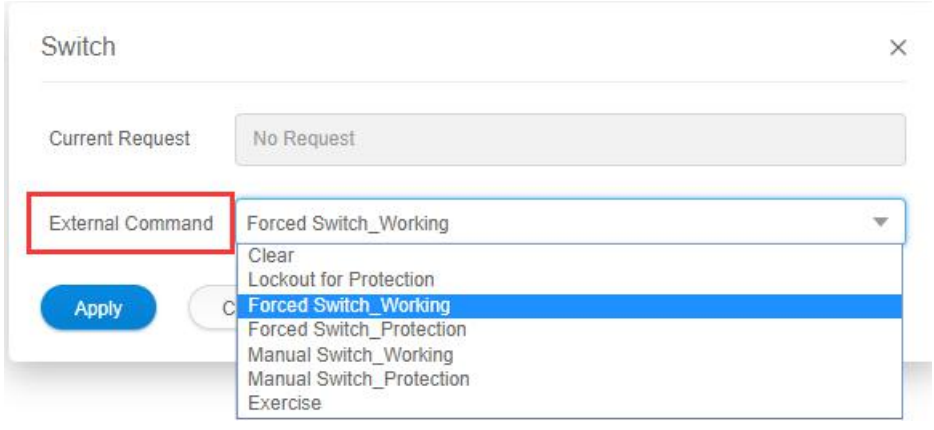


Figure7-15 Select Protection Switching Command

10. Click on"*Unprotect*"option of the created SNC protection cross-connection.

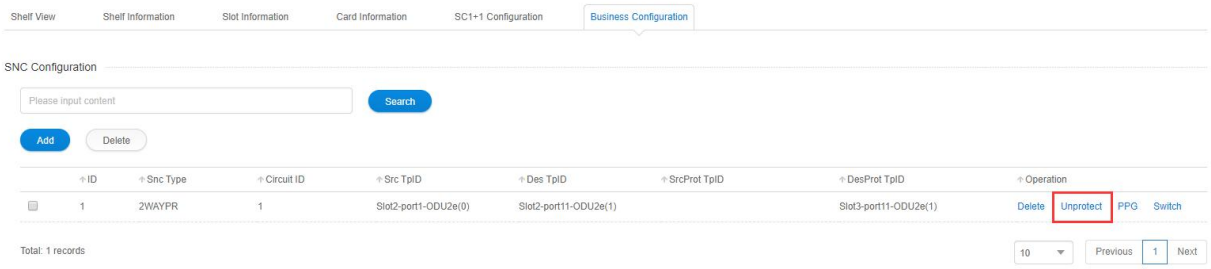



Figure8-16 Delete Protection

You can manually select to delete the working channel or the protection channel.


Figure7-17 Delete Working Channel or Protection Channel

# 8. Alarm Management

## 8.1. Alarm Management Introduction

The alarm management function is a functional group that manages the faults of various network devices managed by the NMS system during the operation of the system. The managed fault is commonly called alarm.

The NMS alarm management function manages two types and four levels of failures. The two types are equipment alarm and communication alarm. The four levels are emergency, primary, secondary and warning.

## 8.2. Main Interface of Alarm Management

After logging in the NMS system, click on "*Maintain*" on the navigation bar – left click on the "*Alarm Management*" menu -- the alarm management sub-menu appears, which includes: current alarm, history alarm, alarm configuration, alarm notification configuration, alarm mailbox server configuration and enable sound.

**Hint**

**In the upper right corner of the NMS main interface, alarm statistics are displayed, including the total number of alarms and the number of alarms at all levels.**

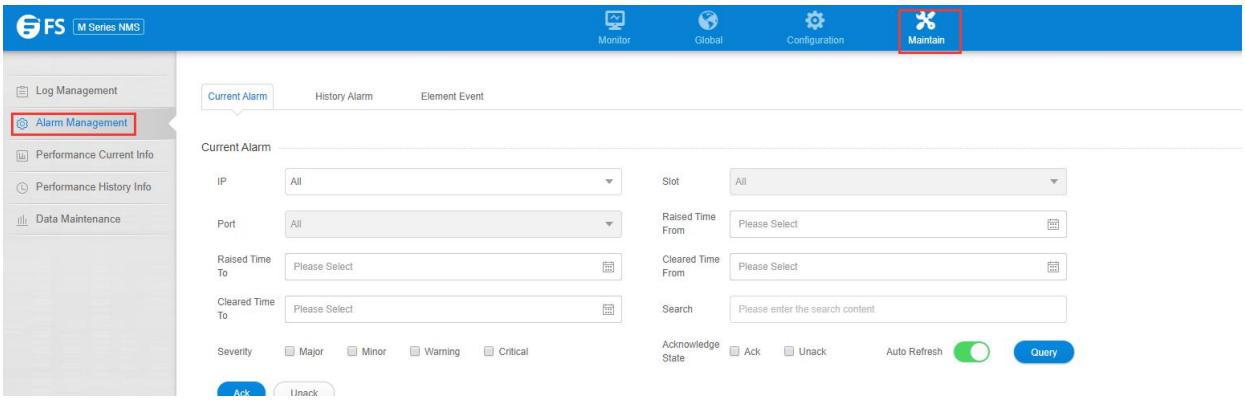



Figure8-1 Alarm Management

### 8.2.1. Current Alarm

Click on"*Current Alarm*"in the sub-menu to enter the current alarm page, as shown in the figure below:

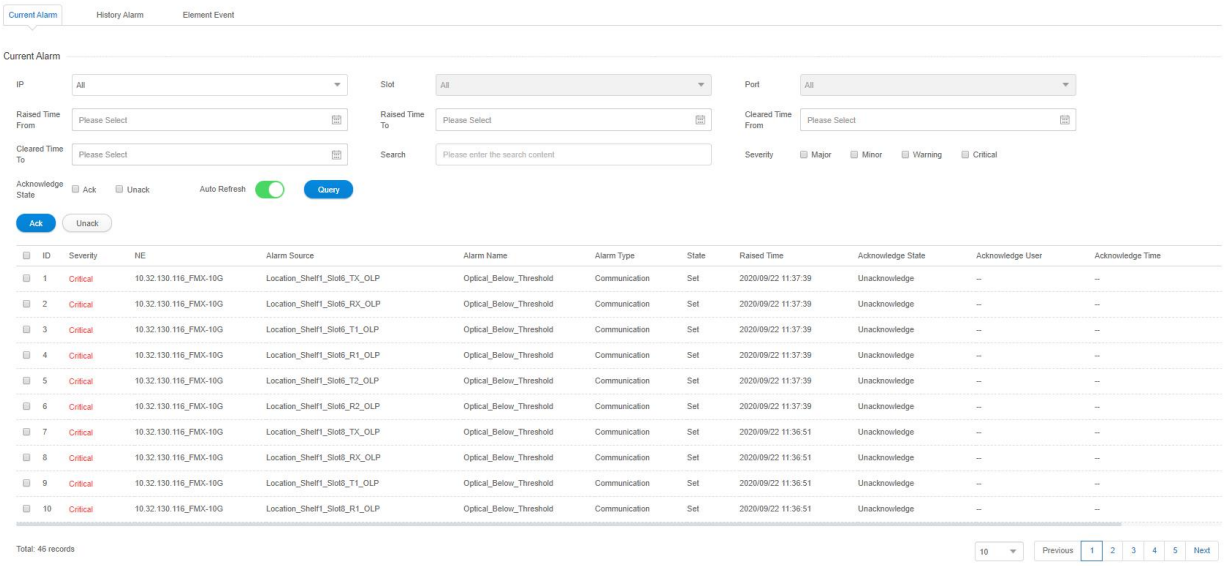



Figure8-2 Current Alarm

The lower right corner of the alarm interface can filter the number of alarms displayed on the current page, and the number of displayed alarms per page can be adjusted to 10, 20, 50 and 100 (as shown below).


Figure8-3 Show Number of Current Alarms

The upper part of the alarm interface is the "*Query*" part and the "*Auto Refresh*" button , the area under the "*Query*" section is the "*Ack*", "*Unack*". The functions of these buttons are:

- The function of"*Ack*"button is to confirm the selected alarm. By ticking the check box on the left of the alarm to be confirmed and clicking the "*Ack*" button, the selected alarms are all in the confirmation state. The confirmation status of the confirmed alarm is "confirmed" and the "confirmation" icon becomes green with specific confirmation person and confirmation time. The specific operation is: select the alarm to be confirmed→click the "*Ack*" button→click on"*apply*"→confirm the alarm.

**Hint**

**Because the current page will refresh once in 10 seconds, the selected alarm will become unchecked after refreshing if it is not confirmed in time.**

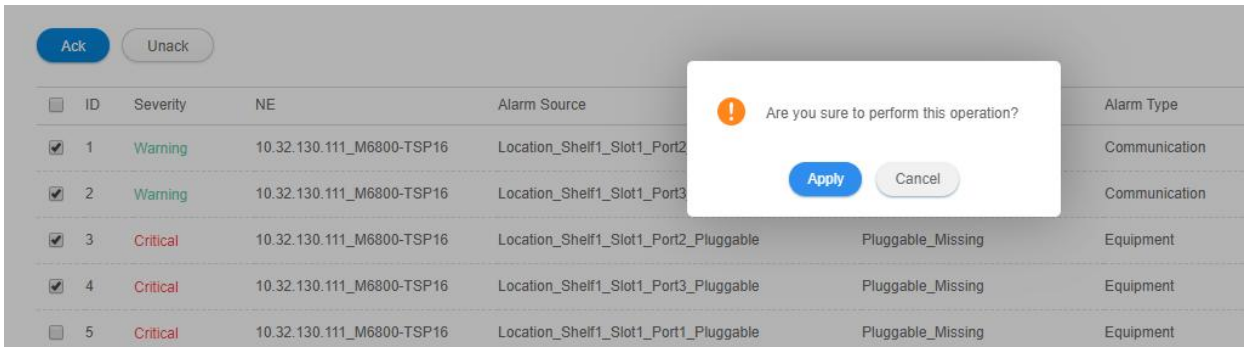



Figure8-4 Select to Confirm Current Alarm

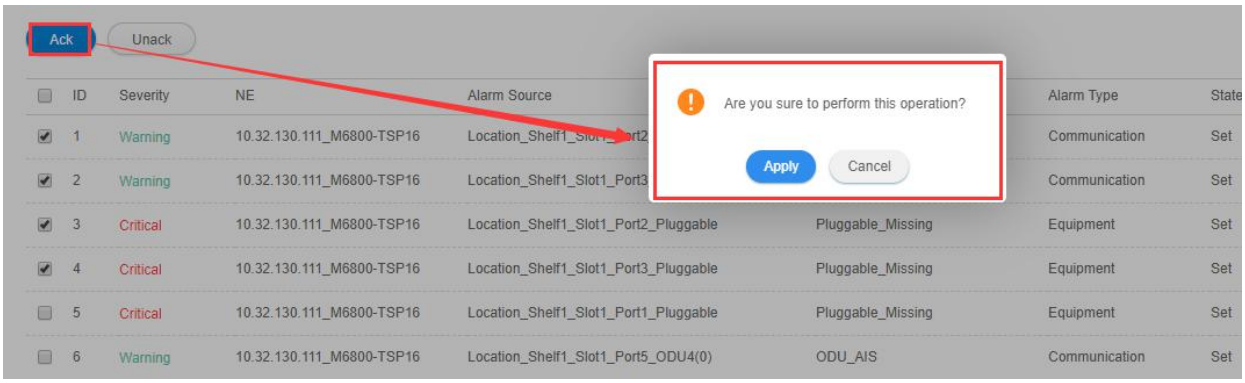



Figure8-5 Carry Out Confirmation of Current Alarm

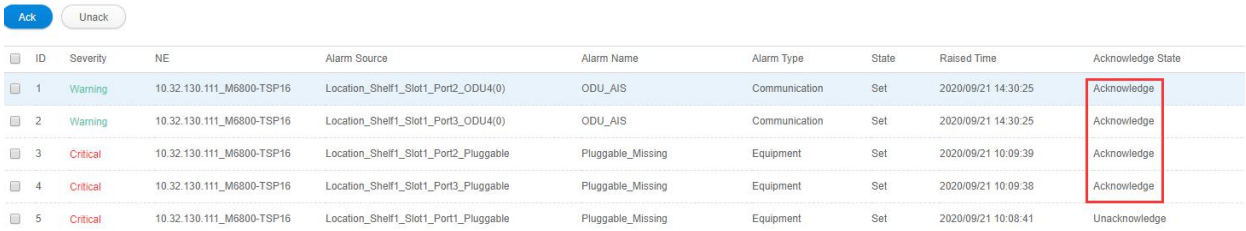


Figure8-6 Complete Confirmation of Current Alarm

- The function of"*Unack*" button is to cancel confirmed alarms and return them to unconfirmed state. The operation method is similar like that to confirm alarm: select the alarm to be canceled confirmation→click the "*Unack*"button→click on "*Apply*"→The alarm is not confirmed.

**Hint**

Because the current page will refresh once in 10 seconds, the selected alarm will become unchecked after refreshing if it is not confirmed in time.

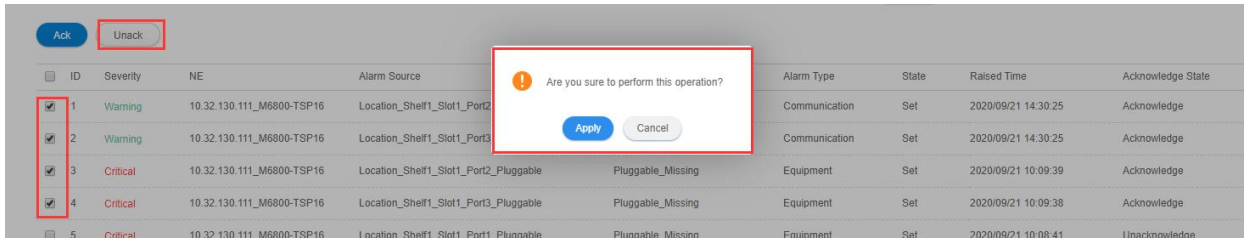



Figure9-7 Cancel Confirmation of Current Alarm

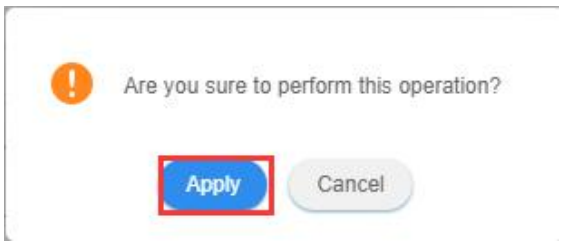



Figure8-8 Cancel Confirmation

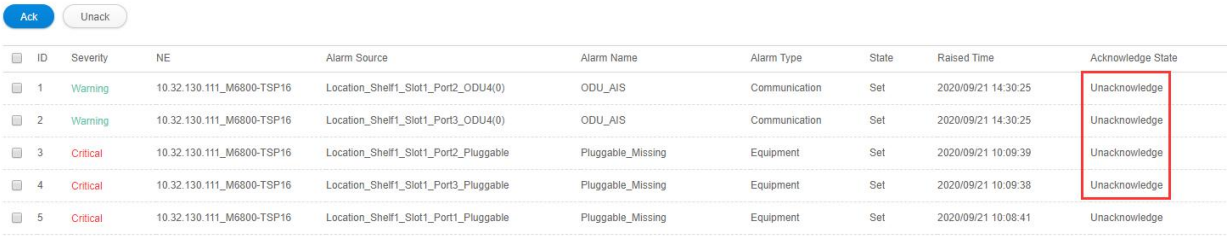



Figure8-9 Complete Confirmation Cancellation of Current Alarm

- The function of"*Query*"button is to use the known conditions to view and operate the specified alarm. The filter conditions include: NE IP, specified slot of specified IP, specified port of specified slot; alarm creation and termination time (i.e. alarm generation period), the beginning and ending time of alarm clearance; alarm level and alarm confirmation status.A single filter condition or a combination of several filter conditions can be used to filter out the alarms required, as shown in the figure below.

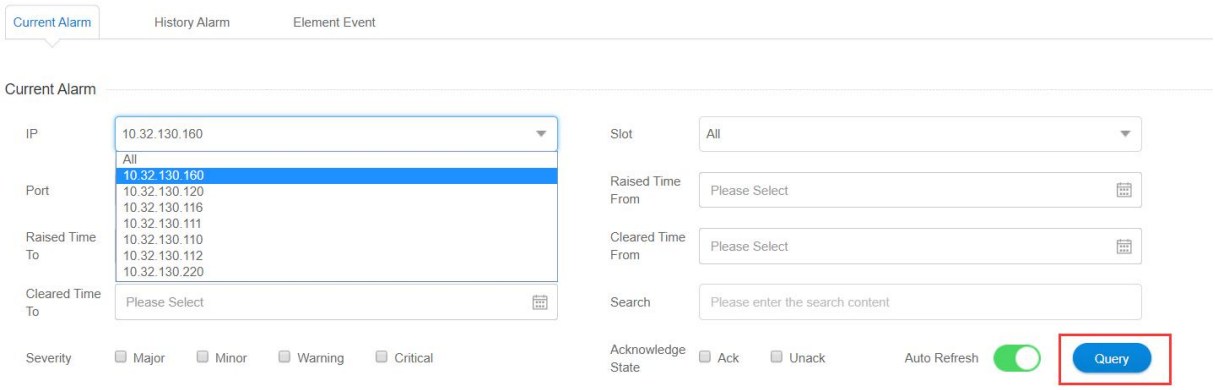



Figure8-10 IP Filter Current Alarm

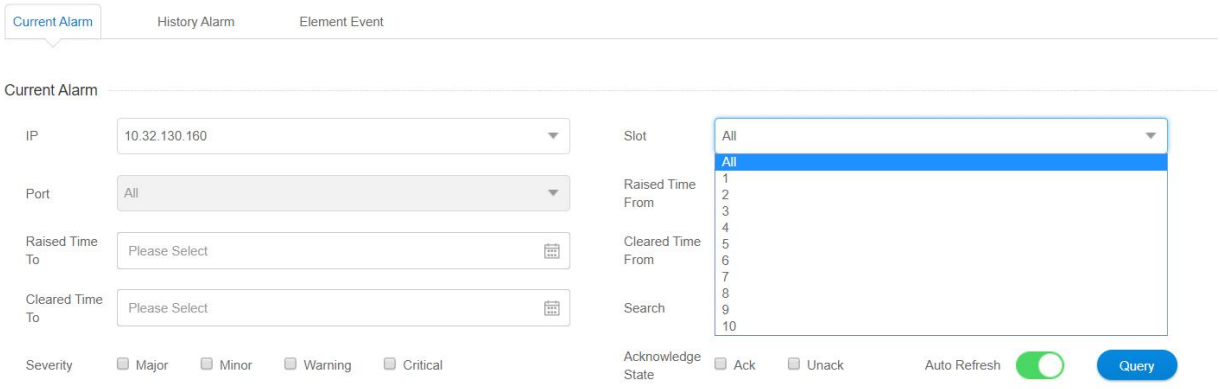



Figure8-11 Filter Current Alarm for Slots & Ports

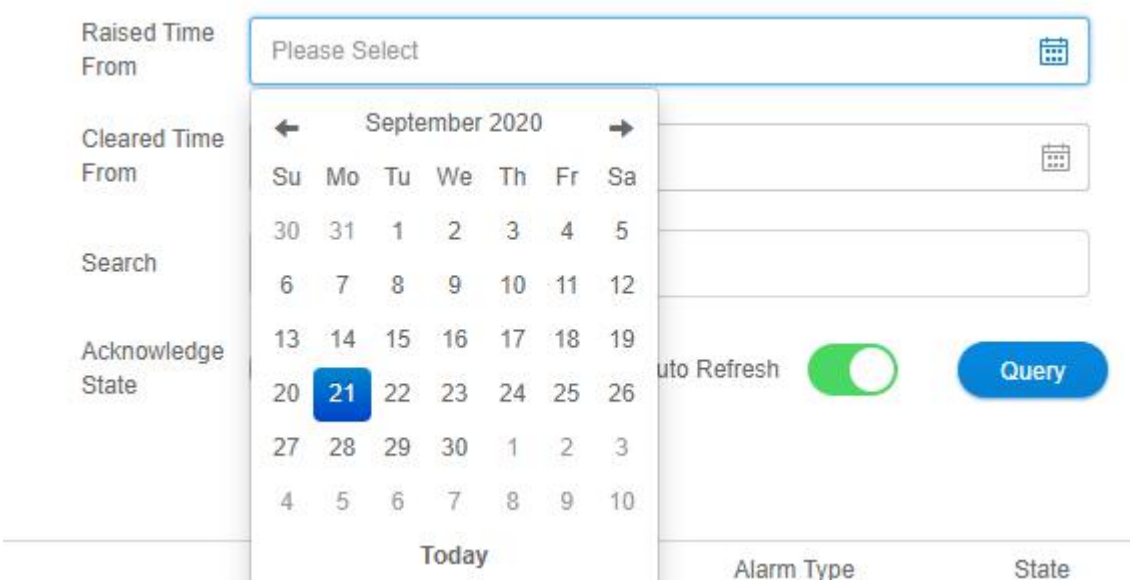



Figure8-12 Create Time to Filter Current Alarm


Figure8-12 Filter Current Alarm According to Alarm Level & Confirmation Status

**Hint**

**The method to filter IP, slot and port is: IP→Slot→Port or IP→Slot or IP. It is not allowed to select slot or port separately.**

- "*Auto Refresh*" button is a button which can move right and left (It can switch from refresh to close or from close to refresh by clicking the button.) The current page is refreshed every 10 seconds when it is in Refresh state and the current page is not refreshed when it is in Close state.

The middle right part of the alarm interface is the search area: By entering specified content, it can get all the alarms that contain that content, as shown in the following figure.

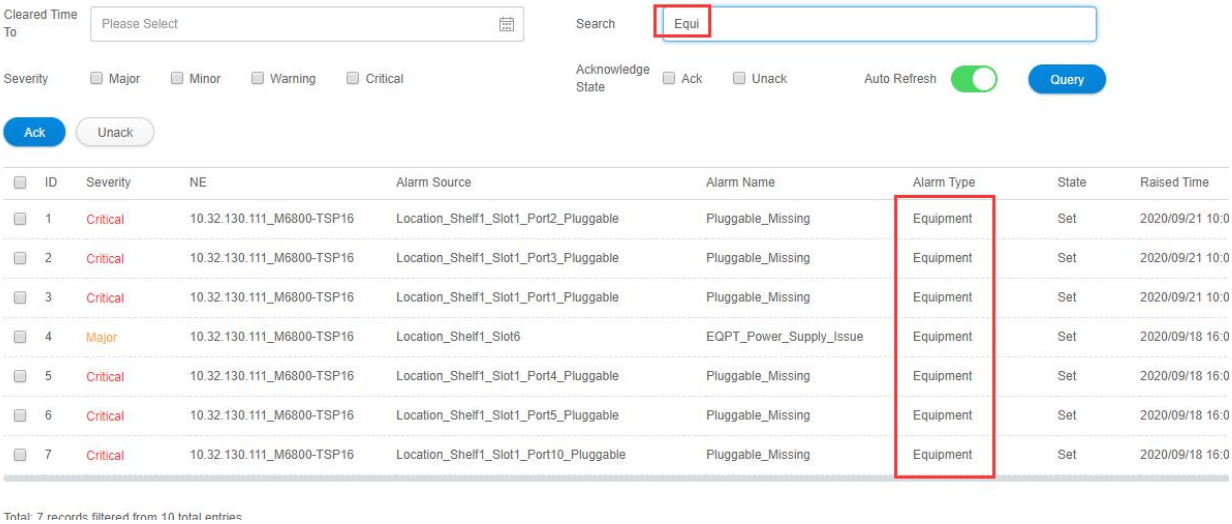



Figure8-13 Search Current Alarm

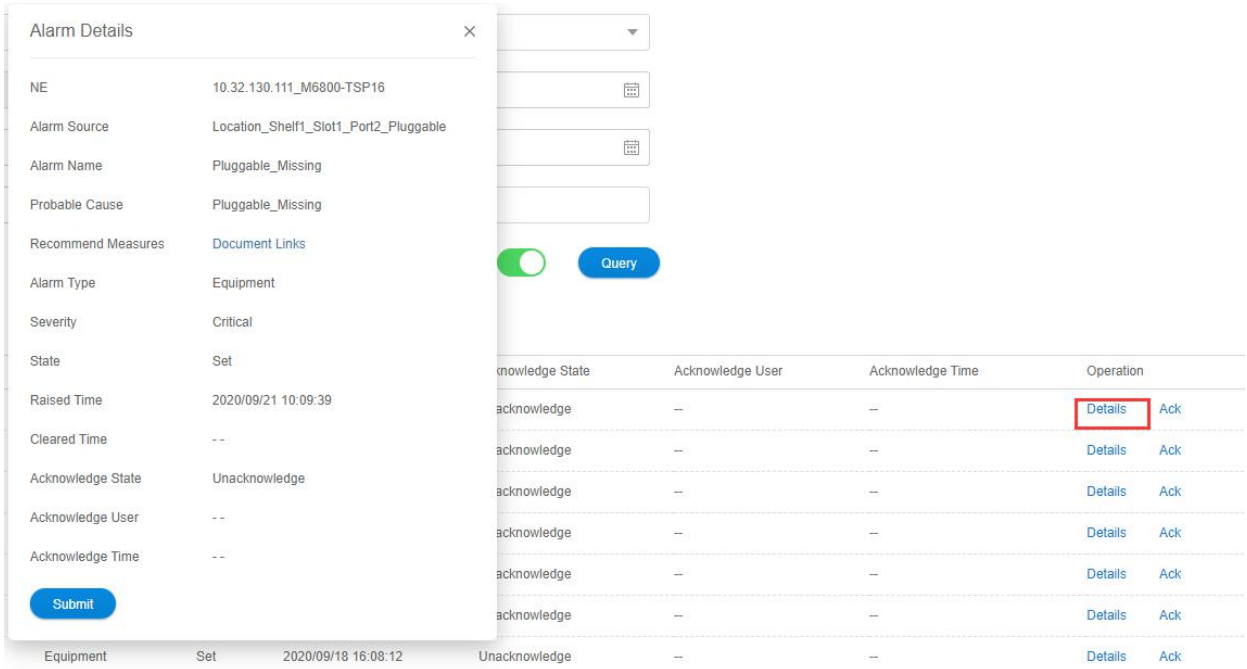



Figure8-14 Alarm Details

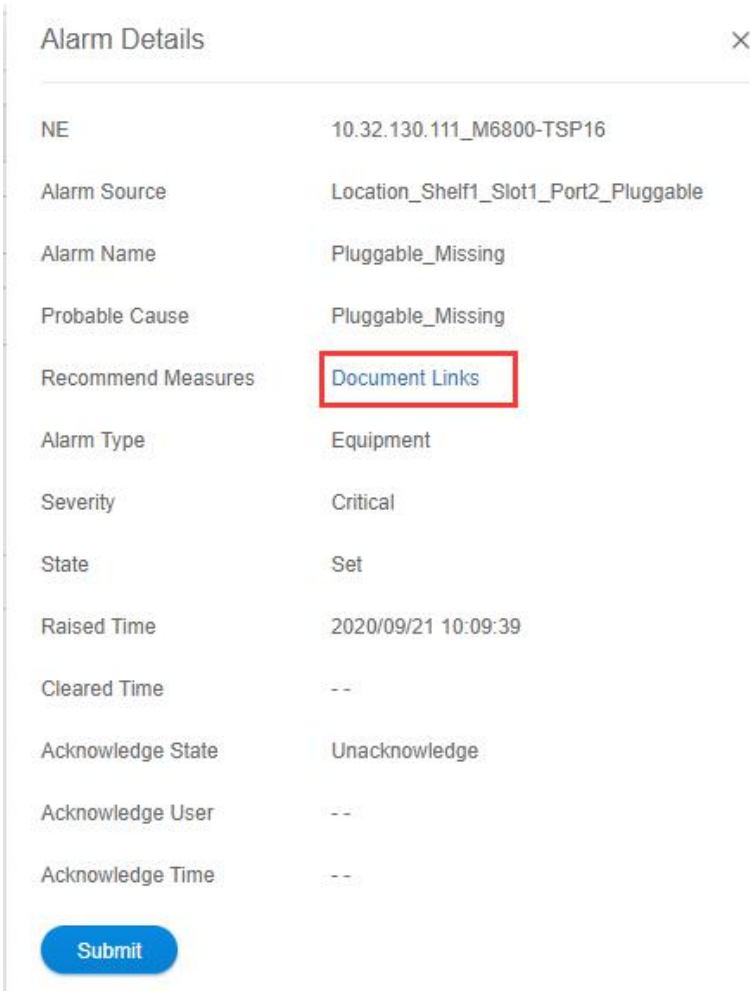


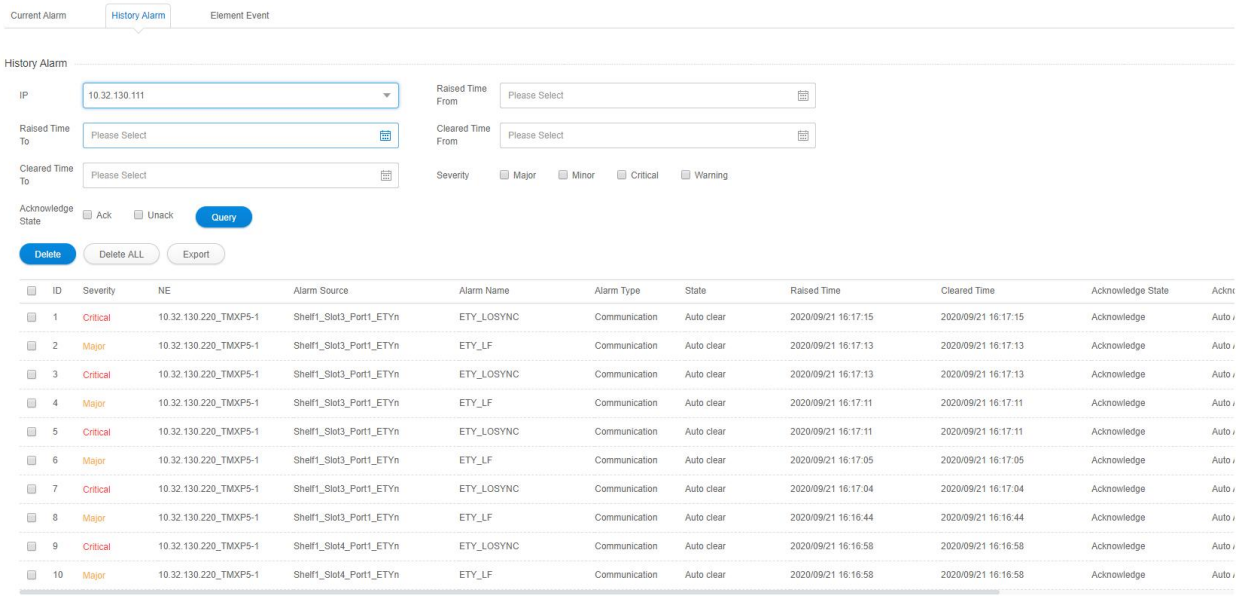

Figure8-15 Alarm Document Link

The lower middle area is the display section of the current alarm. From left to right in turn, the table header is: check box, serial number, alarm level, NE, alarm source, alarm name, alarm type, status, generation time, clearance time, confirmation status, confirmer and confirmation time, operation.

- Check box is used to check or cancel a specified alarm, or the first check box can be used to select all the alarms on the page.
- The serial number is the number of the alarms, sequentially increasing from 1.
- There are four alarm levels, marked by different colors: emergency level (red), main level (orange), secondary level (blue), warning level (cyan).
- Network element is the IP of network equipment that generates alarm.
- The alarm source is the specific slot or port information of NE which generates alarm.
- Alarm name, alarm type, status, generation time, clearance time, confirmation status, confirmer and confirmation time are relatively simple, we will not go into much detail here.

## 8.2.2. History Alarm

Click on "*History Alarm*"in the submenu to enter the history alarm page, as shown in the figure below:




| | ID | Severity | NE | Alarm Source | Alarm Name | Alarm Type | State | Raised Time | Cleared Time | Acknowledge State | Ackn |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | Critical | 10.32.130.220_TMXP5-1 | Shelf1_Slot3_Port1_ETYn | ETY_LOSYNC | Communication | Auto clear | 2020/09/21 16:17:15 | 2020/09/21 16:17:15 | Acknowledge | Auto |
| | 2 | Major | 10.32.130.220_TMXP5-1 | Shelf1_Slot3_Port1_ETYn | ETY_LF | Communication | Auto clear | 2020/09/21 16:17:13 | 2020/09/21 16:17:13 | Acknowledge | Auto |
| | 3 | Critical | 10.32.130.220_TMXP5-1 | Shelf1_Slot3_Port1_ETYn | ETY_LOSYNC | Communication | Auto clear | 2020/09/21 16:17:13 | 2020/09/21 16:17:13 | Acknowledge | Auto |
| | 4 | Major | 10.32.130.220_TMXP5-1 | Shelf1_Slot3_Port1_ETYn | ETY_LF | Communication | Auto clear | 2020/09/21 16:17:11 | 2020/09/21 16:17:11 | Acknowledge | Auto |
| | 5 | Critical | 10.32.130.220_TMXP5-1 | Shelf1_Slot3_Port1_ETYn | ETY_LOSYNC | Communication | Auto clear | 2020/09/21 16:17:11 | 2020/09/21 16:17:11 | Acknowledge | Auto |
| | 6 | Major | 10.32.130.220_TMXP5-1 | Shelf1_Slot3_Port1_ETYn | ETY_LF | Communication | Auto clear | 2020/09/21 16:17:05 | 2020/09/21 16:17:05 | Acknowledge | Auto |
| | 7 | Critical | 10.32.130.220_TMXP5-1 | Shelf1_Slot3_Port1_ETYn | ETY_LOSYNC | Communication | Auto clear | 2020/09/21 16:17:04 | 2020/09/21 16:17:04 | Acknowledge | Auto |
| | 8 | Major | 10.32.130.220_TMXP5-1 | Shelf1_Slot3_Port1_ETYn | ETY_LF | Communication | Auto clear | 2020/09/21 16:16:44 | 2020/09/21 16:16:44 | Acknowledge | Auto |
| | 9 | Critical | 10.32.130.220_TMXP5-1 | Shelf1_Slot4_Port1_ETYn | ETY_LOSYNC | Communication | Auto clear | 2020/09/21 16:16:58 | 2020/09/21 16:16:58 | Acknowledge | Auto |
| | 10 | Major | 10.32.130.220_TMXP5-1 | Shelf1_Slot4_Port1_ETYn | ETY_LF | Communication | Auto clear | 2020/09/21 16:16:58 | 2020/09/21 16:16:58 | Acknowledge | Auto |

Figure8-16 History Alarm

The lower right corner of the history alarm interface can filter the number of alarms displayed on the current page, and the number of displayed alarms per page can be adjusted to 10, 20, 50 and 100.

The Filter, All, Delete, Delete All, Export buttons are shown in the right area of the navigation bar.

- Functions of"*Query*"buttons are the same as the functions of those buttons in the current alarm.
- The function of"*Delete*"button is to delete the selected history alarm, as shown in the following figure.

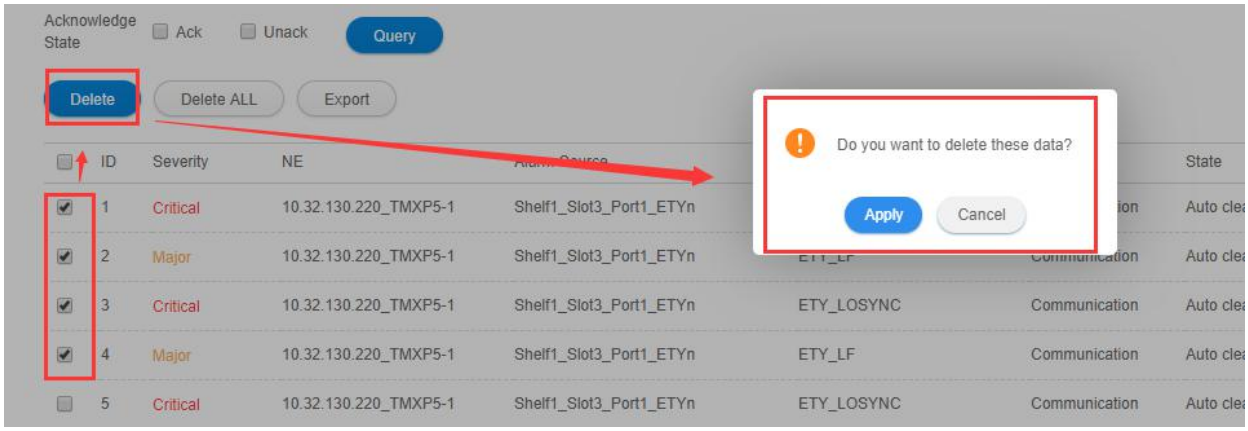



Figure8-17 Delete History Alarm

- The function of"*Delete All*"button is to delete all the history alarms.
- The function of"*Export*"button is to export all the history alarms. A dialog box pops up after clicking the Export button. Enter the name of the file you want to save in the dialog box. After saving, it will prompt to save the path. The exported data is saved in Excel format.

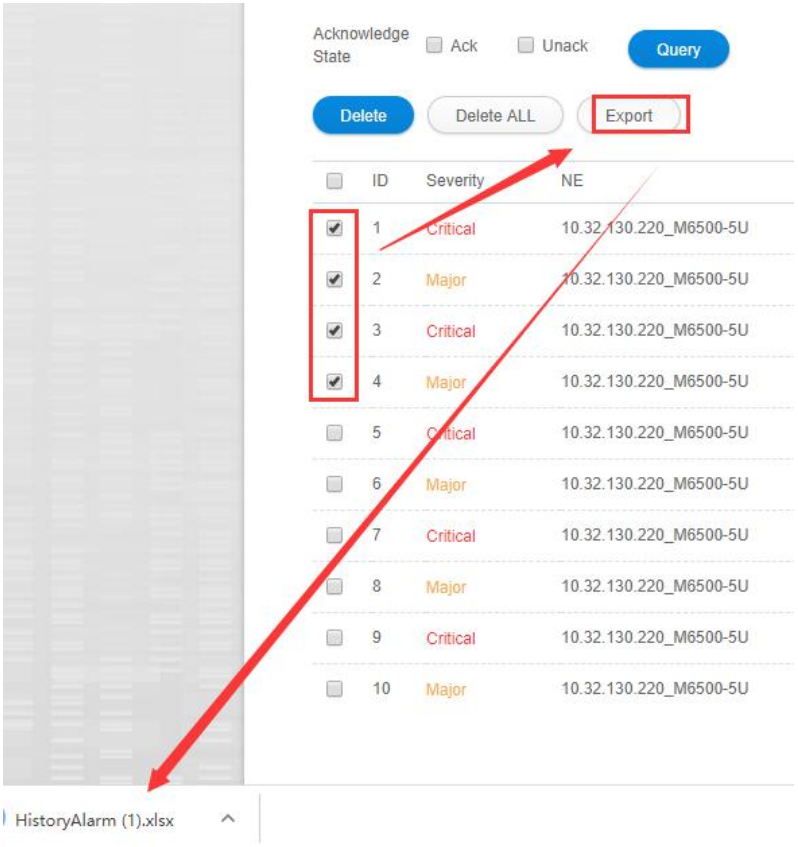



Figure8-18 Export History Alarm

**Hint**

**The path to save the data is: NMS Installation Root Directory→report_out Folder→HistoryAlarm Folder→File Name.xls.**

The lower area of the navigation bar is the display section of the history alarm. From left to right in turn, the table header is: Serial Number, NE, Alarm Source, Alarm Name, Alarm Type, Severity, status, Raised Time, Cleared

Time, Acknowledge State,Acknowledge User, Acknowledge Time. (The functions are the same as that in the current alarm. Here we will not go into much detail.)

Hint

**In history alarm details, there is no recommended measure and linked document. There are three types of alarm clearance states, which are automatic clearance, manual clearance and synchronous clearance.For the confirmation state, it can only be"confirmation" state.There are two types of confirmer, which are automatic confirmation and current login user confirmation, such as root.**

# 8.3. Alarm Configuration

## 8.3.1. Alarm Configuration

Click on"*Configuration*"and click on"*Alarm Configuration*"in the submenu to enter the alarm configuration page, as shown in the figure below:

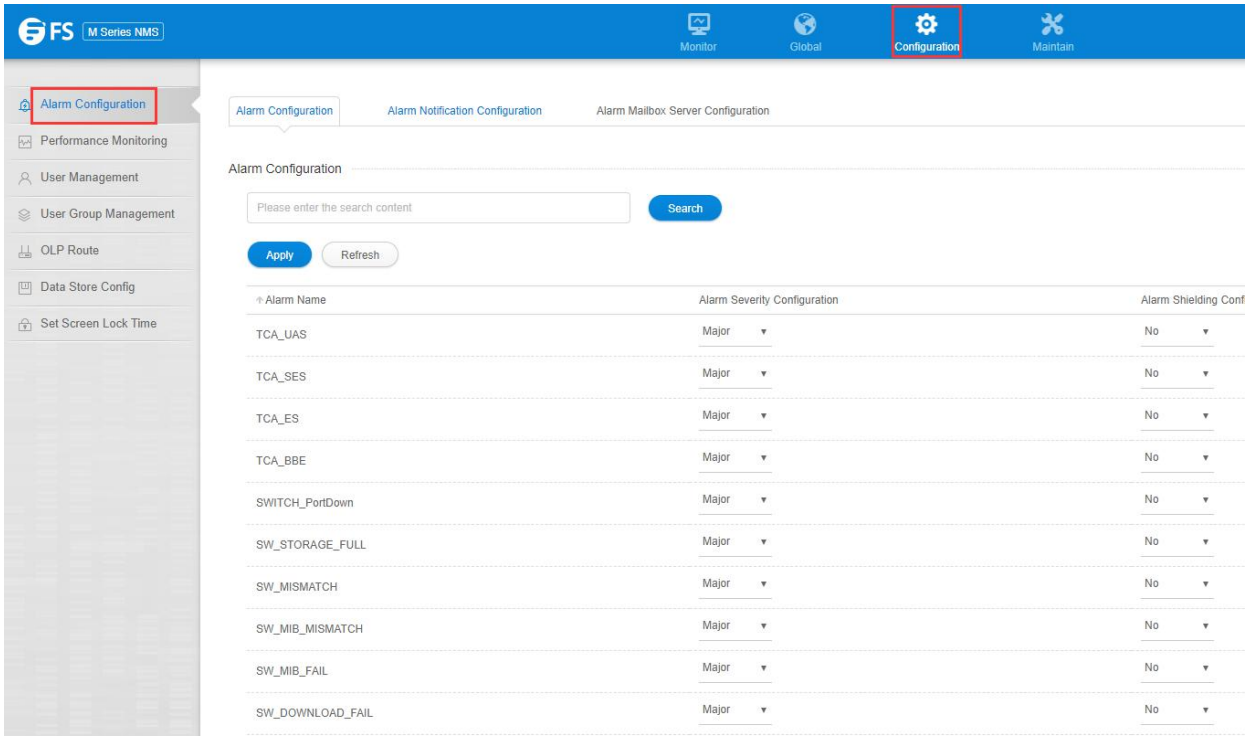



Figure8-19 Alarm Configuration

The lower right corner of the alarm configuration interface can filter the number of alarms displayed on the current page, and the number of displayed alarms per page can be adjusted to 10, 20, 50 and 100.

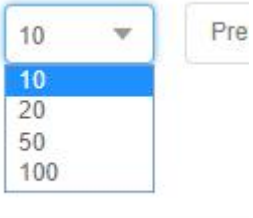



Figure8-17 Number of Alarms Displayed in Alarm Configuration

The upper area of the alarm configuration shows the searching function. By entering the specified content, it can get the alarms which contain that content, as shown in the following figure.

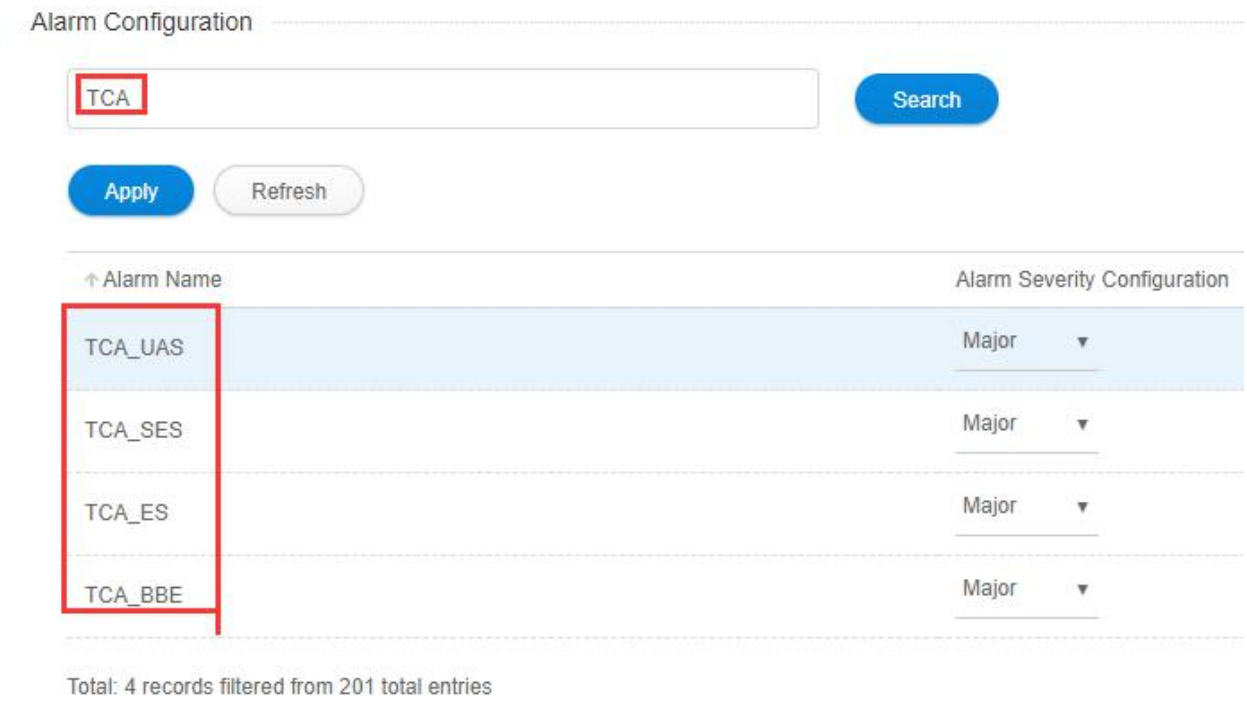



Figure8-18 Searching Function in Alarm Configuration

The middle area of the alarm configuration is the main content of alarm configuration. The table headers are: alarm name, alarm level configuration and alarm shielding configuration.

- Alarm Name: All the alarms on NE are contained in alarm name.
- Alarm Level Configuration: The specified alarm level can be set for the specified alarm. There are four optional levels: emergency, primary, secondary warning. (The alarm level before configuring is the default level.)
- Alarm Shielding Configuration: It can shield the specified alarm. After the alarm is shielded, if the alarm is generated on NE, it will not be displayed on the NMS system. (By default, all the alarms are not shielded.)

### 8.3.2. Alarm Notification Configuration

Click on"*Alarm Notification Configuration*"in the submenu to enter the alarm notification configuration page, as shown in the figure below:

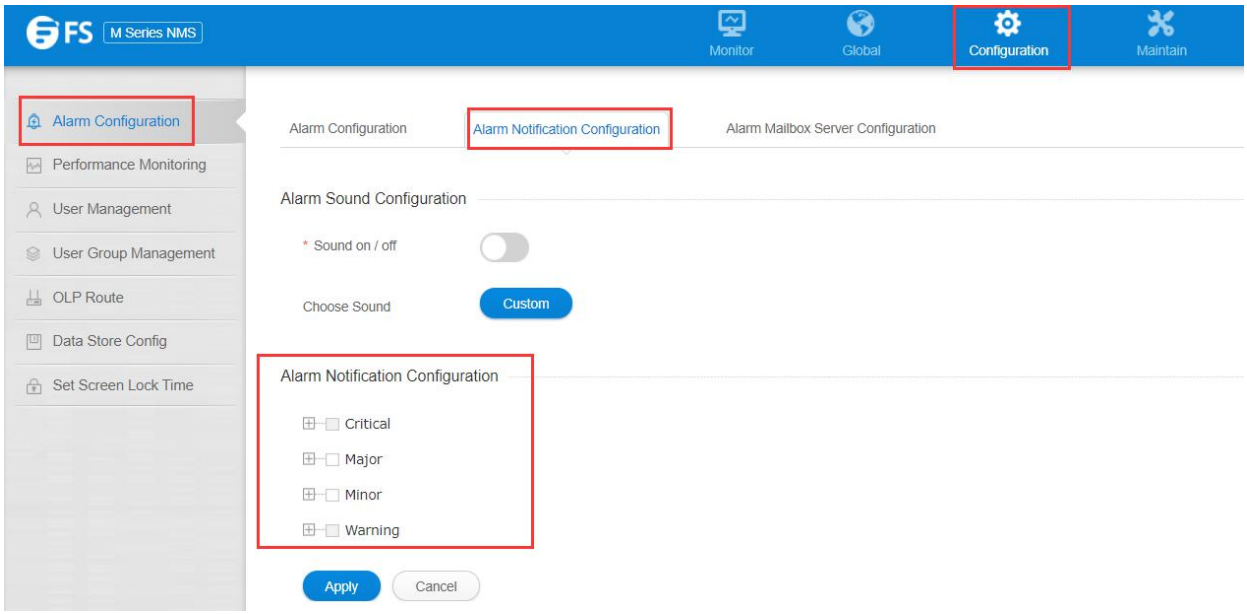



Figure8-19 Alarm Notification Configuration

**Hint**

**The alarm notification configuration is an alarm configuration for alarm mail notifications, and by default only the alarm at the emergency level is checked (that is, the mail receives only the alarm notification at the emergency level).**

After expanding the Emergency Level Alarm Tree, you can find that by default all the Emergency Level Alarms are selected.The designated alarms or all the alarms can be checked or the check can be canceled. In application,it will only receive the generation and elimination information of the selected alarm in the mail system.

### 8.3.3. Alarm Mailbox Server Configuration

Click on"*Alarm Mailbox Server Configuration*"in the submenu to enter the alarm mailbox server configuration page, as shown in the figure below:

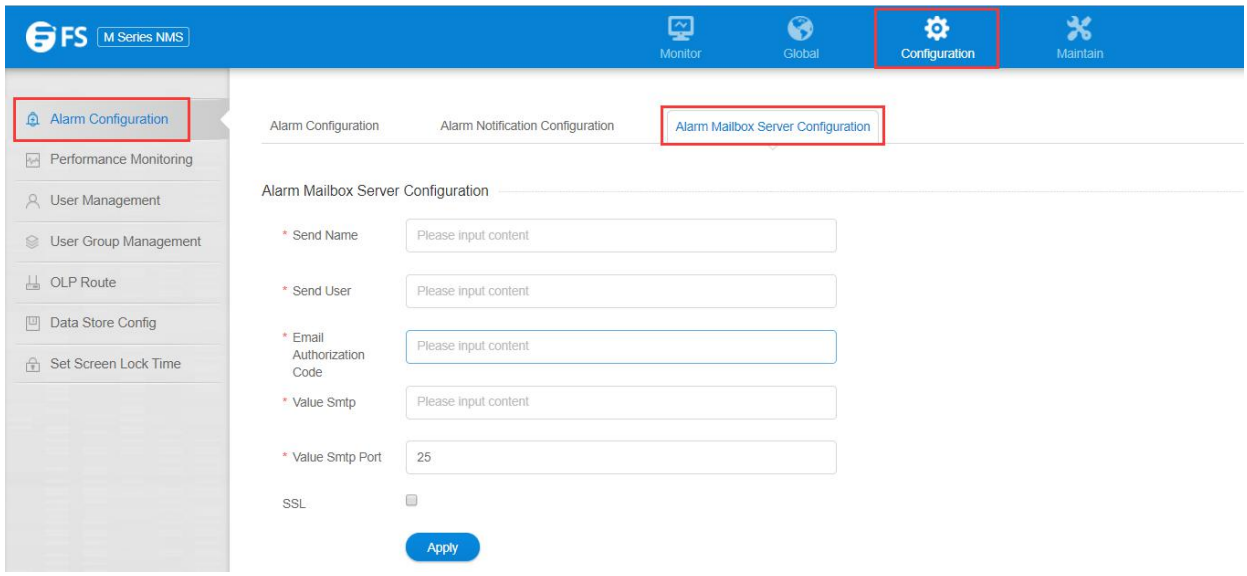



Figure 8-20 Alarm Mailbox Server Configuration

The function of the alarm mailbox server configuration is to configure a mailbox as a server mailbox, and then click on the navigation bar→Configuration.

Configuration→User Management→(Specify User Bar) Modify Information→Fill in a mailbox address for receiving alarm notifications.In this way, the alarm generated on the NE (after the configuration in the previous section) is sent to the specified mailbox by the mailbox server, and the alarm mail can be received.

**Hint**

**For different types of mailboxes, SMTP addresses and port numbers are different.Before setting the server mailbox, please check to confirm the server mailbox type and the SMTP information to be used.**

### 8.3.4. Enable the Alarm Sound

Enable sound function means when there is an alarm on the NMS system, the NMS server will continue to issue an alarm sound after enabling this function, so as to indicate that there is an alarm on the NMS system. Currently, the NMS system only has function to enable or disable the sound.

**Hint**

**There are four kinds of alarm sounds, which correspond to emergency alarm, main alarm, secondary alarm and warning alarm respectively, but when the NMS system enables the sound, only the highest level alarm sound is prompted.When the alarm level changes, the alarm sounds also change (for example, the current alarm level is emergency and main, it will prompt the highest level alarm sound which is emergency alarm sound. If at that time the alarm at the emergency level disappears, then it will turn to the main alarm sound).**

### 8.3.5. Custom Alarm Sound

Custom alarm sound mean that customers can set different alarm tones for different types of alarms according to their own needs.

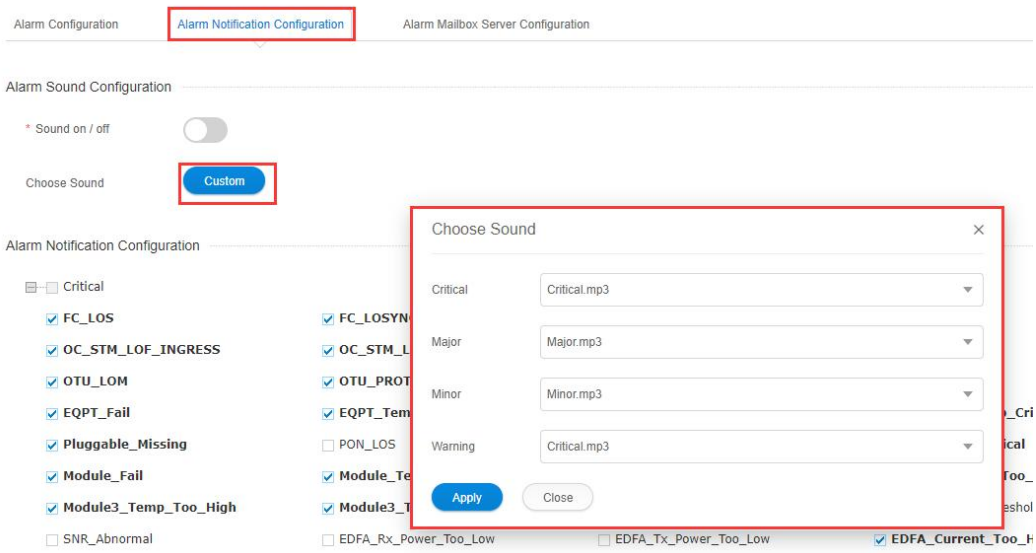



Figure8-21 Custom Alarm Sound

# 9. Performance Management

The first step of performance management is to enable the performance monitoring point to be monitored in the performance monitoring point management interface.

## 9.1. Performance Management Introduction

### 9.1.1. Filter Box

Click on "*Configuration*" on the top menu bar and select"*Performance Monitoring*", as shown in the figure below:

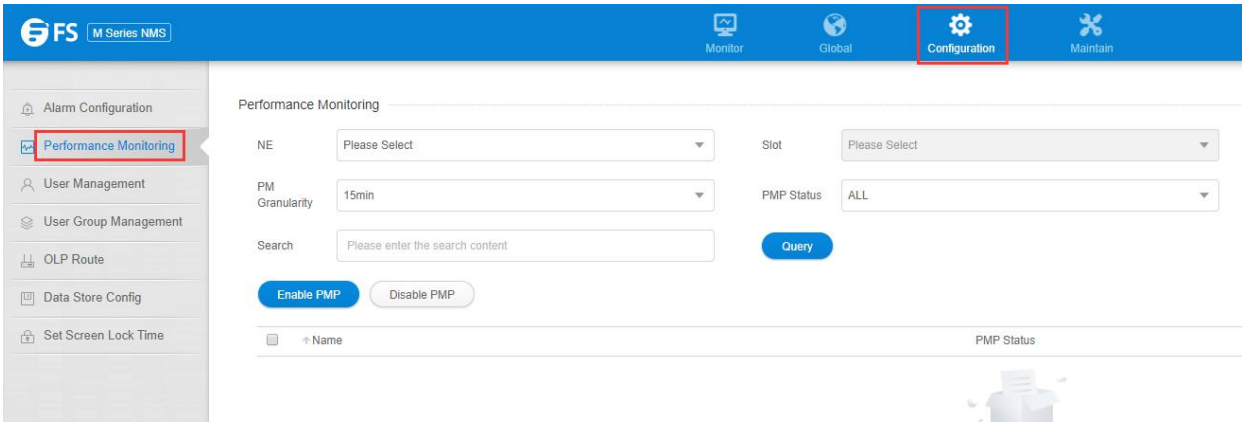



Figure9-1 Performance Monitoring Point Management Interface

Check the status of the corresponding monitoring point through the above filter box. The filter conditions include network element, slot, port, PM monitoring cycle, performance monitoring status. (There are three kinds of monitoring status: enable, disable and all. The three kinds of monitoring status can be viewed separately.) For all filter conditions, when any of them is selected, you can get the corresponding information by clicking "*Query*" in the middle part, as shown in the figure below.

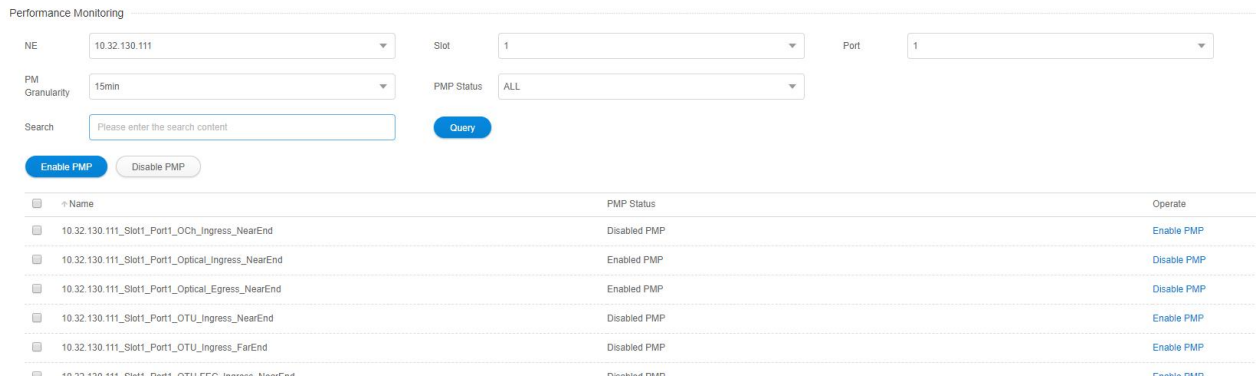



Figure 9-2 Show Monitoring Management Information

### 9.1.2. Performance Monitoring Point Introduction

- The performance monitoring point is determined by monitoring point ID, monitoring point location, monitoring point direction and monitoring cycle.
- Performance monitoring point location: far end and near end (for OTUk and ODUk).
- Near-end monitoring point: according to received BIP8.

- Far-end monitoring point: according to received BEI.
- The direction of performance monitoring points: ingress and egress.
- Monitoring Cycle: 15 minutes, 24 hours.

### 9.1.3. Enable Performance Monitoring Point

When the current 15-minute performance monitoring point is enabled, all the performance monitoring parameters of the performance monitoring point are enabled at the same time, so when the performance monitoring point is enabled, the relevant data of the current performance statistics can be viewed. The 24-hour performance monitoring operation is the same as the 15-minute operation, as shown in the figure below:

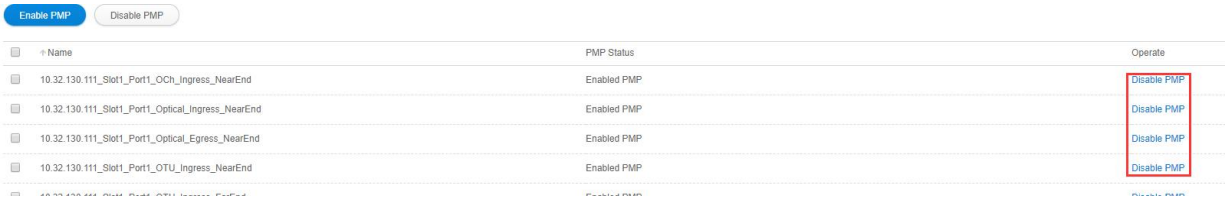



Figure9-1 Enable Monitoring Points

Since the enablement of performance monitoring point will affect the NE performance, currently up to 500 performance monitoring points (including 15 minutes and 24 hours) for a single network element are supported. However, if there are more than 500 points, then the system will prompt the operation failure, as shown in the figure below:

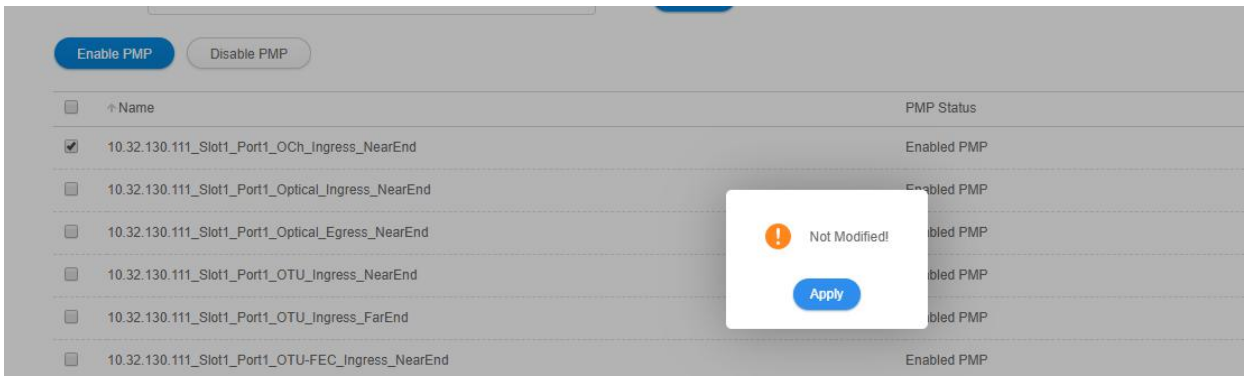



Figure9-2 Operation Failure

Each performance monitoring point can be enabled individually by modifying the status with the button behind it (Disable PMP→Enable PMP), as shown in the figure below:

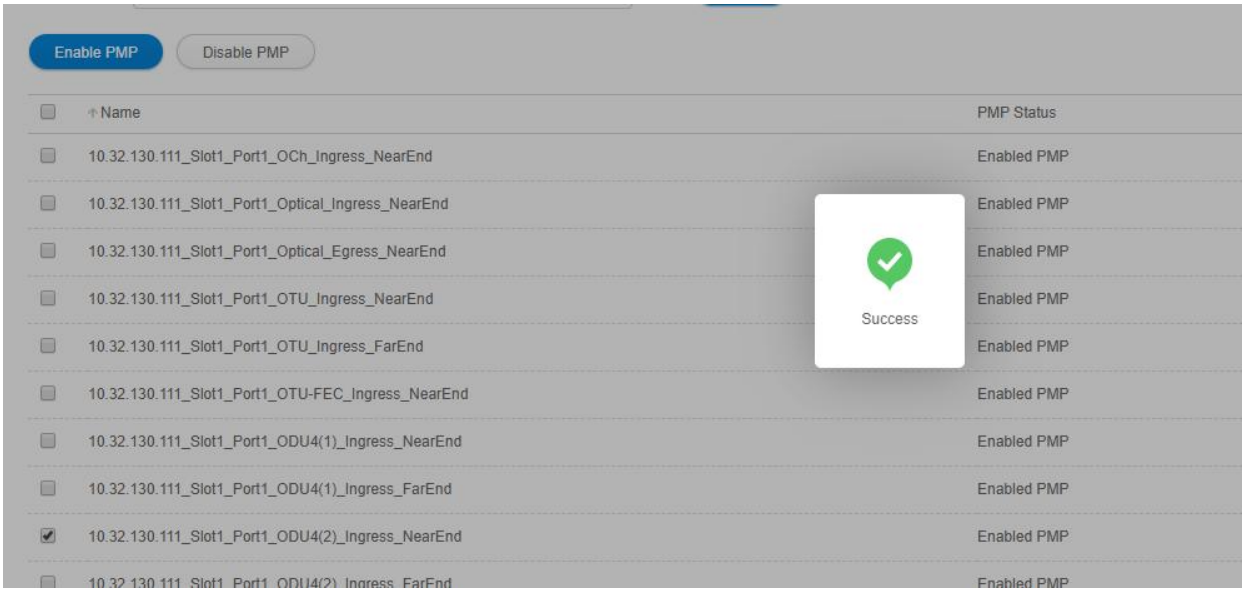



Figure9-3 Enable A Single Monitoring Point

To realize batch enabling operations on multiple pieces of data, you can select the previous multiple checkboxes, then click the button on the table (Enable PMP) to enable the monitoring of selected performance, as shown in the figure below:

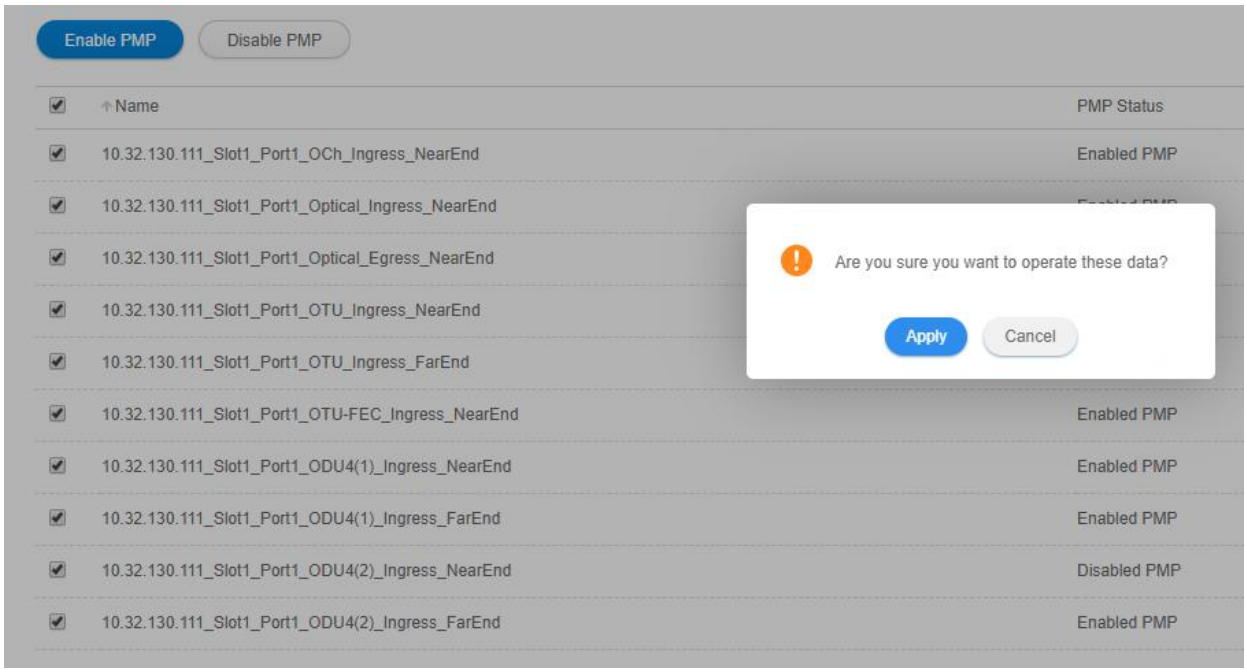



Figure9-4 Batch Enabling Monitoring Point

Select multiple enabled performance monitoring, then select“Enable PMP”button, click on “Apply”, it will display“Not Modified”, as shown in the figure below.

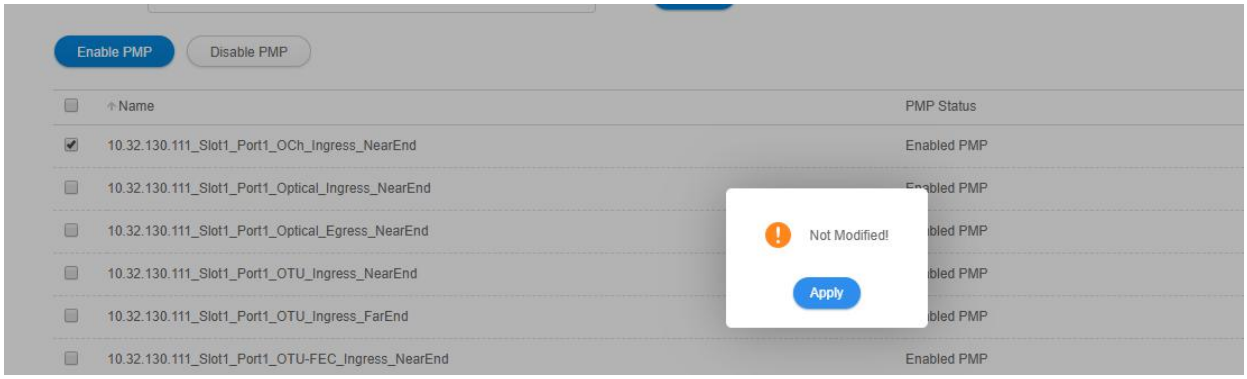



Figure9-5 No Modification of Monitoring Point Status

### 9.1.4. Disable Performance Monitoring Point

When the current 15-minute performance monitoring point is disabled, the 24-hour performance monitoring will be automatically disabled by default, and all the performance monitoring parameters of the performance monitoring point will be disabled at the same time. Therefore, when the performance monitoring point is disabled, the relevant data of the current performance statistics can not be viewed, as shown in the figure below:

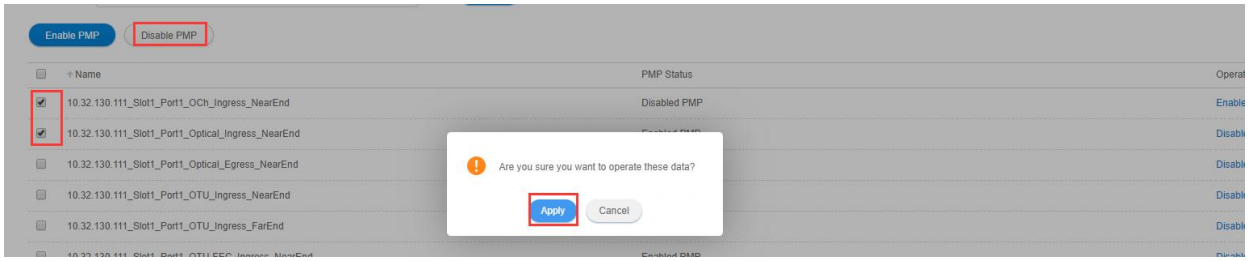



Figure9-6 Disable Monitoring Point

Each monitoring point can be disabled by modifying the status of the monitoring point with the button behind it (Enable PMP - >Disable PMP)，as shown in the figure below:

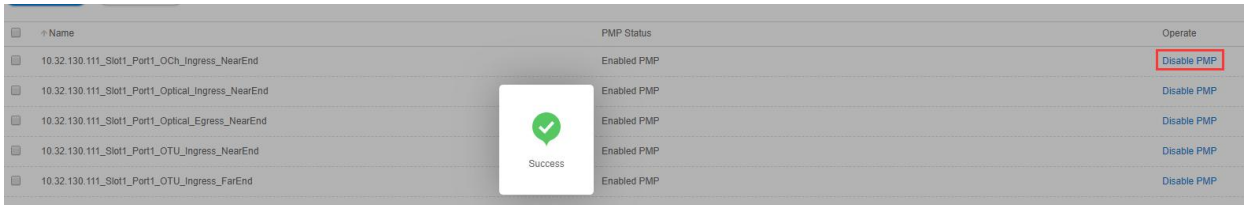



Figure9-7 Disable A Single Monitoring Point

To realize batch disabling operations on multiple pieces of data, you can select the previous multiple checkboxes, then click the button on the table (Disable PMP) to disable the monitoring of selected performance,as shown in the figure below:

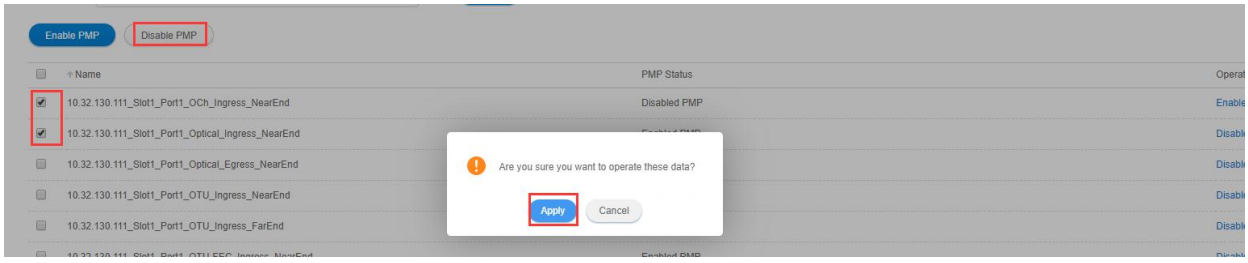


Figure9-8 Disable Batch Monitoring Points

Select multiple disabled performance monitoring, then select “Disable PMP”button, click on“Apply”, it will display “Not Modified”, as shown in the figure below.

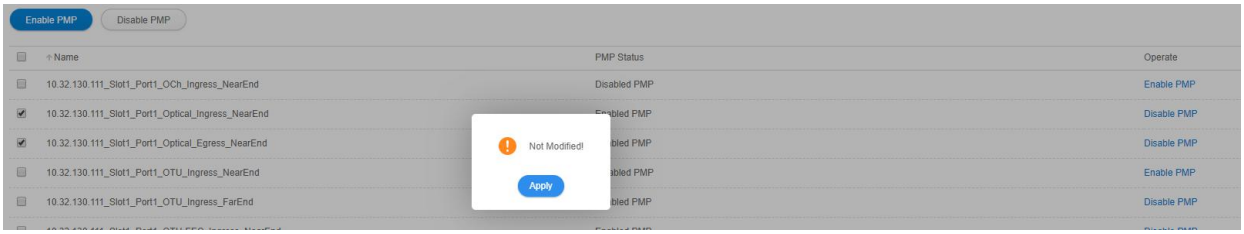



Figure9-11 No Modification of Monitoring Point Status

### 9.1.5. Attentions for Monitoring Performance

- When monitoring points are enabled, they will be disabled in several cases:

  (1) Manually disable a single monitoring point or batch monitoring points.

  (2) After the board mode is switched, all the 15-minute and 24-hour monitoring points of the port are automatically disabled.

  (3) When the port changes the mode, only the monitoring point of the optical power among all the 15-minute and 24-hour monitoring points of the port will not be disabled, and all other performance monitoring points will be automatically disabled.

  (4) When the 15-minute performance monitoring point is disabled, the corresponding 24-hour performance monitoring point will be automatically disabled.

- When the user disable the performance monitoring point:

  (1) The current performance data cannot be acquired.

  (2) The history performance data which has been saved can be viewed by the NMS system and the user.

  (3) When the user issues the disable command, the monitoring data that has been counted during that time period (do not reach a full 15-minute or 24-hour monitoring cycle) will not be saved to history performance data.

  (4) When the port mode is switched or the port mode is set as empty, all the performance monitoring points under this port mode will be automatically deleted. (Previously stored history performance data are still retained.)

  (5) When the TP such as OCh, OTUk, ODUk, Ethernet and SDH/SONET corresponding to the port or the monitoring point is administrative down, all the performance monitoring points of the TP will be automatically disabled. (Previously stored history performance data are still retained.)

## 9.2. Current Performance Statistics

Click on "*Maintenance*" in the top menu bar, and select "*Performance Current Info*" in the left navigation bar, as shown in the figure. you can find current performance statistics of optical power, FEC, OTU/ODU, SDH regeneration segment and Ethernet at the right side, as shown in the figure below:

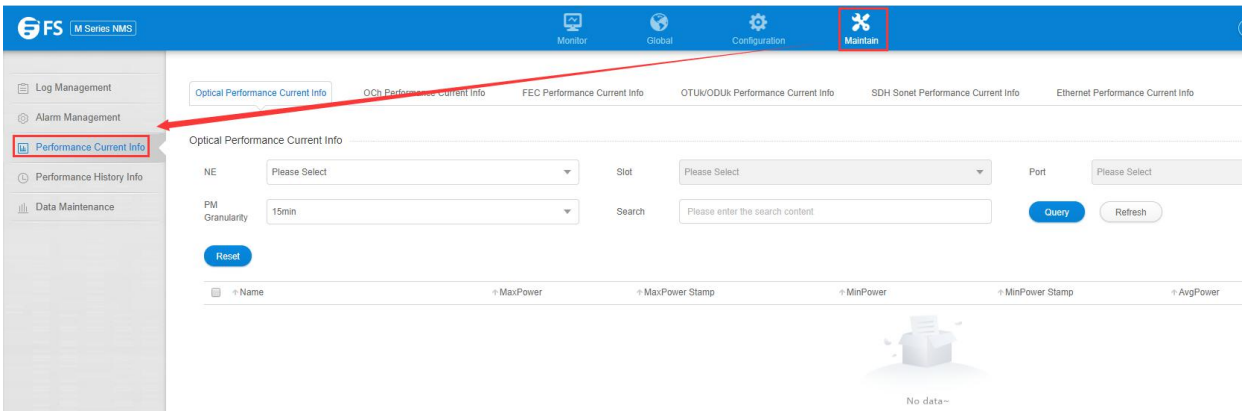



Figure9-12 Current Performance Statistics Directory

## 9.2.1. Monitoring of Optical Power

### 9.2.1.1. Introduction of Optical Power Monitoring Parameters

The monitoring parameters of optical power monitoring point include maximum optical power, maximum optical power time stamp, minimum optical power, minimum optical power time stamp, average optical power, suspicious interval marker, running time and reset operation. The performance parameters of optical power will be enabled or disabled at the same time.

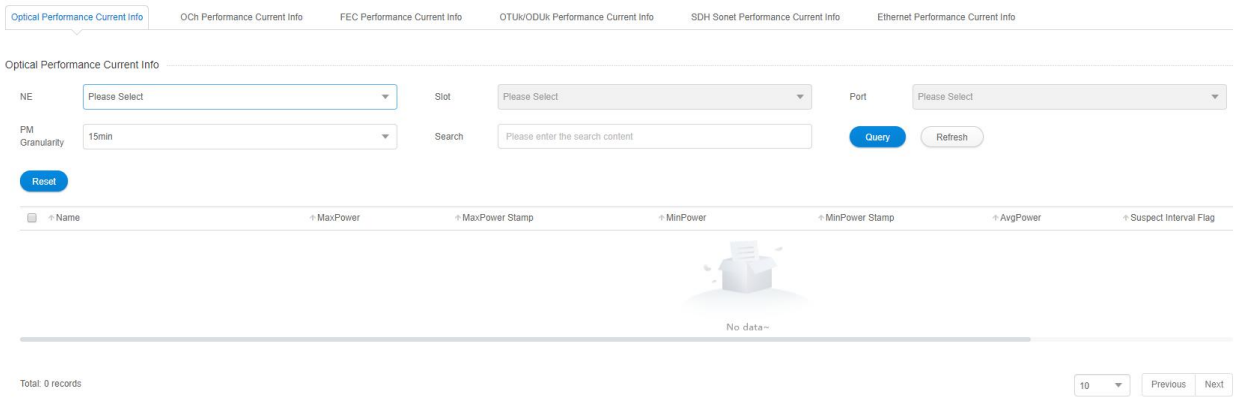



Figure9-13 Display Monitoring Parameters

### 9.2.1.2. View Optical Power Monitoring Information

Select the appropriate network elements, slots, ports and monitoring cycle through the selection box above the menu, the optical power value of a certain network element/slot/port will be displayed. Optical power includes two monitoring points for near-end transmission and near-end reception. Optical module is inserted into the monitoring port. Data of the maximum and minimum optical power and of the corresponding generation time stamp which are currently read will be displayed. After the 15-minute monitoring port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 900 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 15-minute data automatically becomes the history data.

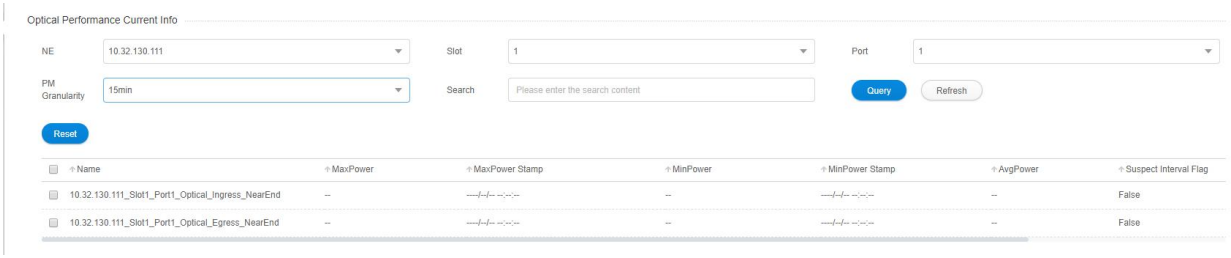



Figure9-14 15-Minute Monitoring Point Data of Optical Power

When the 24-hour monitoring port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 86400 seconds, the suspicious interval marker will become trustworthy. The running time counts again from 0. The last 24-hour data automatically becomes the history data.

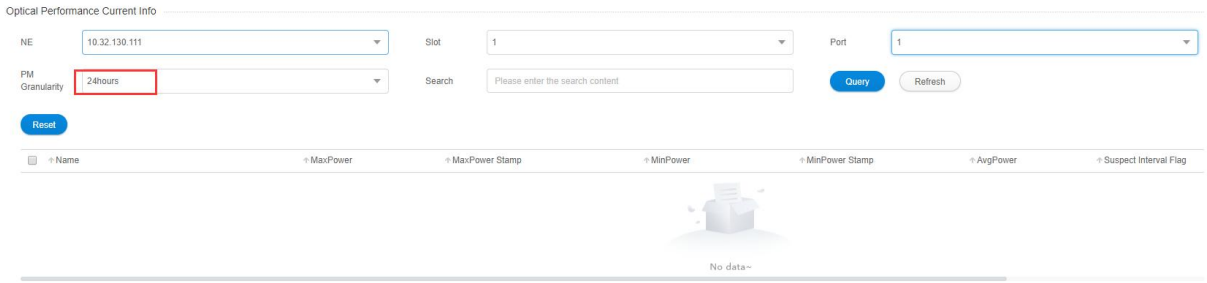



Figure9-15 24-Hour Monitoring Point Data of Optical Power

### 9.2.1.3. Reset Optical Power Monitoring Data

When the current optical power monitoring point needs to be reset and to restart the monitoring, the 15-minute and 24-hour operation steps are the same. Taking 15-minute operation as an example, you can click on Reset behind each piece of monitoring record to perform resetting of a single piece of monitoring record, or you can select the first box to do batch resetting, as shown in the figure below.

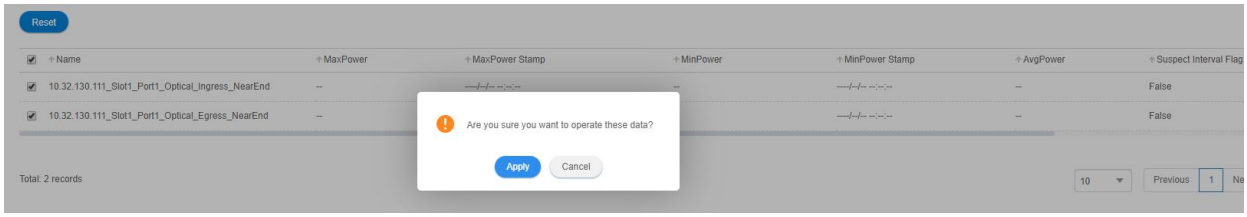



Figure9-16 Batch Resetting of Optical Power

Then click on *Apply* button, as shown in the figure, it will show that the operation is successful. After that, click on "*Refresh* " button to refresh the whole page. At this time, the suspicious interval marker will become from untrustworthy to trustworthy and the running time counts again from 0. The maximum optical power time stamp and the minimum optical power time stamp are updated to the latest time to read the optical power, and the value of the maximum and minimum optical power are updated to the data read at the latest time.

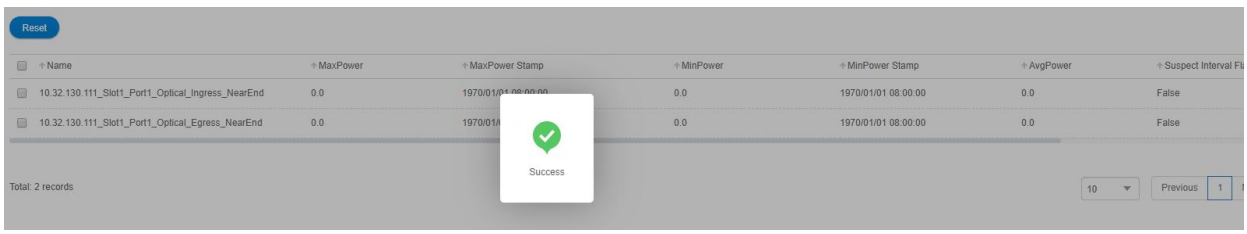



Figure9-17 Successful Reset Operation

#### 9.2.1.4. Optical Power Monitoring Data Shown As"-"

Here are the situations when the monitoring data of optical power for the port is shown as NA:

(1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.

(2) Optical module is inserted into the port but it is mismatched and the port is enabled.

At this time, both the maximum and minimum optical power will be shown as -. The time stamp of the maximum and minimum optical power will be shown as ----/--/--:--:--. The suspicious interval marker is untrustworthy. The running time is normal and counts from 0, as shown in the figure below:

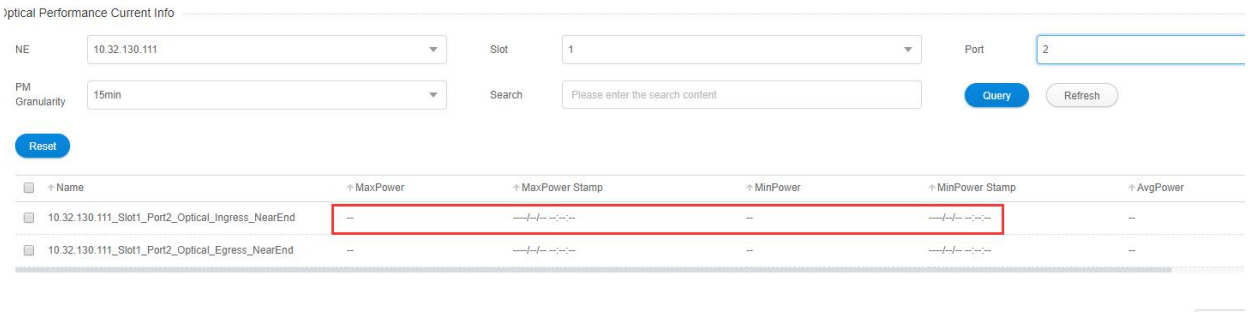



Figure9-18 Optical Module of Optical Power Not in Position

Here are the situations when the monitoring data of optical power for the board is shown as -:

(1) When the board is not in position or is pre-configured with an empty slot and the port for the board is enabled, the maximum and minimum optical power will be shown as -.The time stamp of the maximum and minimum optical power will be shown as - /-:--.The suspicious interval is marked as untrustworthy, and the running time is always 0 without any change, as shown in the figure below.

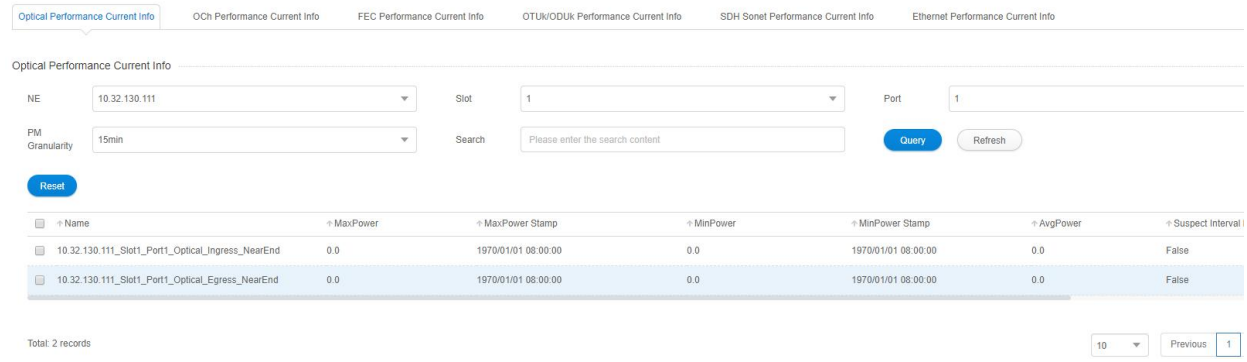



Figure9-19 Optical Power Monitoring Data

When the board is mismatched and the port for the board is enabled, the maximum and minimum optical power will be shown as -. The time stamp of the maximum and minimum optical power will be shown as ----/--/--:--:--. The suspicious interval is marked as untrustworthy, and the running time counts from 0, as shown in the figure below:

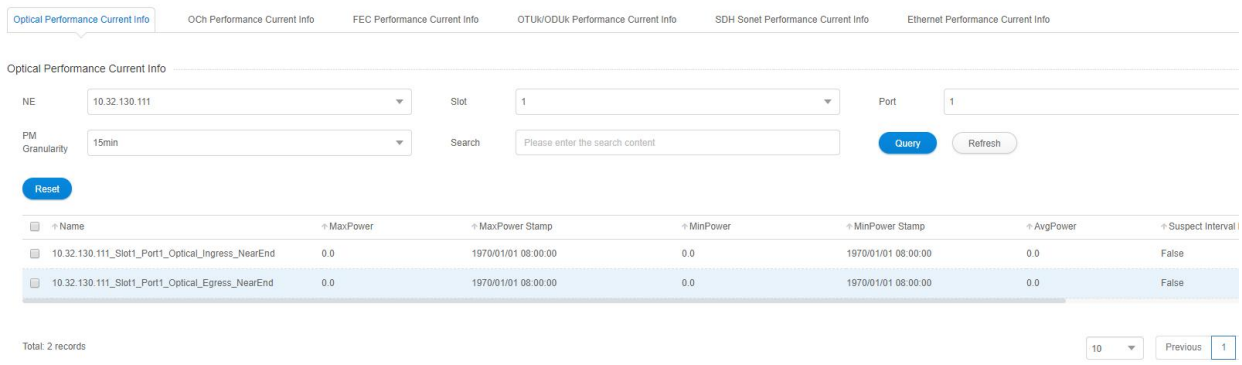



Figure9-20 Optical Power Monitoring Data When Mismatched

## 9.2.2. OCh Current Performance Statistics

### 9.2.2.1. OCh Monitoring Parameters Introduction

Monitoring parameters of OCh monitoring points include maximum differential group delay (DGD), maximum differential group delay (DGD) time stamp, minimum differential group delay (DGD), minimum differential group delay (DGD) time stamp, average differential group delay (DGD), maximum chromatic dispersion (CD), maximum chromatic dispersion (CD) time stamp, minimum chromatic dispersion (CD), minimum chromatic dispersion (CD) times tamp, average chromatic dispersion (CD), maximum optical signal-to-noise ratio (OSNR), maximum optical signal-to-noise ratio (OSNR) time stamp, minimum optical signal-to-noise ratio (OSNR), minimum optical signal-to-noise ratio (OSNR) time stamp, average optical signal-to-noise ratio (OSNR), suspicious interval marker, running time and reset operation. The performance parameters of OCh will be enabled or disabled at the same time.

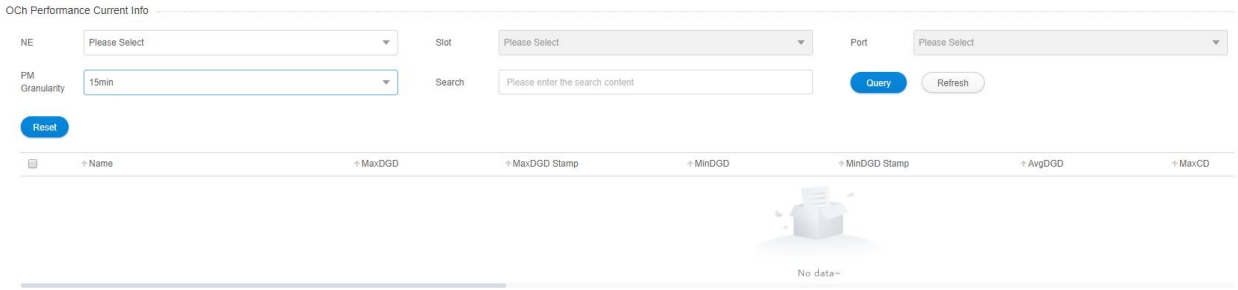



Figure9-21 OCh Monitoring Parameters

### 9.2.2.2. View OCh Monitoring Information

Only when WDM optical module is inserted can OCh monitoring point and related data exist.Select the appropriate network elements, slots, ports and monitoring cycle through the selection box above the menu, the OCh value of a certain network element/slot/port will be displayed. OCh includes only one monitoring point which is entrance-near end. WDM module is inserted into the monitoring port. OCh data and corresponding generation time which are currently read will be displayed. After the port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 900 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 15-minute data automatically becomes the history data.

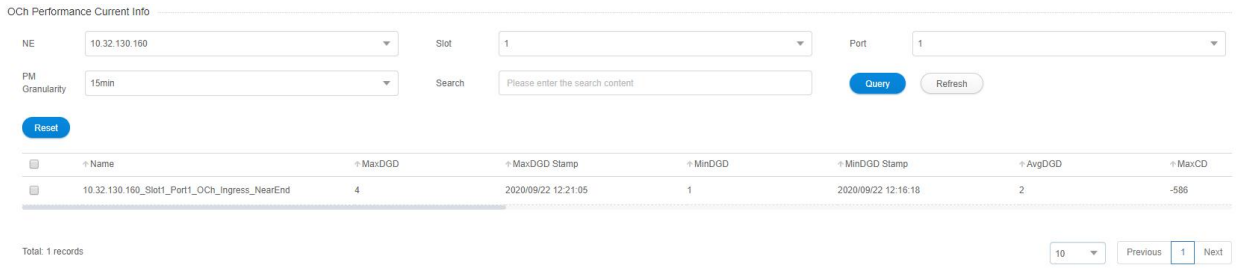



Figure9-22 15-Minute OCh Monitoring Data

WDM module is inserted into the monitoring port. OCh data and corresponding generation time stamp which are currently read will be displayed. After the 24-hour performance monitoring port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 86400 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 24-hour data automatically becomes the history data, as shown in the figure below:

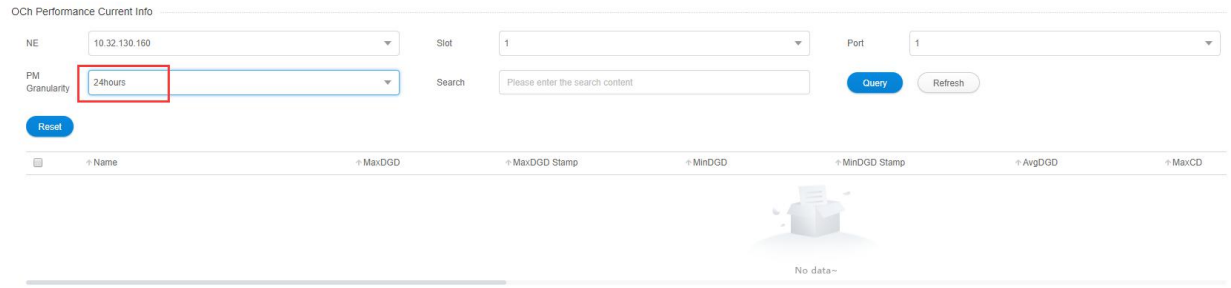



Figure9-23 24-Hour OCh Monitoring Data

### 9.2.2.3. Reset OCh Monitoring Data

When the current OCh monitoring data needs to be reset and to restart the monitoring, the 15-minute and 24-hour operation steps are the same. Taking 15-minute operation as an example, you can click on Reset behind each piece of monitoring record to perform resetting of a single piece of monitoring record, or you can select the first box to do batch resetting, as shown in the figure below.

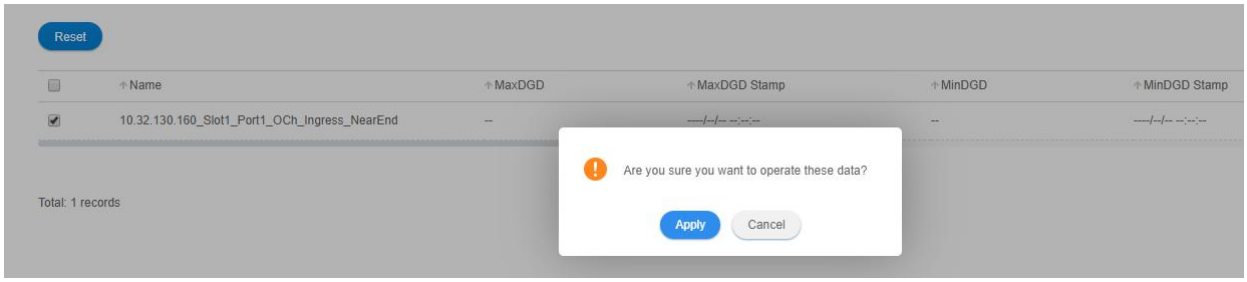



Figure9-24 Reset OCh Data

Then click on *Apply* button, as shown in the figure, it will show that the operation is successful. After that, click on *Refresh* button to refresh the whole page. At this time, the suspicious interval marker will become from untrustworthy to trustworthy and the running time counts again from 0. All the time stamps are updated to the latest time to read the value, and other data will be updated to that read at the latest time.

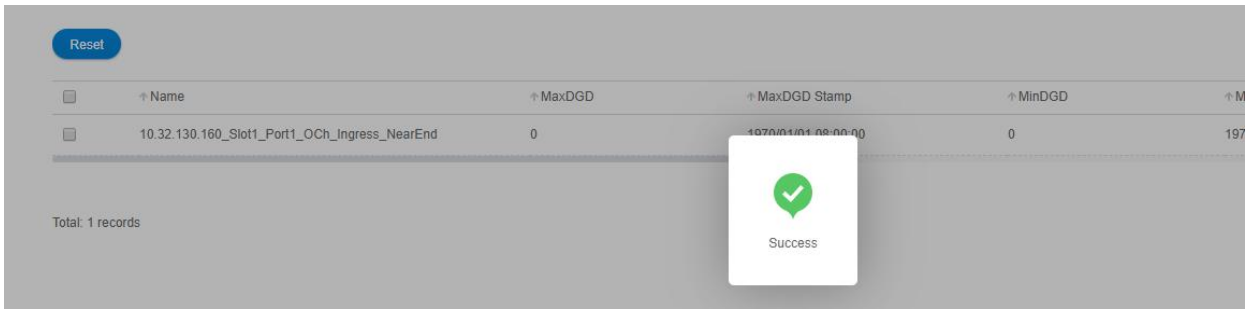



Figure 9-25 Successful Resetting of OCh

### 9.2.2.4. OCh Monitoring Data Shown As"-"

Here are the situations when the OCh monitoring data for the port is shown as -:

(1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.

(2) Optical module is inserted into the port but it is mismatched and the port is enabled.

(3) Optical module is inserted into the port but there is los, that is, no light is received.

At this time, both the maximum and minimum data will be shown as -. The times tamp of the maximum and minimum data will be shown as ----/--/--:--:--. The suspicious interval marker is untrustworthy. The running time is normal and counts from 0, as shown in the figure below:


Figure9-26 Optical Module of OCh Not In Position

Here are the situations when the monitoring data for the board is shown as NA:

(1) When the board is not in position or is pre-configured with an empty slot and the port for the board is enabled, the maximum and minimum data will be shown as NA.The time stamp of the maximum and minimum data will be shown as - /-:--.The suspicious interval is marked as untrustworthy, and the running time is always 0 without any change, as shown in the figure below.


Figure9-27 OCh Monitoring Data

(2) When the board is mismatched and the port for the board is enabled, the maximum and minimum data will be shown as -. The time stamp of the maximum and minimum data will be shown as ----/--/--:--:--. The suspicious interval is marked as untrustworthy, and the running time counts from 0, as shown in the figure below:


Figure9-28 OCh Monitoring Data When Mismatched

## 9.2.3. FEC Current Performance Statistics

### 9.2.3.1. FEC Monitoring Parameters Introduction

As shown in the figure, the monitoring parameters of FEC monitoring points include maximum error correction rate, maximum error correction rate time stamp, average error correction rate, suspicious interval marker, running time and reset operation. The performance parameters of FEC will be enabled or disabled at the same time.

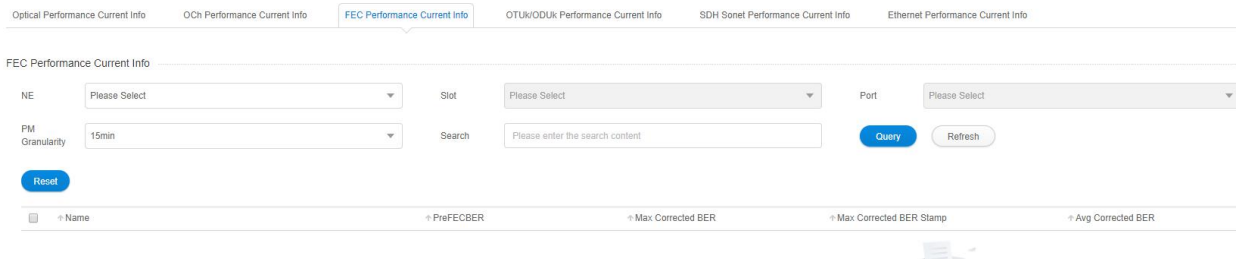



Figure9-29 FEC Monitoring Parameters

### 9.2.3.2. View FEC Monitoring Information

As shown in the figure, select the appropriate network elements, slots, ports and monitoring cycle through the selection box above the menu, the FEC value of a certain network element/slot/port will be displayed. There is only one entrance-near end monitoring point for FEC. Optical module is inserted into the monitoring port. FEC data and corresponding generation time stamp which are currently read will be displayed. After the port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 900 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 15-minute data automatically becomes the history data.

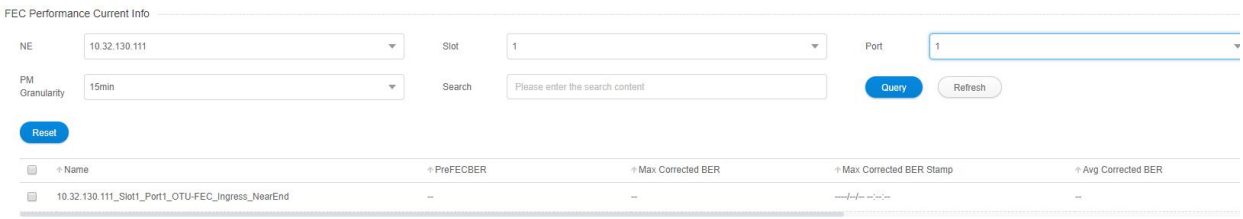



Figure9-30 15-Minute Monitoring Data of FEC

Optical module is inserted into the monitoring port. FEC data and corresponding generation time stamp which are currently read will be displayed. After the 24-hour performance monitoring port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 86400 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 24-hour data automatically becomes the history data, as shown in the figure below:

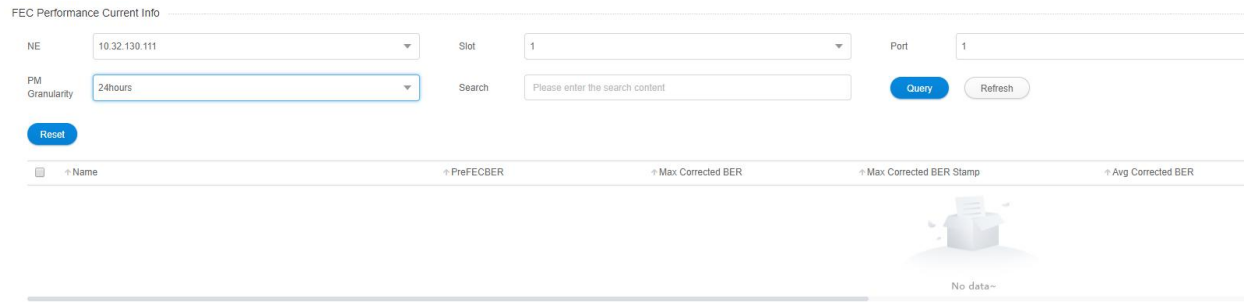



Figure9-31 24-Hour Monitoring Data of FEC

### 9.2.3.3. Reset FEC Monitoring Data

When the current FEC monitoring data needs to be reset and to restart the monitoring, the 15-minute and 24-hour operation steps are the same. Taking 15-minute operation as an example, you can click on Reset behind each piece of monitoring record to perform resetting of a single piece of monitoring record, or you can select the first box to reset, as shown in the figure below.

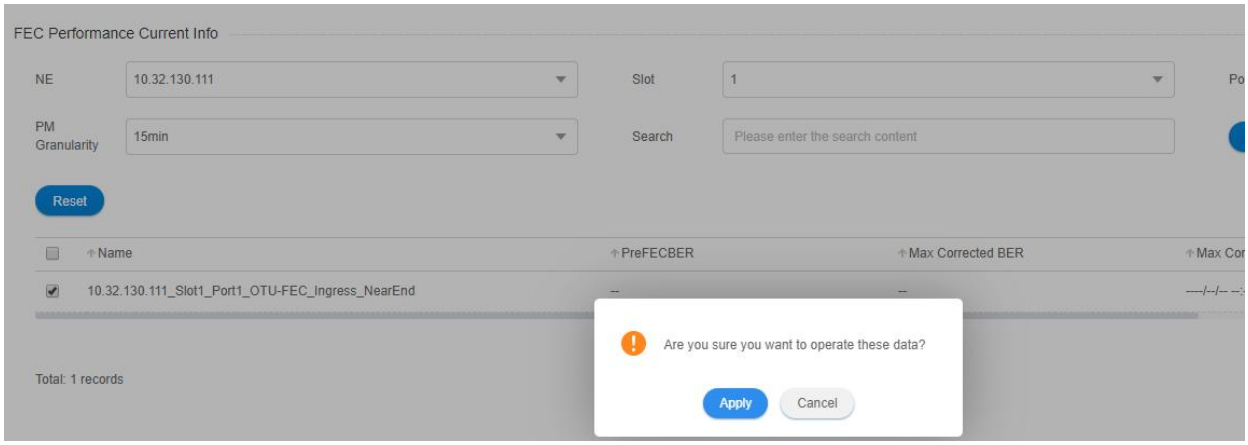



Figure9-32 FEC Reset

Then click on Apply button, as shown in the figure, it will show that the operation is successful. After that, click on Refresh button to refresh the whole page. At this time, the suspicious interval marker will become from untrustworthy to trustworthy and the running time counts again from 0. All the time stamps are updated to the latest time to read the value, and other data will be updated to that read at the latest time.

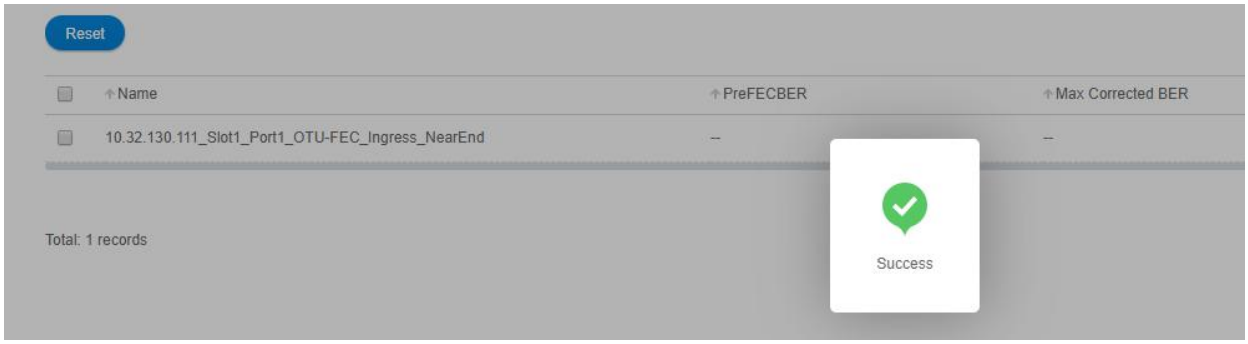



Figure9-33 FEC Successfully Reset

### 9.2.3.4. FEC Monitoring Data Shown As"-"

Here are the situations when the FEC monitoring data for the port is shown as -:

(1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.

(2) Optical module is inserted into the port but it is mismatched and the port is enabled.

At this time, all the non-time stamp data will be shown as -,and all the time stamps will be shown as ----/--/--:--:--. The suspicious interval marker is untrustworthy. The running time is normal and counts from 0, as shown in the figure below:

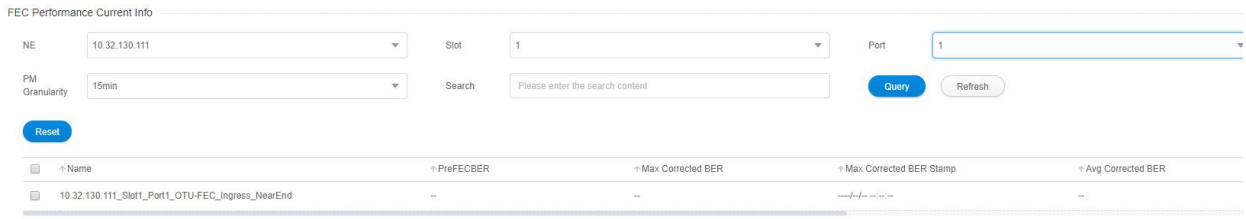



Figure9-34 Optical Module of FEC Not In Position

Here are the situations when the monitoring data for the board is shown as -:

(1) When the board is not in position or is pre-configured with an empty slot and the port for the board is enabled, all the non-time stamp data will be shown as -,and all the time stamps will be shown as - /-:--.The suspicious interval is marked as untrustworthy, and the running time is always 0 without any change, as shown in the figure below.

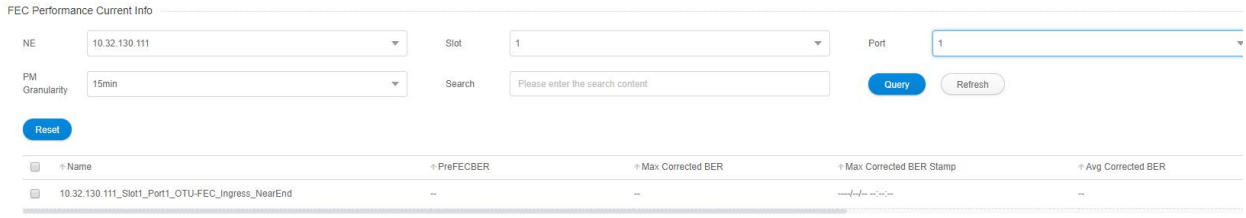



Figure9-35 FEC Monitoring Data

(2) When the board is mismatched and the port for the board is enabled, all the non-time stamp data will be shown as - and all the time stamps will be shown as ----/--/--:--:--. The suspicious interval is marked as untrustworthy, and the running time counts from 0, as shown in the figure below:

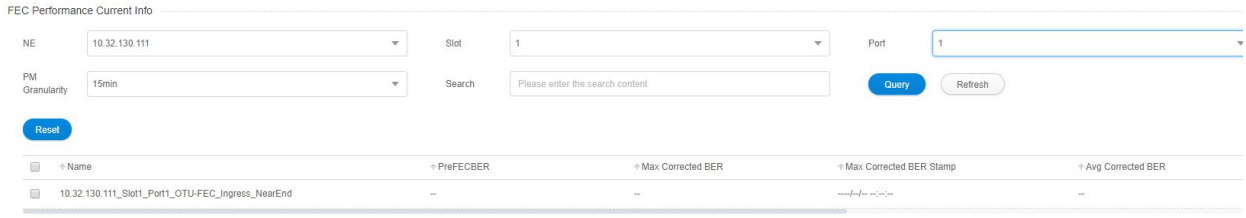



Figure9-36 FEC Monitoring Data When Mismatched

## 9.2.4. OTUk/ODUk Current Performance Statistics

### 9.2.4.1. OTUk/ODUk Monitoring Parameters Introduction

As shown in the figure, the monitoring parameters of OTUk/ODUk monitoring points include background error block (BBE), error second (ES), serious error second (SES), unavailable second (UAS), suspicious interval marker,

runtime (S) and reset operation.The performance parameters of OTUk / ODUk will be enabled or disabled at the same time.

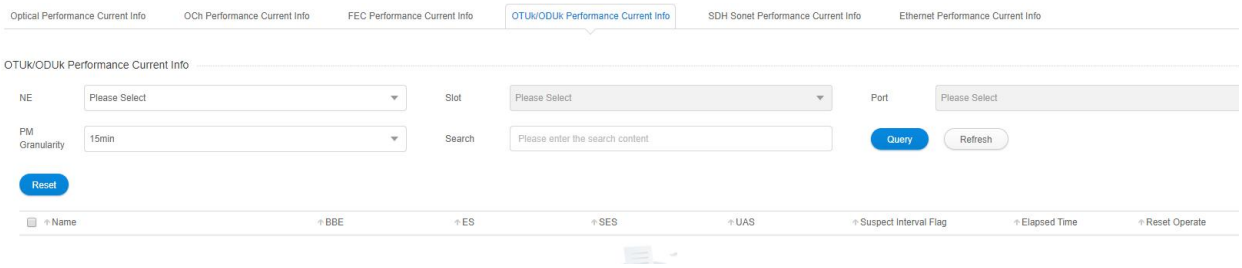



Figure9-37 OTUk/ODUk Monitoring Parameters

### 9.2.4.2. View OTUk/ODUk Monitoring Information

As shown in the figure, select the appropriate network elements, slots, ports and monitoring cycle through the selection box above the menu, the OTUk/ODUk value of a certain network element/slot/port will be displayed. The monitoring points of OTUk/ODUk include near end and far end, and the monitoring directions include entrance and exit. (Generally, the client port which is not OTU is corresponding to exit of ODU. The monitoring direction of OTU and ODU for OTU port is entrance. Non-OTU means that the services of the port are not OTU2/OTU2e.)

Optical module is inserted into the monitoring port. OTUk/ODUk monitoring data which is currently read will be displayed. After the port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 900 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 15-minute data automatically becomes the history data.

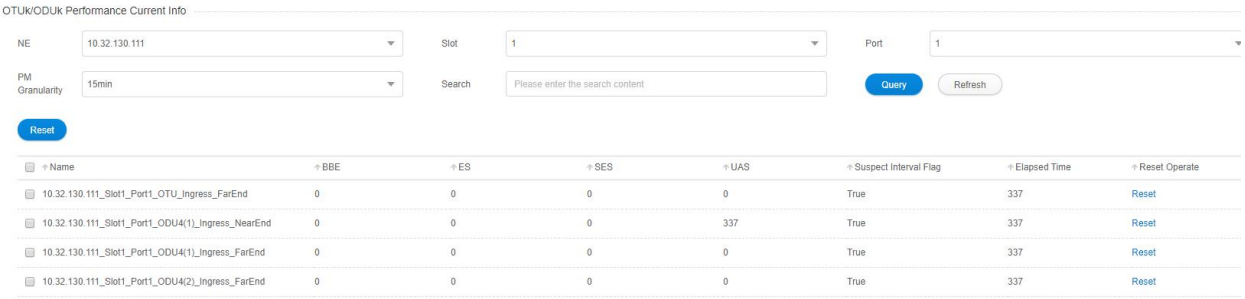



Figure9-38 15-Minute OTUk/ODUk Monitoring Data

Optical module is insertedw: into the monitoring port. OTUk/ODUk data which is currently read will be displayed. After the 24-hour performance monitoring port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 86400 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 24-hour data automatically becomes the history data, as shown in the figure belo

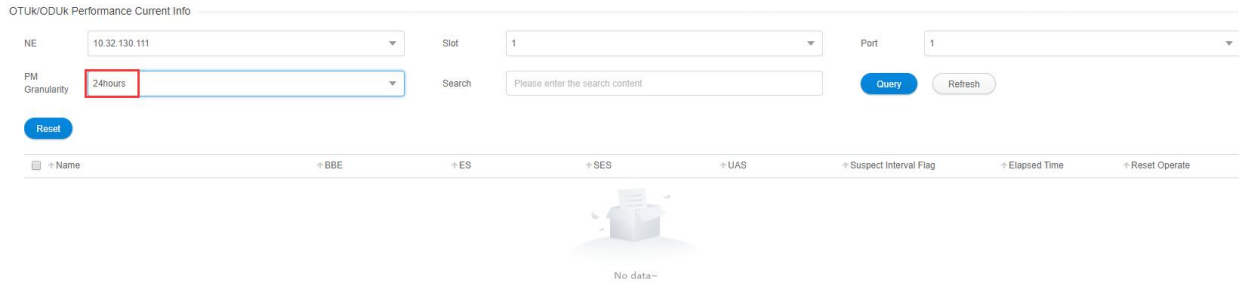


Figure9-39 24-Hour OTUk/ODUk Monitoring Data

#### 9.2.4.3. Error Generation Conditions for Monitoring Parameters

SES counts are generated when the following alarms are generated at the near end, and continuous 10S of SES becomes a UAS. If the alarm persists, the ES and SES stops counting, but the UAS counts all the time, as shown in the figure.

- Equipment Missing
- Equipment Mismatch
- Equipment Failure
- OTUk defects: OTU-LOS, OTU-LOF, OTU-LOM, OTU-AIS and OTU-TIM.
- ODUk defects: alarms of the Server layer (e.g. LOS, LOF, LOM), ODU-AIS, ODU-LCK, ODU-TIM, ODU-OCI and ODU-PLM.
- When alarms are generated at the far end, SES counts generate.
- BDI.
- When low-rate bit error is inserted by the meter, BBE and ES generate.
- ES and SES are generated when high-rate bit error is inserted by the meter. The continuous 10S of SES will become a UAS. If the high-rate bit error of the meter keeps, then ES and SES stops counting but UAS will count all the time.

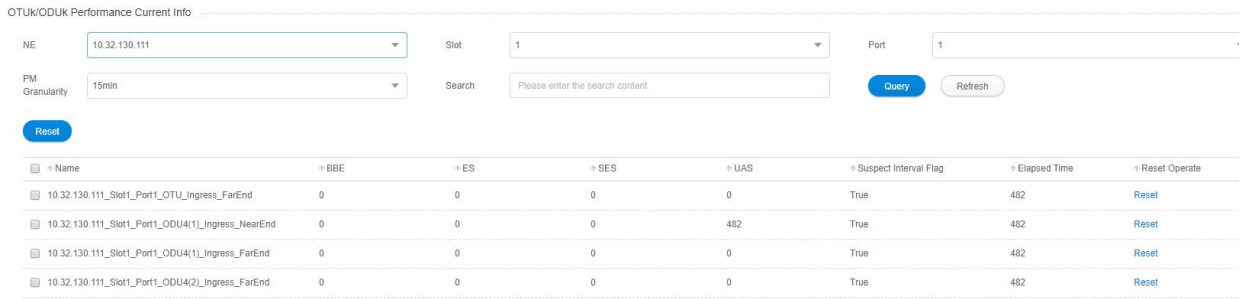



Figure9-40 UAS Always Counts

#### 9.2.4.4. OTUk/ODUk Monitoring Data Reset

When the current OTUk/ODUk monitoring data needs to be reset and to restart the monitoring, the 15-minute and 24-hour operation steps are the same. Taking 15-minute operation as an example, you can click on Reset behind each piece of monitoring record to perform resetting of a single piece of monitoring record, or you can select the first box to do batch resetting, as shown in the figure below.

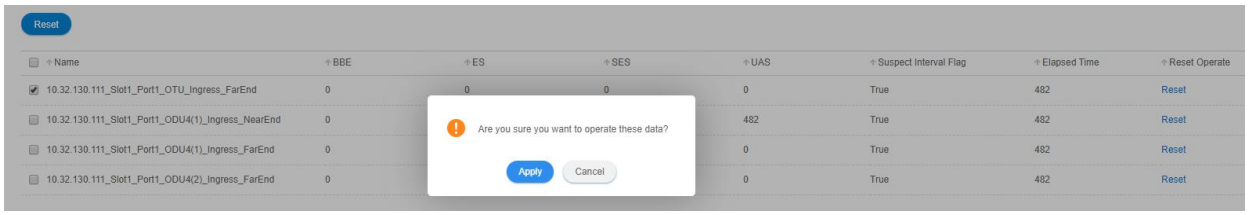



Figure9-41 OTUk/ODUk Reset

Then click on *Apply* button, as shown in the figure, it will show that the operation is successful. After that, click on *Refresh* button to refresh the whole page. At this time, the suspicious interval marker will become from

untrustworthy to trustworthy and the running time counts again from 0. All the details updated to the latest time to read the value.

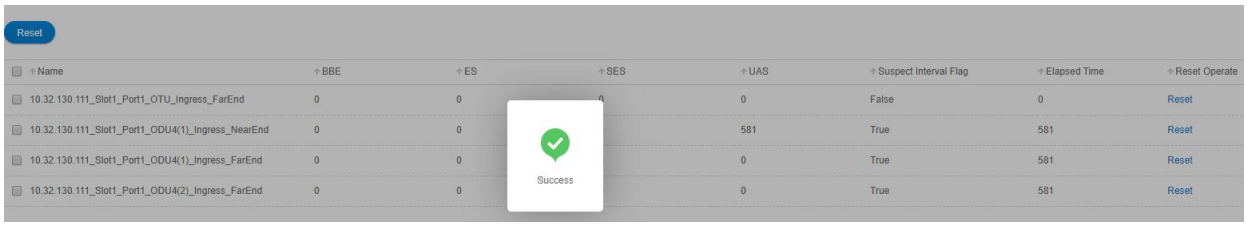



Figure9-42 OTUk/ODUk Successfully Reset

### 9.2.4.5. OTUk/ODUk Monitoring Data Shown As"-"

Here are the situations when the OTUk/ODUk monitoring data for the port is shown as -:

(1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.

(2) The port and the module are normal and the port is enabled.

(3) Optical module is inserted into the port but it is mismatched and the port is enabled.

At this time, all the data will be shown as -. The suspicious interval marker is trustworthy or untrustworthy (after 900/86400 seconds). The running time is normal and counts from 0, as shown in the figure below:

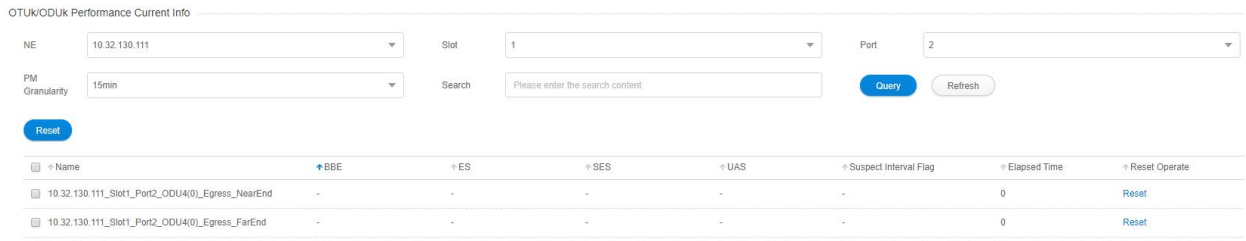



Figure9-43 Optical Module of OTUk/ODUk Not In Position

Here are the situations when the monitoring data for the board is shown as -:

(1) When the board is not in position or is pre-configured with an empty slot and the port for the board is enabled, all the data will be shown as -.The suspicious interval is marked as untrustworthy, and the running time is always 0 without any change, as shown in the figure below.

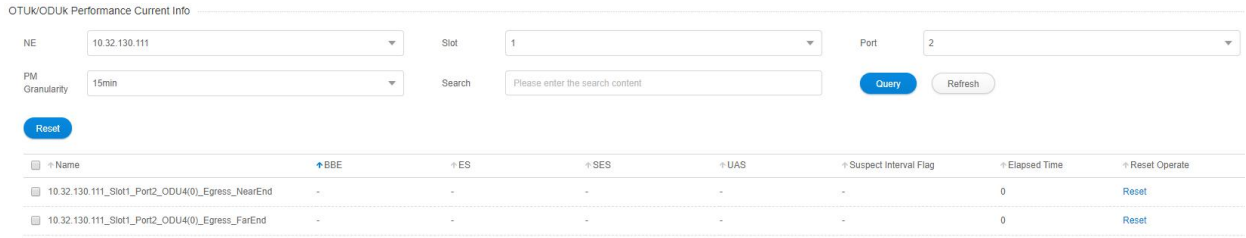



Figure9-44 OTUk/ODUk Monitoring Data

(2) When the board is mismatched and the port for the board is enabled, all the data will be shown as -. The suspicious interval is marked as untrustworthy, and the running time counts from 0 without any change, as shown in the figure below:

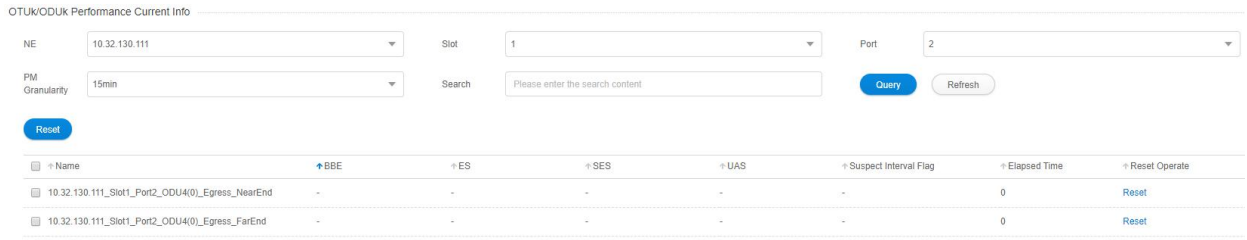



Figure9-45 OTUk/ODUk Monitoring Data When Mismatched

## 9.2.5. Current Performance Statistics of SDH Regeneration Segment

### 9.2.5.1. Monitoring Parameters Introduction of SDH Regeneration Segment

Monitoring parameters of SDH monitoring points include background error block (BBE), error second (ES), serious error second (SES), unavailable second (UAS), suspicious interval marker, runtime (S) and reset operation. Performance parameters of SDH will be enabled or disabled at the same time.

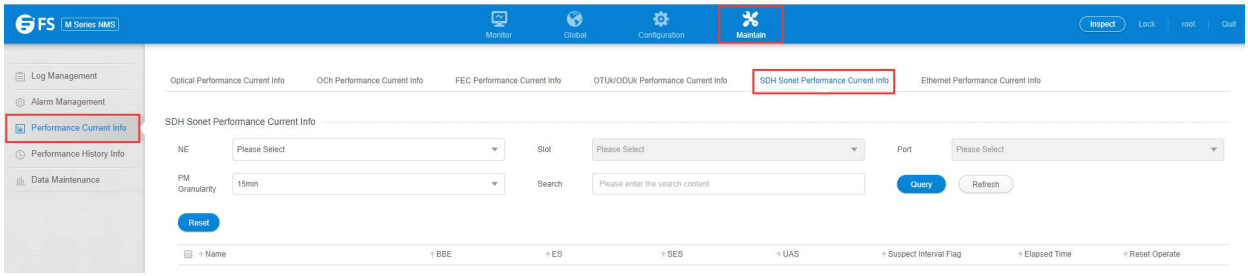



Figure9-46 Monitoring Parameters of SDH Regeneration Segment

### 9.2.5.2. View Monitoring Information of SDH Regeneration Segment

As shown in the figure, select the appropriate network elements, slots, ports and monitoring cycle through the selection box above the menu, the SDH value of a certain network element/slot/port will be displayed. The monitoring point of SDH only includes the near end, and the monitoring direction only includes entrance. (Generally, the client port which is not OTU is corresponding to exit of ODU. The monitoring direction of OTU and ODU for OTU port is entrance. Non-OTU means that the services of the port are not OTU2/OTU2e.)

Optical module is inserted into the monitoring port. SDH monitoring data which is currently read will be displayed. After the port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 900 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 15-minute data automatically becomes the history data.

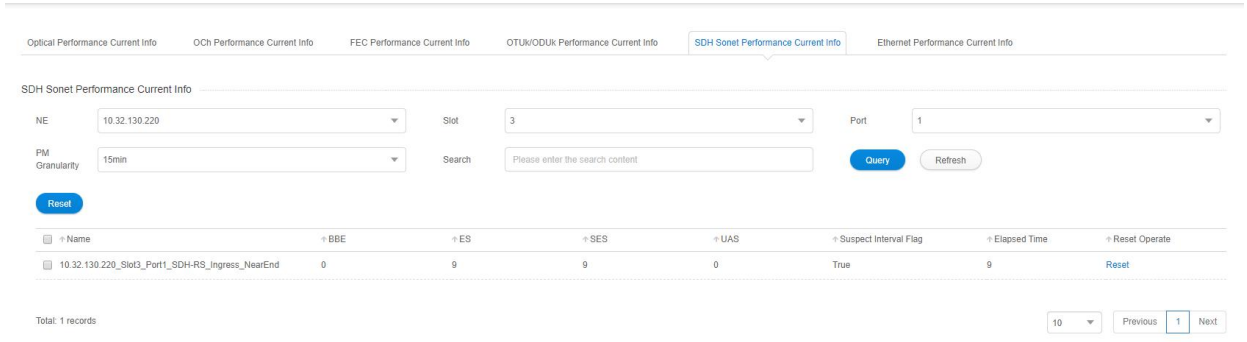



Figure9-47 15-Minute SDH Monitoring Data

Optical module is inserted into the monitoring port. SDH data which is currently read will be displayed. After the 24-hour performance monitoring port is enabled, the suspicious interval marker should be untrustworthy. The

running time counts from 0. After 86400 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 24-hour data automatically becomes the history data, as shown in the figure below:

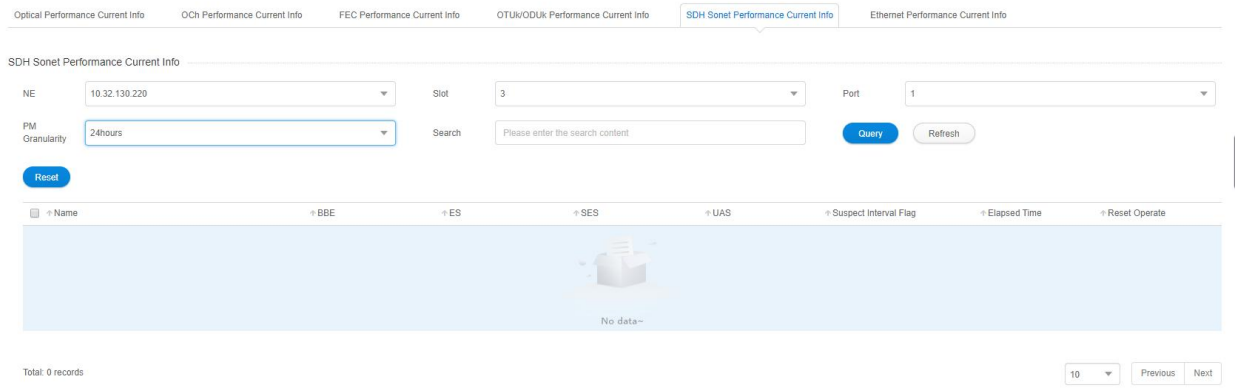



Figure9-48 24-Hour SDH Monitoring Data

### 9.2.5.3. SDH Regeneration Segment Monitoring Data Reset

When the current SDH monitoring data needs to be reset and to restart the monitoring, the 15-minute and 24-hour operation steps are the same. Taking 15-minute operation as an example, you can click on Reset behind each piece of monitoring record to perform resetting of a single piece of monitoring record, or you can select the first box to do batch resetting, as shown in the figure below.

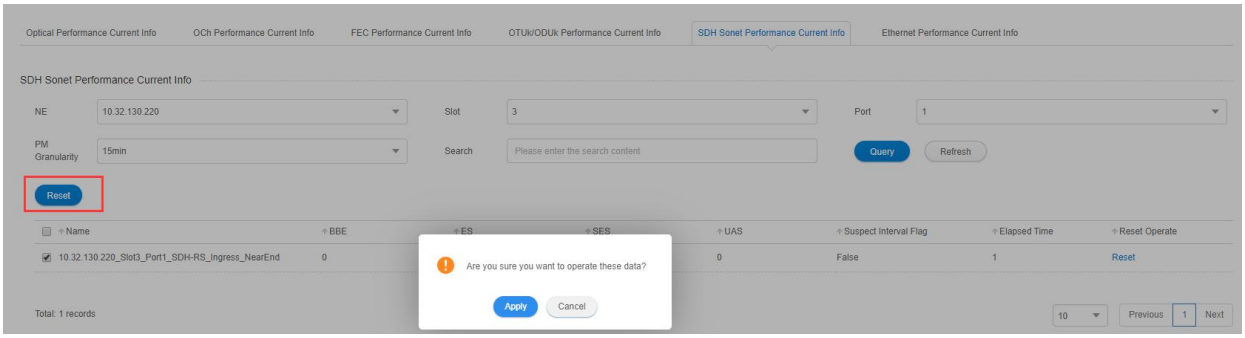



Figure9-49 SDH Regeneration Segment Reset

Then click on *Apply* button, as shown in the figure, it will show that the operation is successful. After that, click on *Refresh* button to refresh the whole page. At this time, the suspicious interval marker will become from untrustworthy to trustworthy and the running time counts again from 0. All the data is updated to the latest time to read the value.

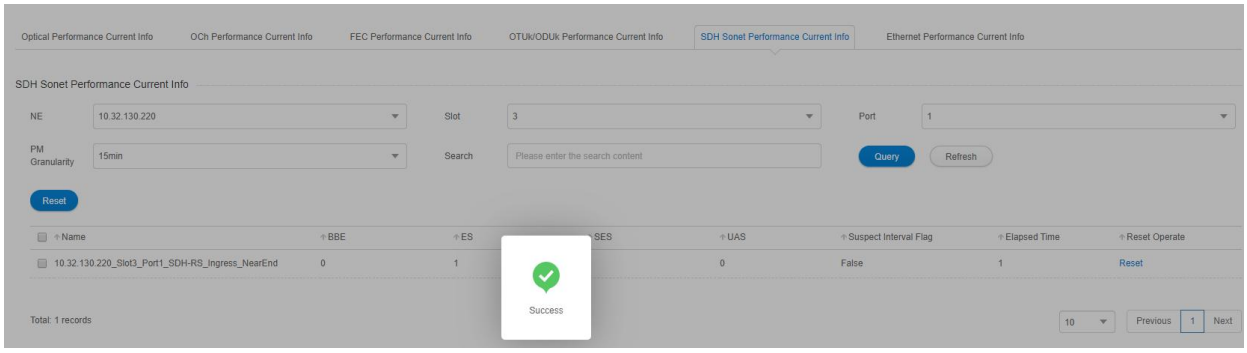



Figure9-50 SDH Regeneration Segment Successfully Reset

#### 9.2.5.4. Monitoring Data of SDH Regeneration Segment Shown As NA

Here are the situations when the monitoring data of the SDH regeneration segment for the port is shown as NA:

(1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.

(2) The port and the module are normal and the port is enabled.

(3) Optical module is inserted into the port but it is mismatched and the port is enabled.

At this time, all the data will be shown as NA. The suspicious interval marker is trustworthy (after 900/86400 seconds) or untrustworthy. The running time is normal and counts from 0, as shown in the figure below:

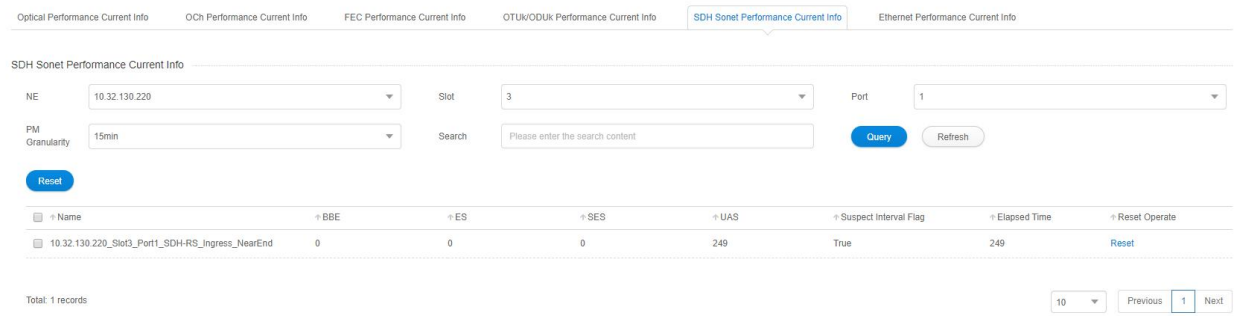



Figure9-51 Optical Module of SDH Regeneration Segment Not In Position

Here are the situations when the monitoring data for the board is shown as NA:

(1) When the board is not in position or is pre-configured with an empty slot and the port for the board is enabled, all the data will be shown as NA.The suspicious interval is marked as untrustworthy, and the running time is always 0 without any change, as shown in Figure 2.5-7:

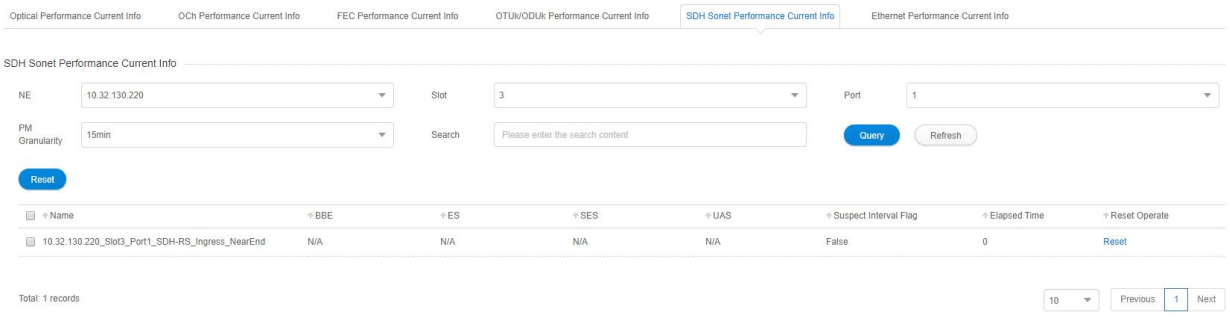



Figure9-52 SDH Regeneration Segment Monitoring Data

(2) When the board is mismatched and the port for the board is enabled, all the data will be shown as NA. The suspicious interval is marked as untrustworthy, and the running time counts from 0 without any change, as shown in Figure 2.5-8:

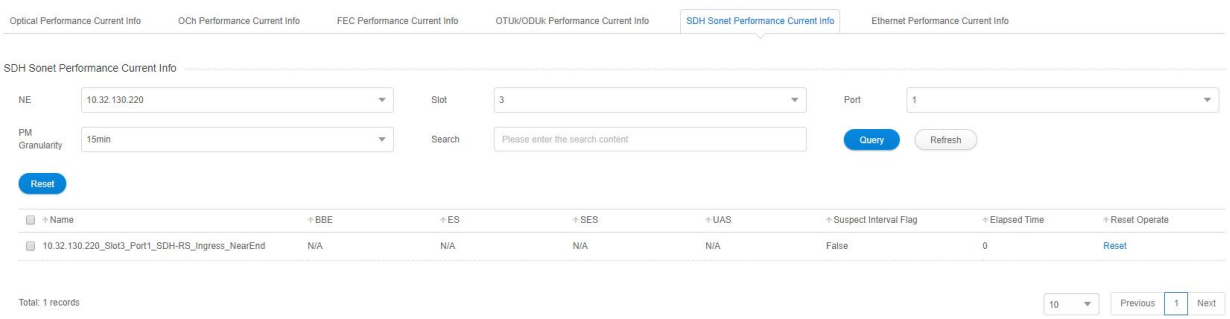


Figure9-53 Monitoring Data of SDH Regeneration Segment When Mismatched

## 9.2.6. Current Performance Statistics of Ethernet

### 9.2.6.1. Ethernet Monitoring Parameters Introduction

Monitoring parameters of Ethernet monitoring points include normal frame number, unicast frame number, multicast frame number, broadcast frame number, CRC error frame, alignment error frame number, ultra-long frame number (Frame Too Long), ultra-long Jabber frame number (CRC error), ultra-short frame number (CRC error), discarded frame number, ultra-short frame number (CRC normal), 64-byte frame number. 65-127 byte frame number, 128-255 byte frame number, 256-511 byte frame number, 512-1023 byte frame number, 1024-1518 byte frame number, 1519-maximum byte frame number, ultra-long frame number (CRC normal), normal pause frame number (Pause), total frame number, suspicious interval marker, running time (S) and reset operation. The performance parameters of Ethernet will be enabled or disabled at the same time.

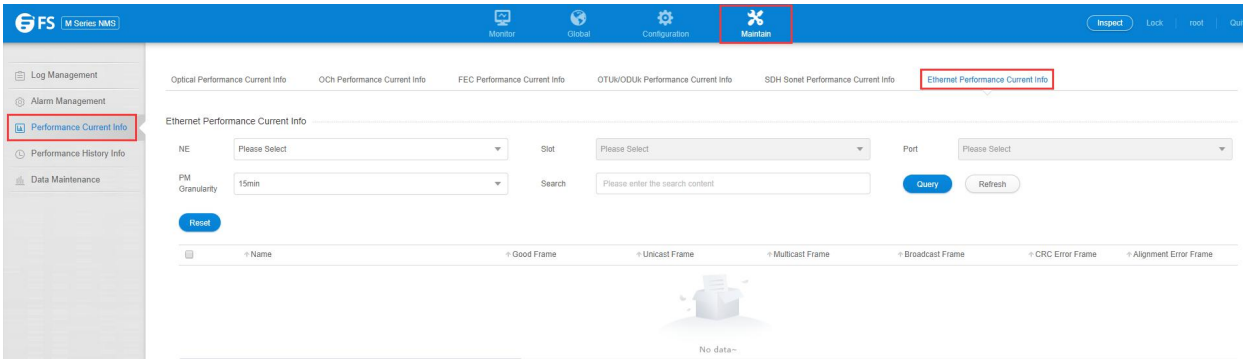



Figure9-54 Ethernet Monitoring Parameters

### 9.2.6.2. View Ethernet Monitoring Information

As shown in the figure, select the appropriate network elements, slots, ports and monitoring cycle through the selection box above the menu, the Ethernet value of a certain network element/slot/port will be displayed. The monitoring point of Ethernet only includes the near end, and currently the monitoring directions include entrance and exit. (Generally, the client port which is not OTU is corresponding to exit of ODU. The monitoring direction of OTU and ODU for OTU port is entrance. Non-OTU means that the services of the port are not OTU2/OTU2e.)

Optical module is inserted into the monitoring port. Ethernet monitoring data which is currently read will be displayed. After the port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 900 seconds, the suspicious interval marker will become trustworthy and the running time counts again from 0. The last 15-minute data automatically becomes the history data.

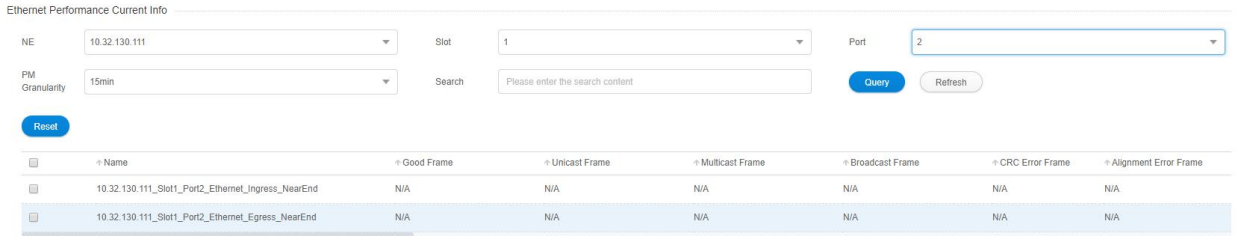



Figure9-55 15-Minute Ethernet Monitoring Data

Optical module is inserted into the monitoring port. Ethernet data which is currently read will be displayed. After the 24-hour performance monitoring port is enabled, the suspicious interval marker should be untrustworthy. The running time counts from 0. After 86400 seconds, the suspicious interval marker will

become trustworthy and the running time counts again from 0. The last 24-hour data automatically becomes the history data, as shown in the figure below:

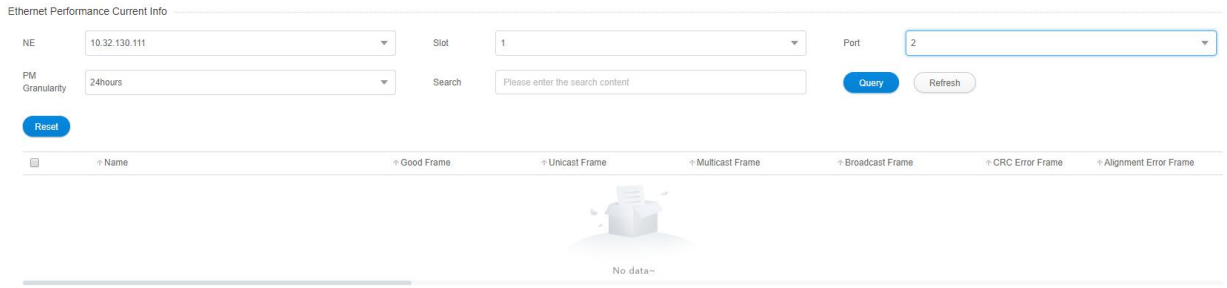



Figure9-56 24-Hour Ethernet Monitoring Data

### 9.2.6.3. Ethernet Monitoring Data Reset

When the current Ethernet monitoring data needs to be reset and to restart the monitoring, the 15-minute and 24-hour operation steps are the same. Taking 15-minute operation as an example, you can click on Reset behind each piece of monitoring record to perform resetting of a single piece of monitoring record, or you can select the first box to do batch resetting, as shown in the figure below:

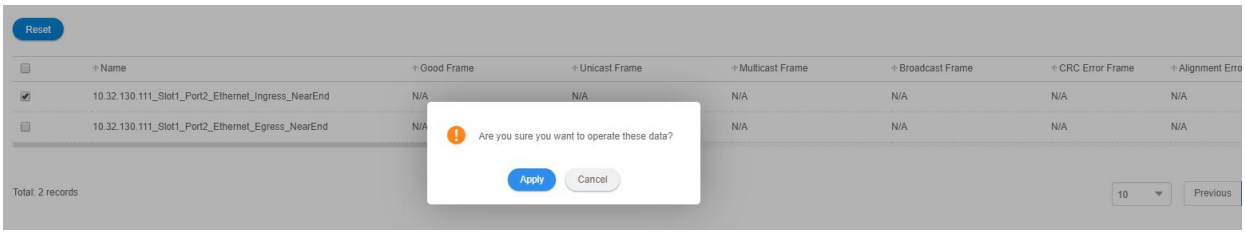



Figure9-57 Ethernet Reset

Then click on *Apply* button, as shown in the figure, it will show that the operation is successful. After that, click on *Refresh* button to refresh the whole page. At this time, the suspicious interval marker will become from untrustworthy to trustworthy and the running time counts again from 0. All the data is updated to the latest time to read the value.

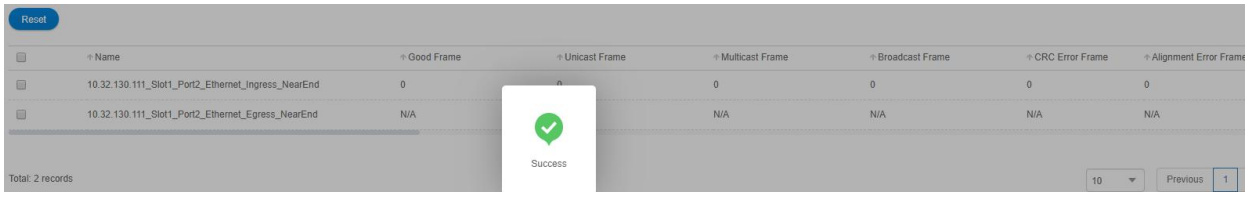



Figure9-58 Ethernet Successfully Reset

### 9.2.6.4. Ethernet Monitoring Data Shown As NA

Here are the situations when the Ethernet for the port is shown as NA:

(1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.

(2) The port and the module are normal and the port is enabled.

(3) Optical module is inserted into the port but it is mismatched and the port is enabled.

At this time, all the data will be shown as NA. The suspicious interval marker is trustworthy (after 900/86400 seconds) or untrustworthy. The running time is normal and counts from 0, as shown in the figure below:

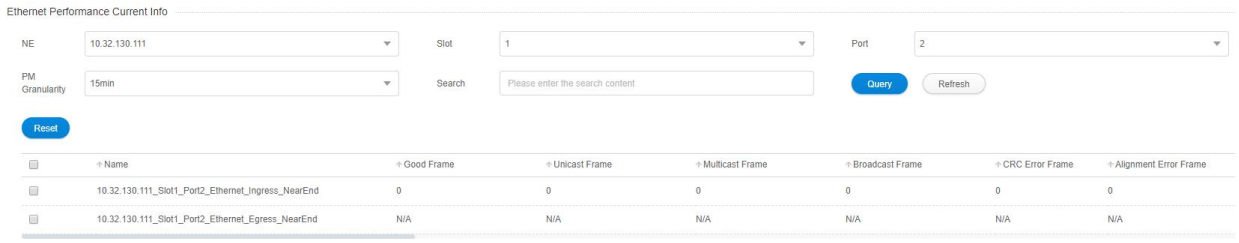



Figure9-59 Optical Module of Ethernet Not In Position

Here are the situations when the monitoring data for the board is shown as NA:

(1) When the board is not in position or is pre-configured with an empty slot and the port for the board is enabled, all the data will be shown as NA.The suspicious interval is marked as untrustworthy, and the running time is always 0 without any change, as shown in figure below:

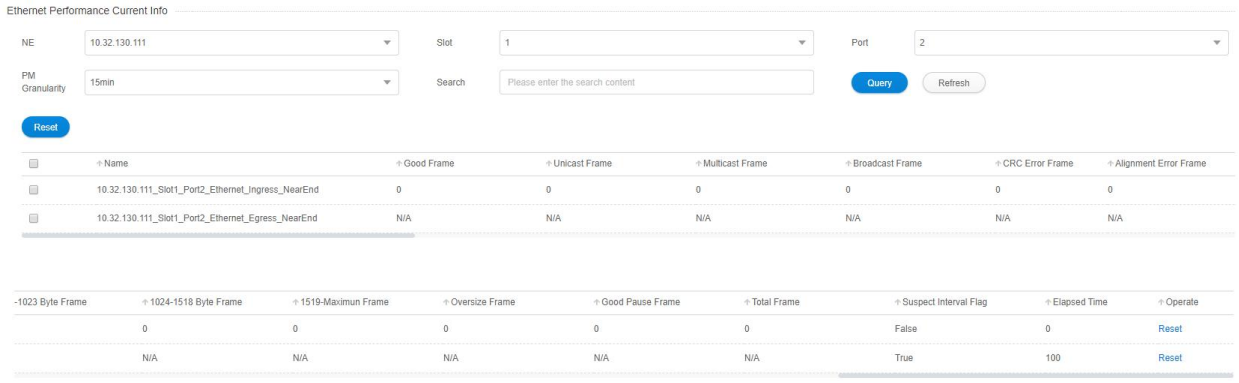



Figure9-60 Ethernet Monitoring Data

(2) When the board is mismatched and the port for the board is enabled, all the data will be shown as NA. The suspicious interval is marked as untrustworthy, and the running time counts from 0 without any change, as shown in the figure below:

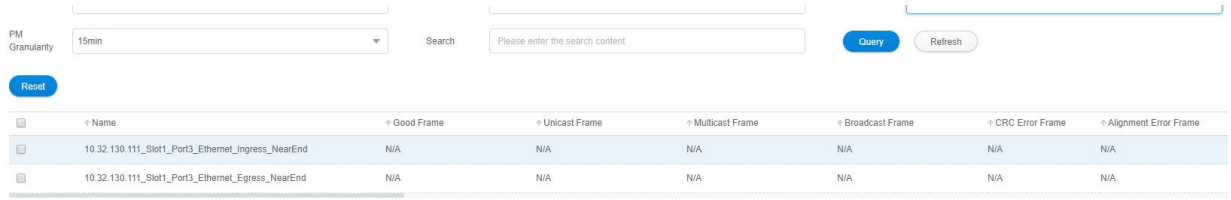



Figure9-61 Ethernet Monitoring Data When Mismatched

# 9.3. History Performance Statistics

## 9.3.1. History Performance Statistics of Optical Power

### 9.3.1.1. History Monitoring Parameters Introduction of Optical Power

The monitoring parameter of the history monitoring point for optical power includes time interval, which is a shortcut to choose the time. There are three options--one day, three days and a week for you to choose.

Duration: You can choose a specific day or a period of time according to your needs.

Performance Monitoring Point: entrance-near end, exit-near end.

Performance Monitoring Parameters: maximum optical power, minimum optical power, average optical power.

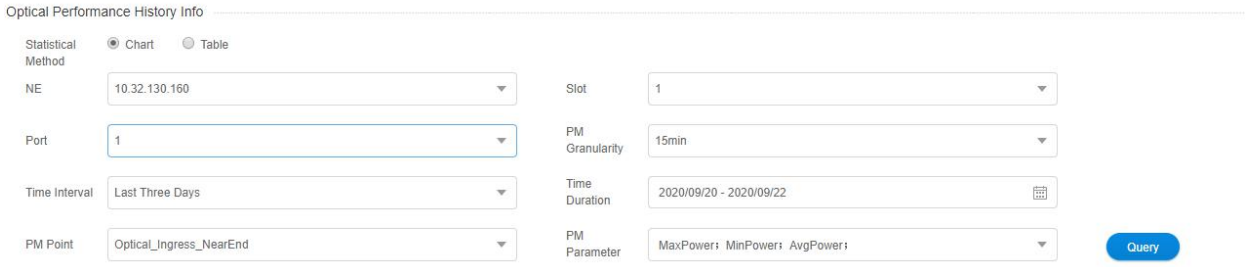



Figure9-62 History Performance Parameters of Optical Power

### 9.3.1.2. View History Monitoring Information of Optical Power

15minutes and 24hours of optical power history data operation and display are the same form. Here we take 15-minute optical power history monitoring point as an example. Choose the appropriate network elements, slots, ports and monitoring cycles through the screening box above the menu, and then select the time interval, performance monitoring point and parameters which need to be monitored in the right menu. The maximum optical power, minimum optical power and average optical power can be all selected or only select one or two of them to check.After that, click Apply button on the lower right corner. From the graph, we can see the trend of the refraction chart of the maximum, minimum and average optical power. The ordinate represents the value of the optical power, and the abscissa represents the time. Data which has been read for more than 15 minutes will be automatically transferred from current statistics to history statistics.

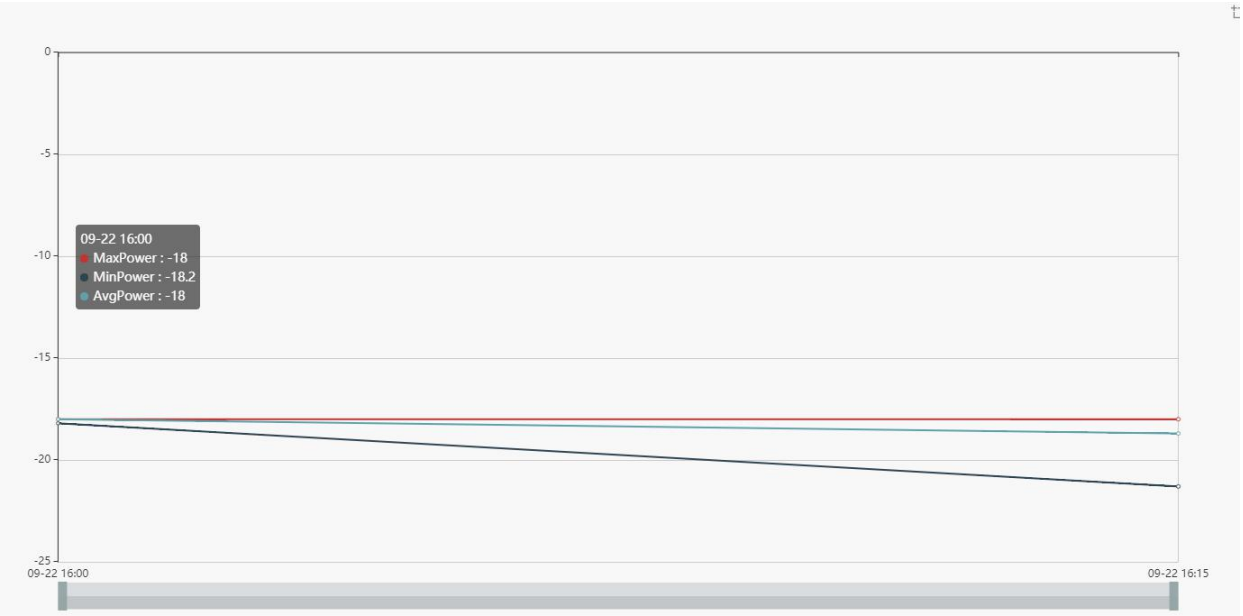



Figure9-63 15-Minute Chart Data of Optical Power

History performance statistics of optical power also show history data in tabular form. Click on the table, the interface as shown in the figure below appears:

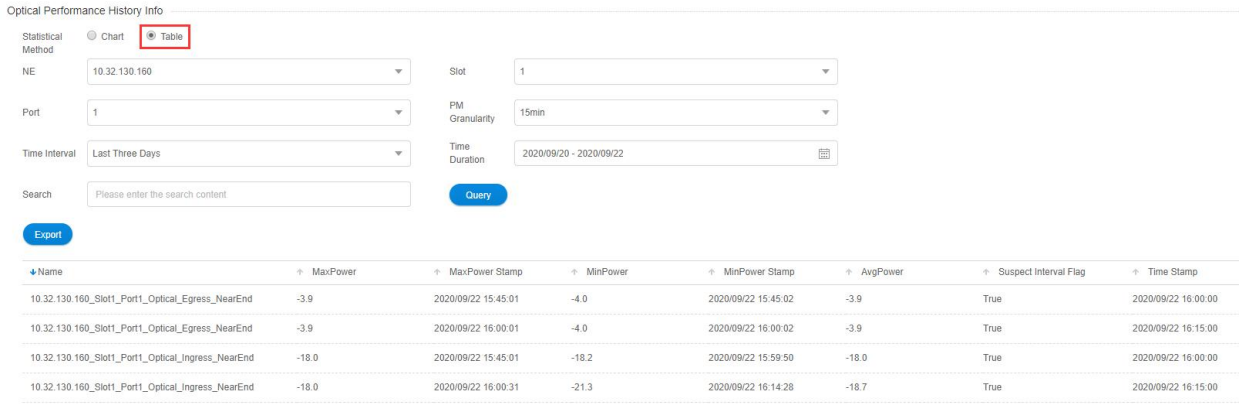



Figure9-64 15-Minute Tabular Interface of Optical Power

Click the time interval shortcut in the right menu or select the required time interval in Duration, and then click on Apply button in the lower right corner, the history data of all the optical power records on this port will be displayed, as shown in the figure below:

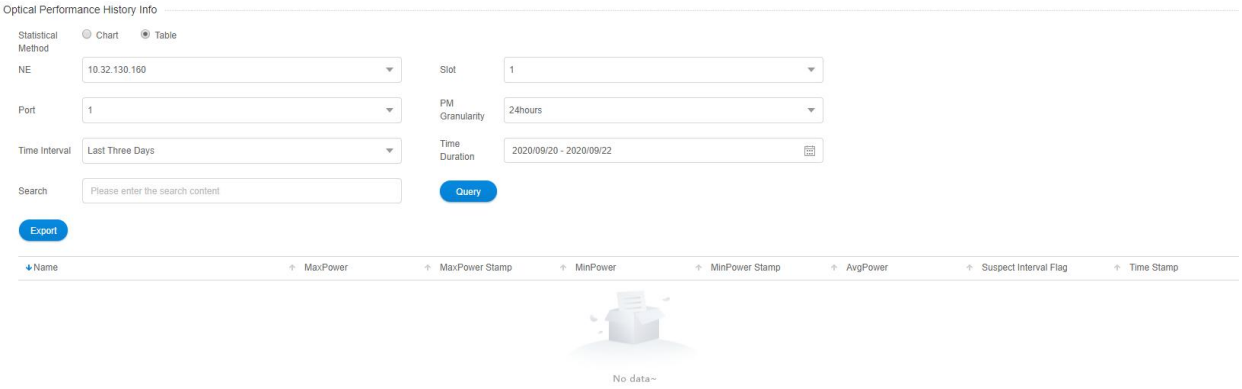



Figure9-65 15-Minute Tabular History Data of Optical Power

### 9.3.1.3. Export History Monitoring Information of Optical Power

To save the history data, you can click on the upper Export button, and an interface will pop up, as shown in the figure below:

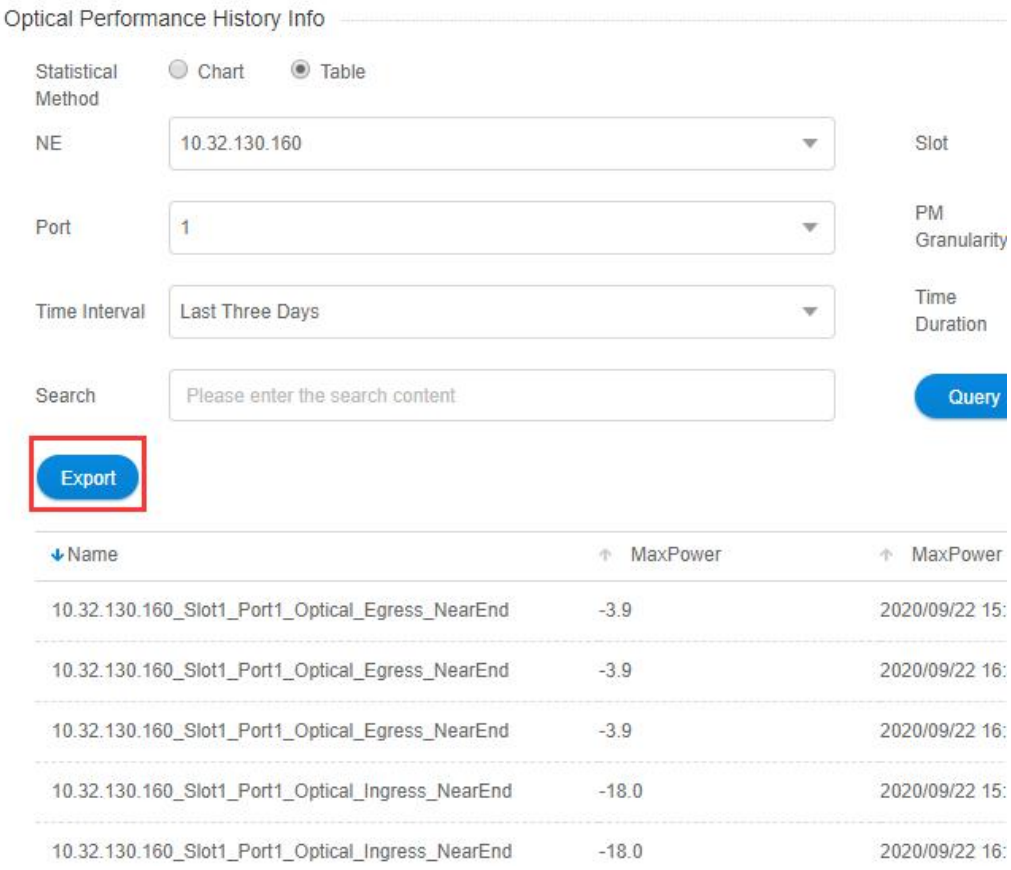



Figure9-66 Export History Data of Optical Power

Any character such as English, Chinese, alphabet or number can be entered as the file name, and then click on Apply button, it will prompt that the export is successful, as shown in the figure below:

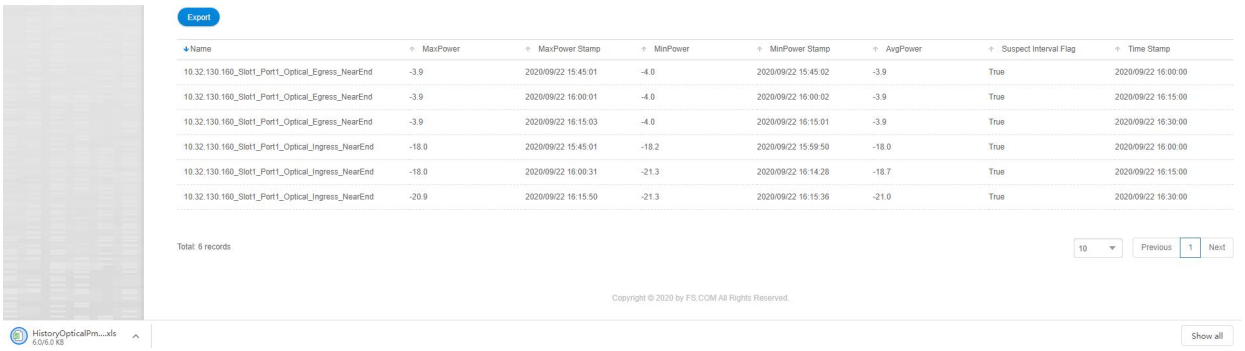



Figure9-67 Successfully Export Data of Optical Power

## 9.3.2. OCh History Performance Statistics

### 9.3.2.1. OCh History Monitoring Parameters Introduction

The monitoring parameter of the history monitoring point for OCh includes time interval, which is a shortcut to choose the time. There are three options--one day, three days and a week for you to choose.

Duration: You can choose a specific day or a period of time according to your needs.

Performance Monitoring Point: entrance-near end.

Performance Monitoring Parameters: maximum differential group delay (DGD), minimum differential group delay (DGD), average differential group delay (DGD), maximum chromatic dispersion (CD), minimum chromatic

dispersion (CD), average chromatic dispersion (CD), maximum optical signal-to-noise ratio (OSNR), minimum optical signal-to-noise ratio (OSNR), average optical signal-to-noise ratio (OSNR).

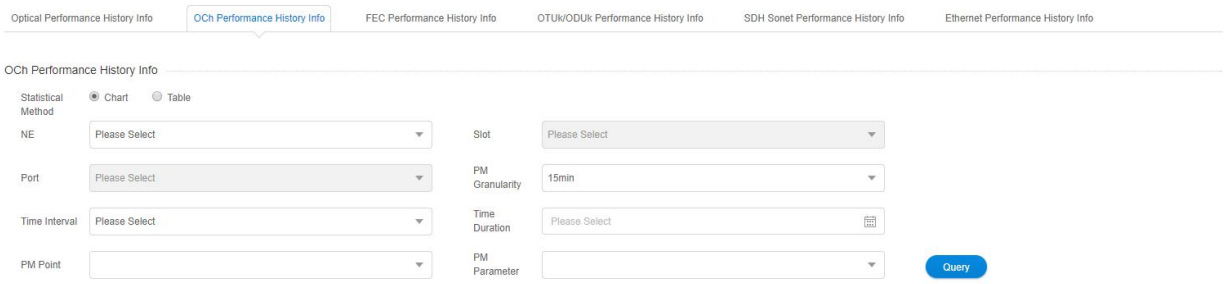



Figure9-68 OCh History Performance Parameters

### 9.3.2.2. View OCh History Monitoring Information

15minutes and 24hours of OCh history data operation and display are the same form. Here we take 15-minute OCh history monitoring point as an example. Choose the appropriate network elements, slots, ports and monitoring cycles through the screening box above the menu, and then select the time interval, performance monitoring point and parameters which need to be monitored in the right menu.Parameters to be monitored can be all selected or only select one or two of them to check.After that, click Apply button on the lower right corner. From the graph, we can see the trend of the refraction chart of the monitoring parameters. The ordinate represents the value of the monitoring data, and the abscissa represents the time. Data which has been read for more than 15 minutes will be automatically transferred from current statistics to history statistics.

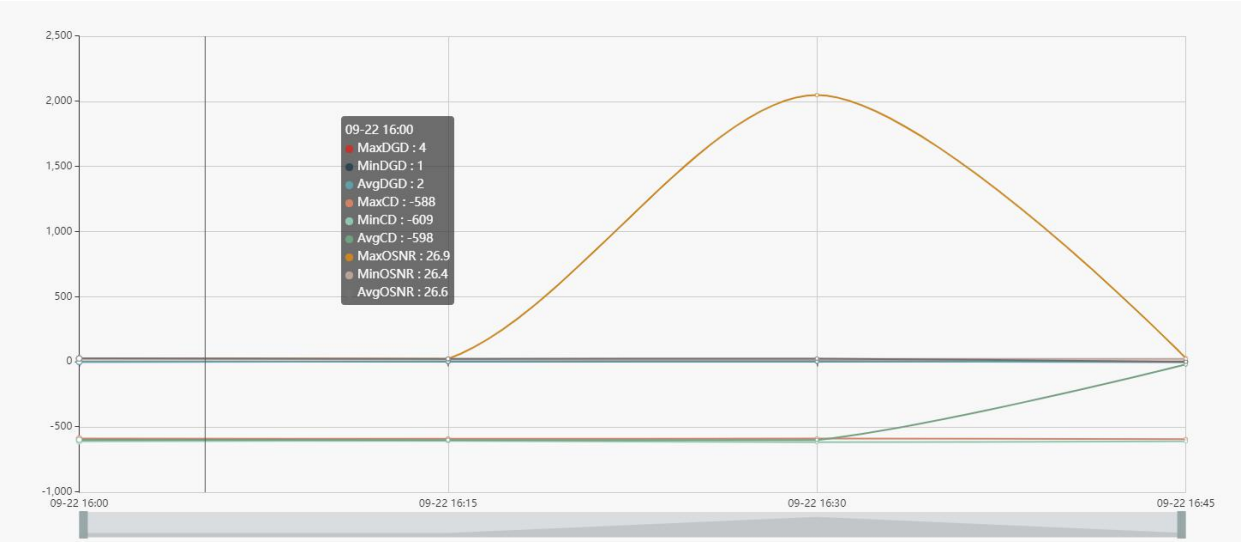



Figure9-69 15-Minute Chart Data of OCh

History performance statistics of OCh also show history data in tabular form. Click on the table, the interface as shown in the figure below appears:

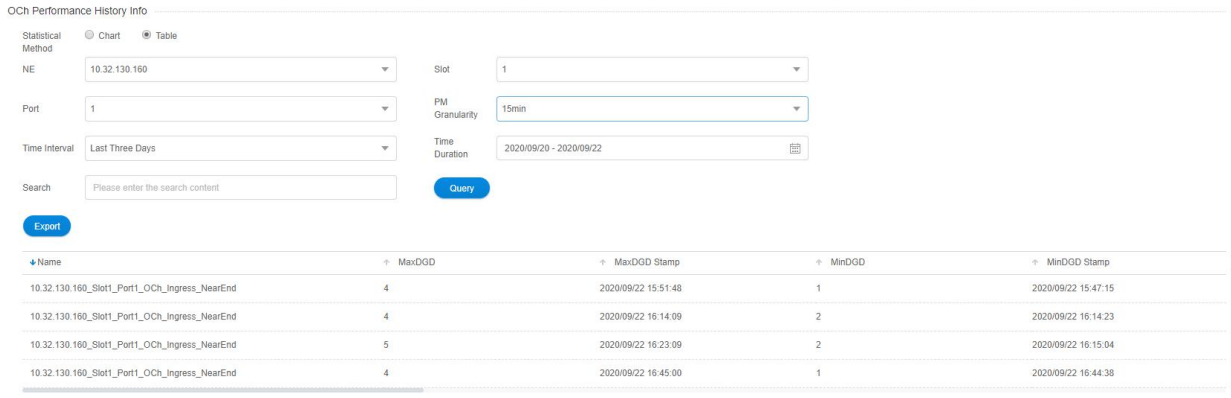



Figure9-70 15-Minute Tabular Interface of OCh

Click the time interval shortcut in the right menu or select the required time interval in Duration, and then click on Apply button in the lower right corner, the history data of all the OCh records on this port will be displayed, as shown in the figure below:

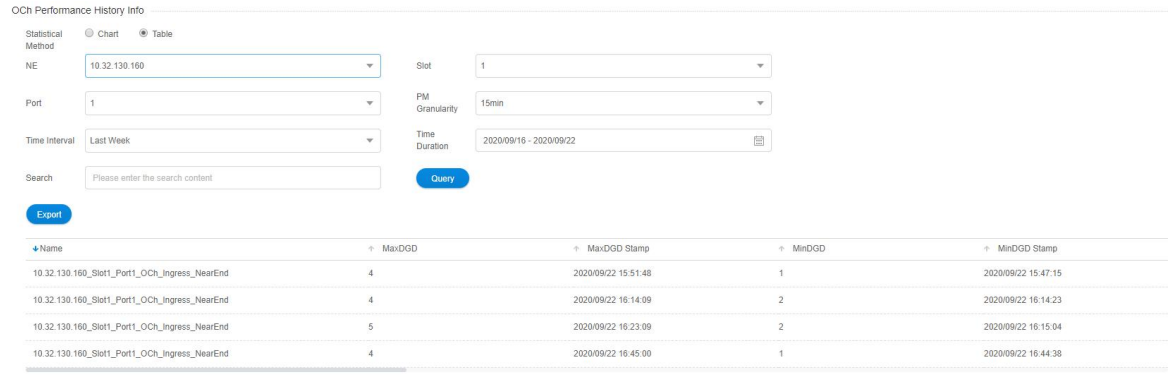
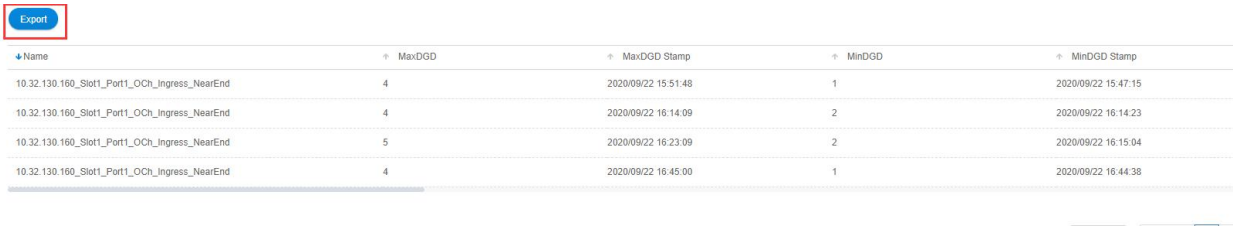



Figure9-71 15-Minute Tabular History Data of OCh

### 9.3.2.3. Export OCh History Monitoring Information

To save the history data, you can click on the

upp




er Export button, and an interface will pop up, as shown in the figure below:

Figure9-72 Export History Data of OCh

Any character such as English, Chinese, alphabet or number can be entered as the file name, and then click on Apply button, it will prompt that the export is successful, as shown in the figure below:

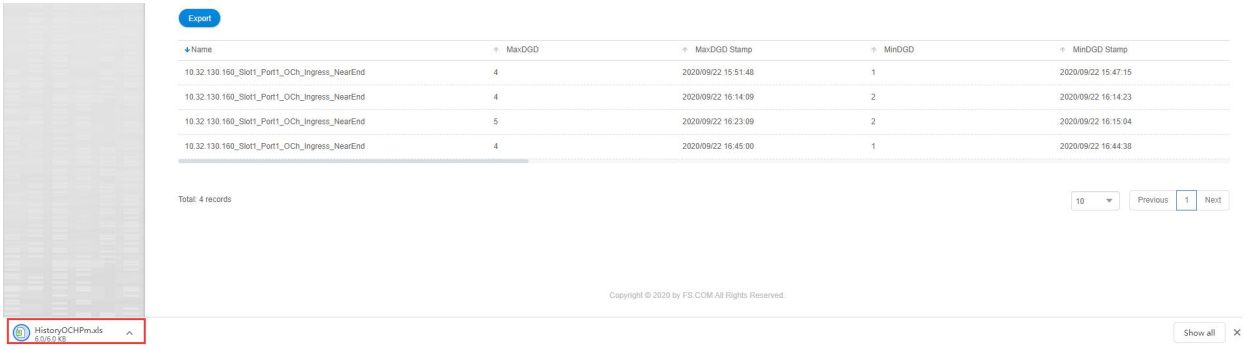



Figure9-73 Successfully Export Data of OCh

## 9.3.3. FEC History Performance Statistics

### 9.3.3.1. FEC History Monitoring Parameters Introduction

The monitoring parameter of the history monitoring point for FEC includes time interval, which is a shortcut to choose the time. There are three options--one day, three days and a week for you to choose.

Duration: You can choose a specific day or a period of time according to your needs.

Performance Monitoring Point: entrance-near end.

Performance Monitoring Parameters: maximum error correction rate and average error correction rate.

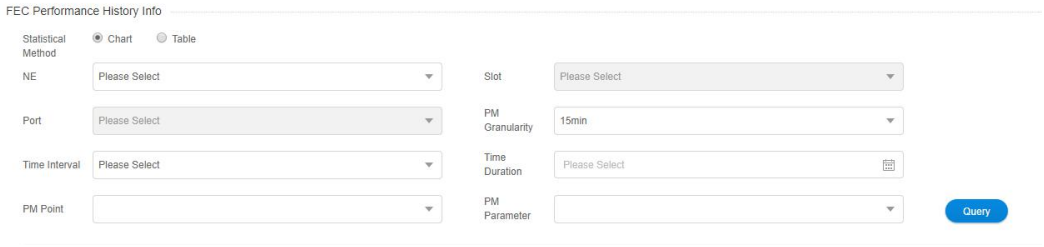



Figure9-74 FEC History Performance Parameters

### 9.3.3.2. View FEC History Monitoring Information

15minutes and 24hours of FEC history data operation and display are the same form. Here we take 15-minute FEC history monitoring point as an example. Choose the appropriate network elements, slots, ports and monitoring cycles through the screening box above the menu, and then select the time interval, performance monitoring point and parameters which need to be monitored in the right menu.Parameters to be monitored can be all selected or only select one or two of them to check.After that, click Apply button on the lower right corner. From the graph, we can see the trend of the refraction chart of the monitoring parameters. The ordinate represents the value of the monitoring data, and the abscissa represents the time. Data which has been read for more than 15 minutes will be automatically transferred from current statistics to history statistics.

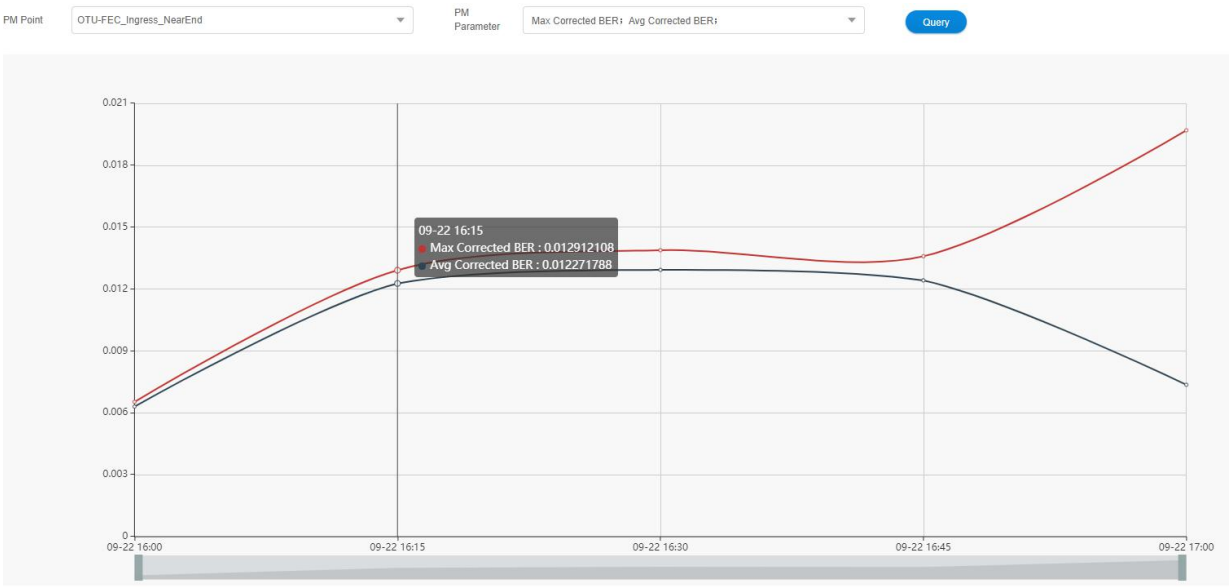



Figure9-75 15-Minute Chart Data of FEC

History performance statistics of FEC also show history data in tabular form. Click on the table, the interface as shown in the figure below appears:

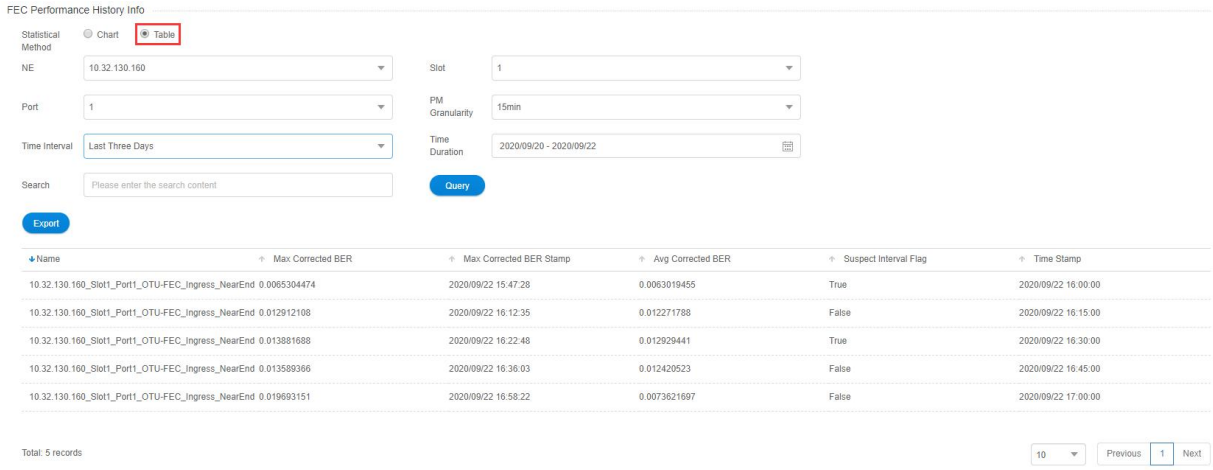



Figure9-76 15-Minute Tabular Interface of FEC

Click the time interval shortcut in the right menu or select the required time interval in Duration, and then click on Apply button in the lower right corner, the history data of all FEC monitoring points on this port will be displayed, as shown in the figure below:

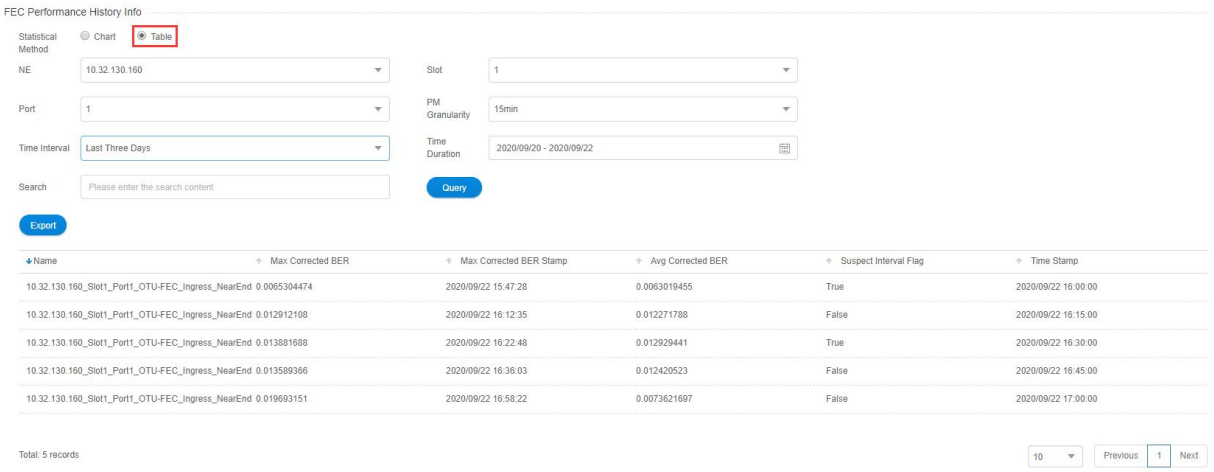



Figure9-77 15-Minute Tabular History Data of FEC

#### 9.3.3.3. Export FEC History Monitoring Information

To save the history data, you can click on the upper Export button, and an interface will pop up, as shown in the figure below:

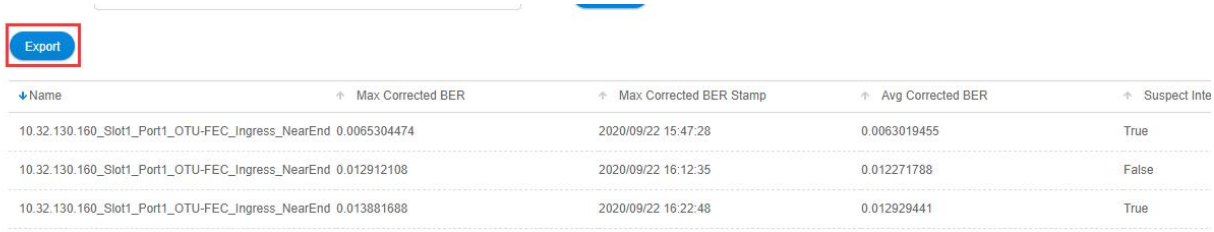



Figure9-78 Export History Data of FEC

Any character such as English, Chinese, alphabet or number can be entered as the file name, and then click on Apply button, it will prompt that the export is successful, as shown in the figure below:

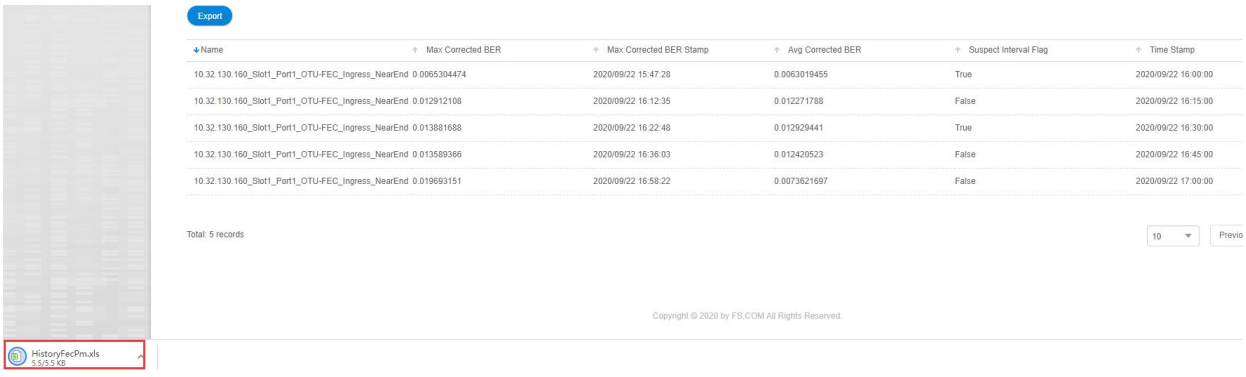



Figure9-79 Successfully Export Data of FEC

## 9.3.4. OTUk/ODUk History Performance Statistics

### 9.3.4.1. OTUk/ODUk History Monitoring Parameters Introduction

The monitoring parameter of the history monitoring point for OTUk/ODUk includes time interval, which is a shortcut to choose the time. There are three options--one day, three days and a week for you to choose.

Duration: You can choose a specific day or a period of time according to your needs.

Performance Monitoring Point: There are near end and far end, as well as entrance and exit for OTUk/ODUk monitoring points.

Performance Monitoring Parameters: background error code block (BBE), bit error seconds (ES), serious bit error seconds (SES) and unavailable seconds.

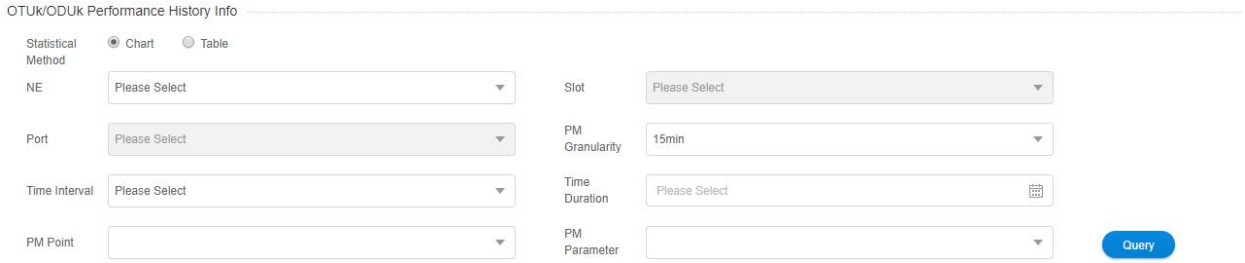



Figure9-80 OTUk/ODUk History Performance Parameters

### 9.3.4.2. View OTUk/ODUk History Monitoring Information

15minutes and 24hours of OTUk/ODUk history data operation and display are the same form. Here we take 15-minute OTUk/ODUk history monitoring point as an example. Choose the appropriate network elements, slots, ports and monitoring cycles through the screening box above the menu, and then select the time interval, performance monitoring point and parameters which need to be monitored in the right menu.Parameters to be monitored can be all selected or only select one or two of them to check.After that, click Apply button on the lower right corner. From the graph, we can see the trend of the refraction chart of the monitoring parameters. The ordinate represents the value of the monitoring data, and the abscissa represents the time. Data which has been read for more than 15 minutes will be automatically transferred from current statistics to history statistics.

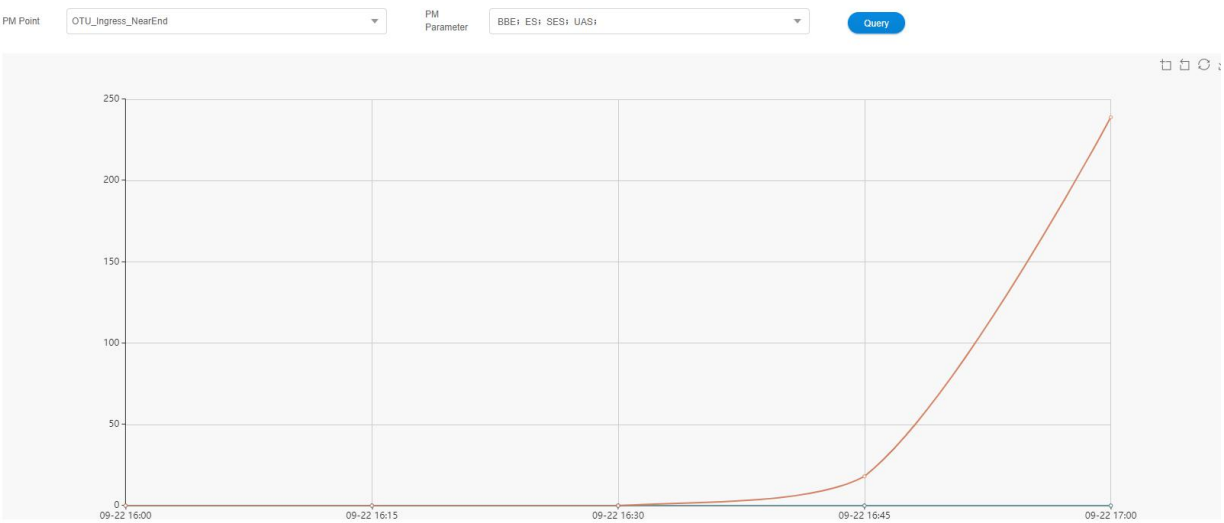



Figure9-81 15-Minute Chart Data of OTUk/ODUk

History performance statistics of OTUk/ODUk also show history data in tabular form. Click on the table, the interface as shown in the figure below appears:

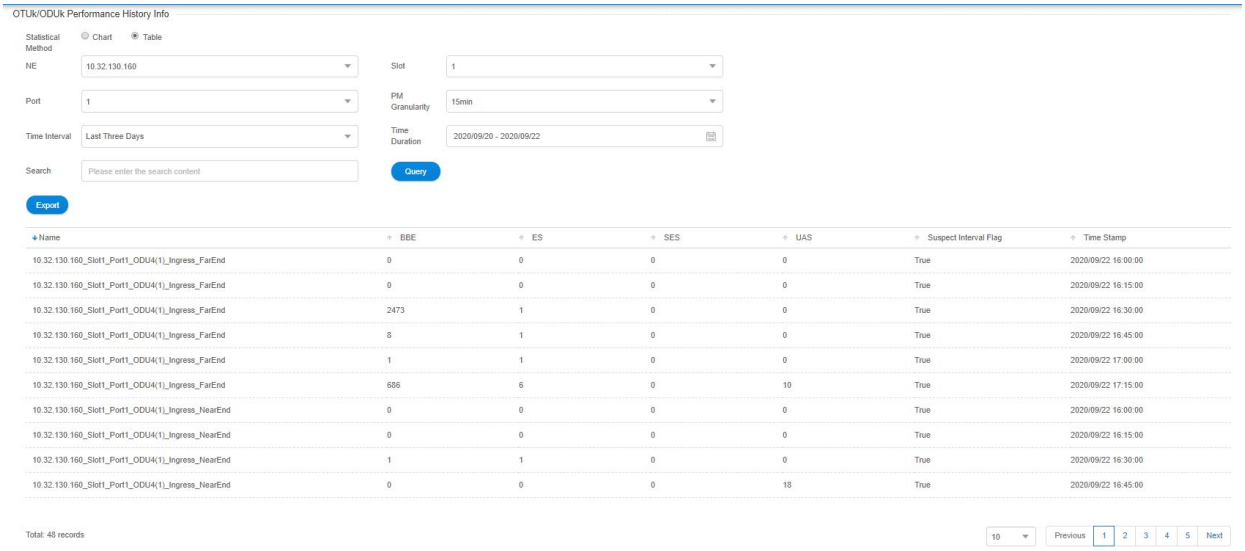



Figure9-82 15-Minute Tabular Interface of OTUk/ODUk

Click the time interval shortcut in the right menu or select the required time interval in Duration, and then click on Apply button in the lower right corner, the history data of all OTUk/ODUk monitoring points on this port will be displayed, as shown in the figure below:

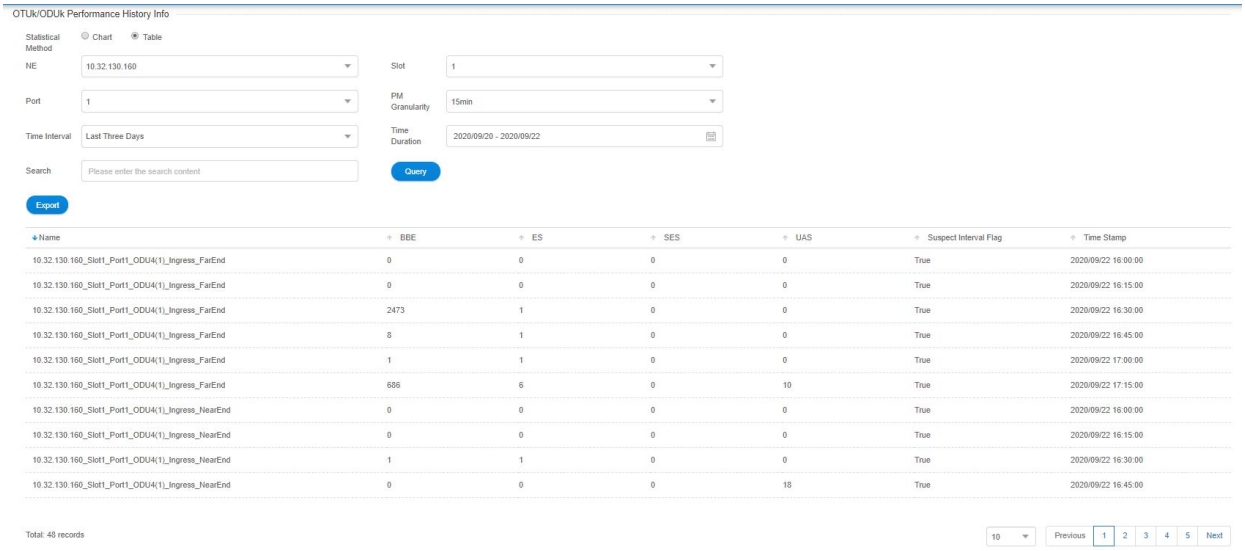



Figure9-83 15-Minute Tabular History Data of OTUk/ODUk

### 9.3.4.3. Export OTUk/ODUk History Monitoring Information

To save the history data, you can click on the upper Export button, and an interface will pop up, as shown in the figure below:


Figure9-84 Export History Data of OTUk/ODUk

Any character such as English, Chinese, alphabet or number can be entered as the file name, and then click on Apply button, it will prompt that the export is successful, as shown in the figure below:

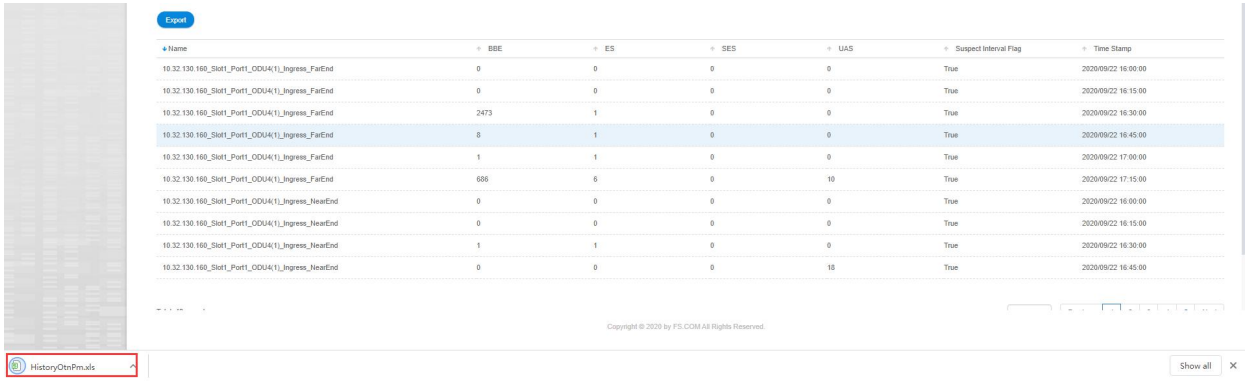



Figure9-85 Successfully Export Data of OTUk/ODUk

## 9.3.5. History Performance Statistics of SDH Regeneration Segment

### 9.3.5.1. History Monitoring Parameters Introduction of SDH Regeneration Segment

The monitoring parameter of the history monitoring point for SDH regeneration segment includes time interval, which is a shortcut to choose the time. There are three options--one day, three days and a week for you to choose.

Duration: You can choose a specific day or a period of time according to your needs.

Performance Monitoring Point: entrance-near end.

Performance Monitoring Parameters: background error code block (BBE), bit error seconds (ES), serious bit error seconds (SES) and unavailable seconds.

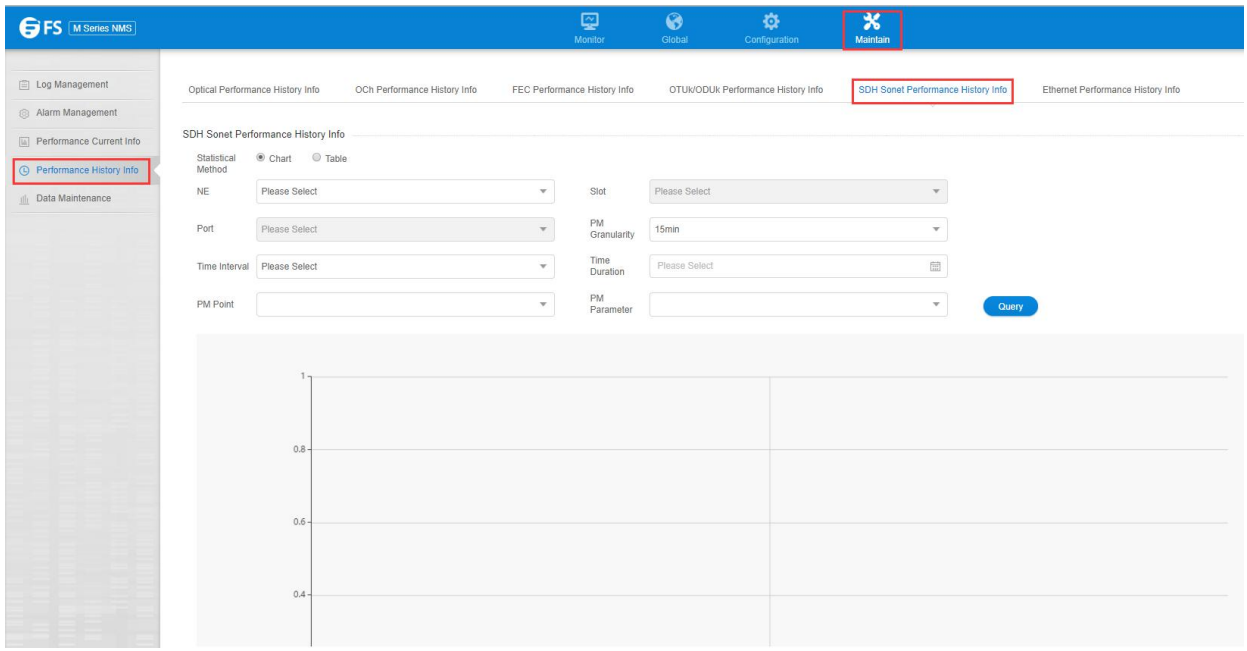



Figure9-86 SDH Regeneration Segment History Performance Parameters

### 9.3.5.2. View SDH Regeneration Segment History Monitoring Information

15minutes and 24hours of SDH regeneration segment history data operation and display are the same form. Here we take 15-minute history monitoring point for the SDH regeneration segment as an example. Choose the appropriate network elements, slots, ports and monitoring cycles through the screening box above the menu,

and then select the time interval, performance monitoring point and parameters which need to be monitored in the right menu.Parameters to be monitored can be all selected or only select one or two of them to check.After that, click Apply button on the lower right corner. From the graph, we can see the trend of the refraction chart of the monitoring parameters. The ordinate represents the value of the monitoring data, and the abscissa represents the time. Data which has been read for more than 15 minutes will be automatically transferred from current statistics to history statistics.

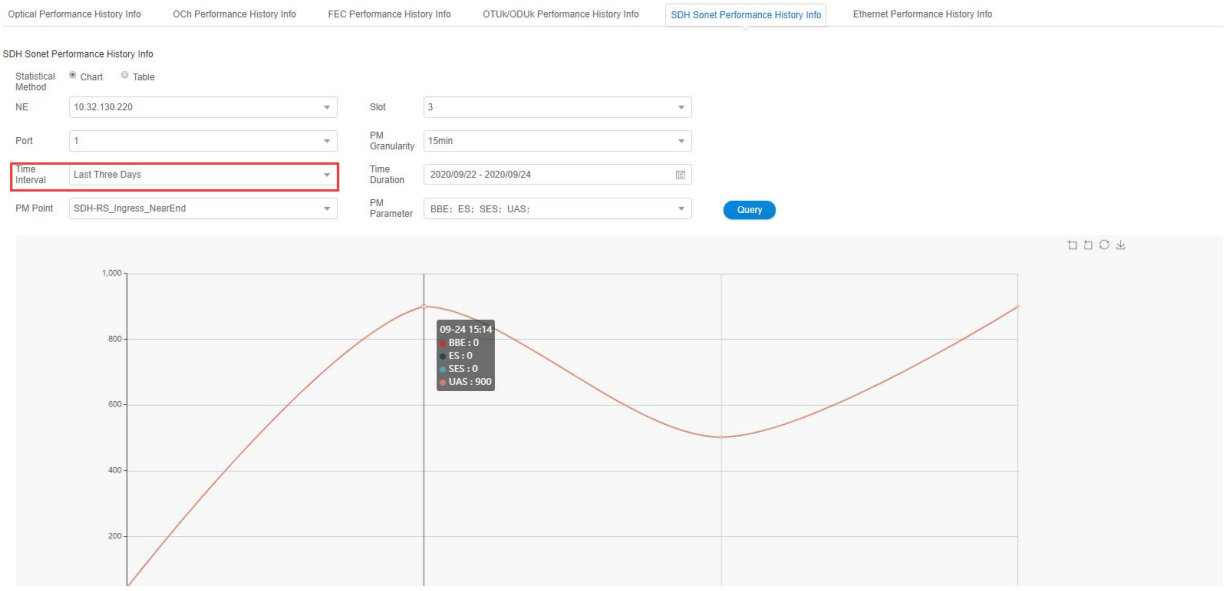



Figure9-87 15-Minute Chart Data of SDH Regeneration Segment

History performance statistics of SDH regeneration segment also show history data in tabular form. Click on the table, the interface as shown in the figure below appears:

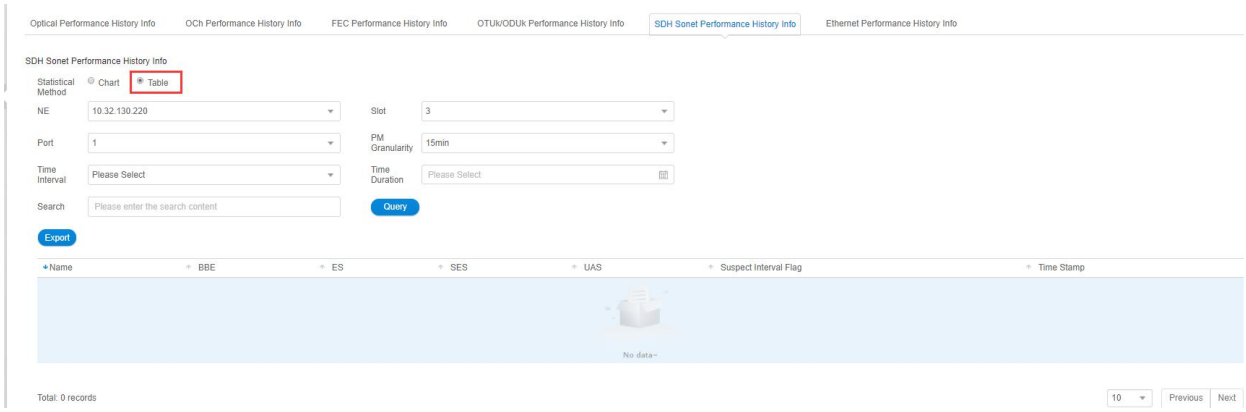



Figure9-88 15-Minute Tabular Interface of SDH Regeneration Segment

Click the time interval shortcut in the right menu or select the required time interval in Duration, and then click on Apply button in the lower right corner, the history data of all SDH regeneration segment monitoring points on this port will be displayed, as shown in the figure below:

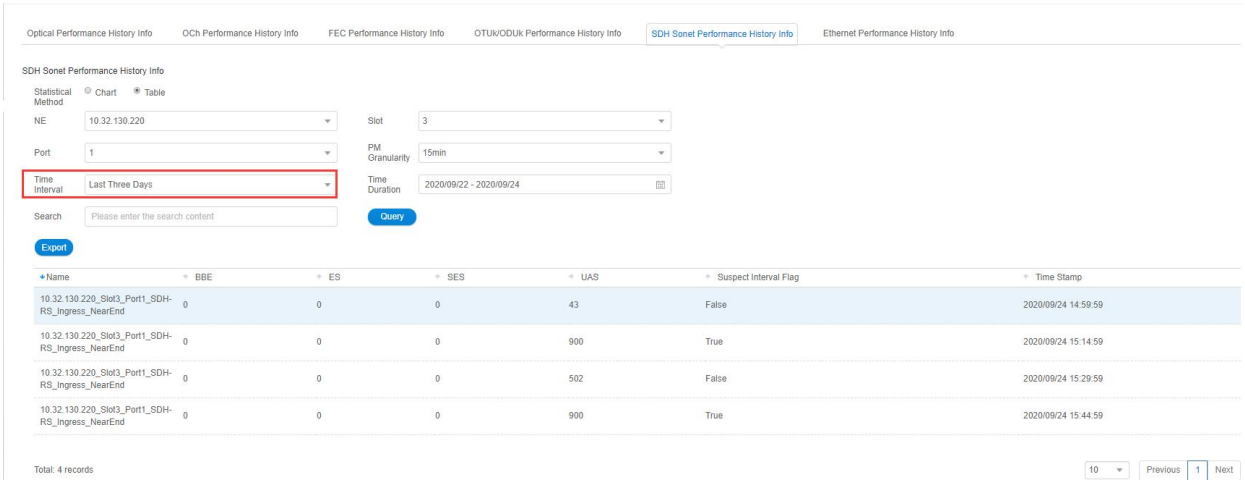



Figure9-89 15-Minute Tabular History Data of SDH Regeneration Segment

### 9.3.5.3. Export SDH Regeneration Segment History Monitoring Information

To save the history data, you can click on the Export button, and an interface will pop up, as shown in the figure below:

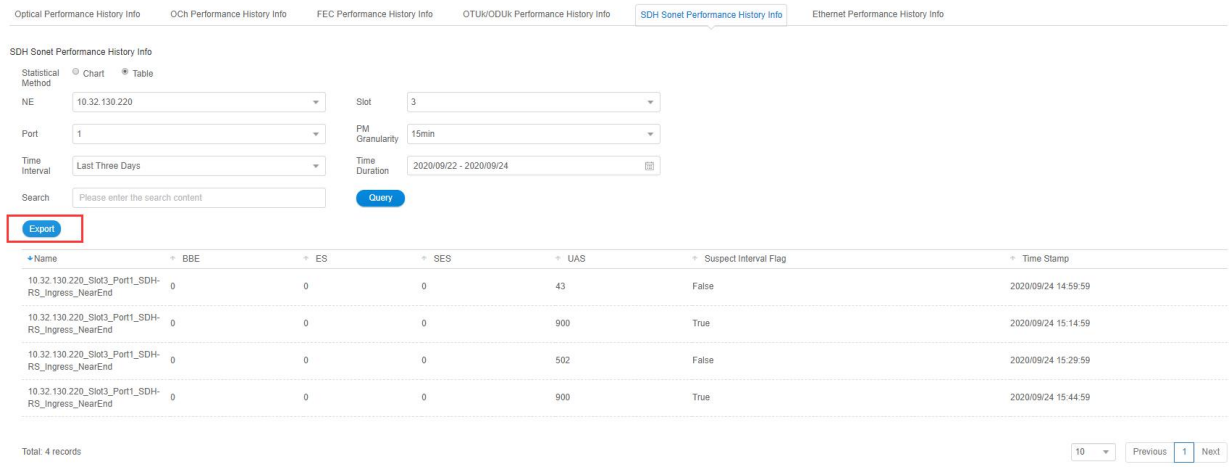



Figure9-90 Export History Data of SDH Regeneration Segment

After click on export, the download file default name is HistorySdhPm.xls as shown in the figure below:

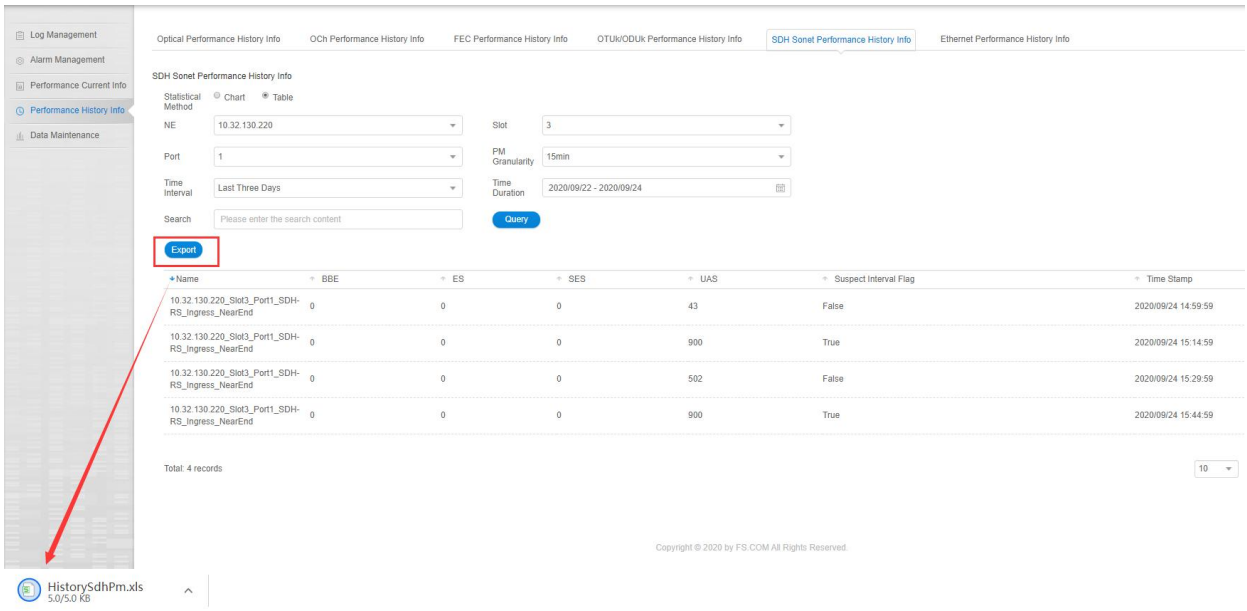



Figure9-91 Successfully Export Data of SDH Regeneration Segment

## 9.3.6. History Performance Statistics of Ethernet

### 9.3.6.1. Ethernet History Monitoring Parameters Introduction

The monitoring parameter of the history monitoring point for Ethernet includes time interval, which is a shortcut to choose the time. There are three options--one day, three days and a week for you to choose.

Duration: You can choose a specific day or a period of time according to your needs.

Performance Monitoring Point: entrance-near end, exit-near end.

Performance Monitoring Parameters: The monitoring parameters of Ethernet monitoring point include normal frame number, unicast frame number, multicast frame number, broadcast frame number, CRC error frame, alignment error frame number, ultra long frame number (Frame Too Long), ultra long Jabber frame number (CRC error), ultra short frame number (CRC error), discarded frame number, ultra short frame number (CRC normal), 64-byte frame number, 65-127-byte frame number, 128-255-byte frame number, 256-511-byte frame number, 512-1023-byte frame number, 1024-1518-byte frame number.

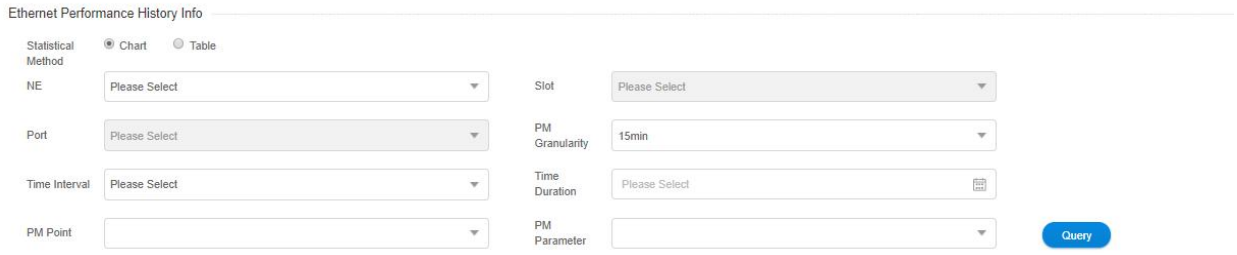



Figure9-92 Ethernet History Performance Parameters

### 9.3.6.2. View Ethernet History Monitoring Information

15minutes and 24hours of Ethernet history data operation and display are the same form. Here we take 15-minute Ethernet history monitoring point as an example. Choose the appropriate network elements, slots, ports and monitoring cycles through the screening box above the menu, and then select the time interval, performance monitoring point and parameters which need to be monitored in the right menu.Parameters to be monitored can be all selected or only select one or two of them to check.After that, click Apply button on the lower right corner. From the graph, we can see the trend of the refraction chart of the monitoring parameters.

The ordinate represents the value of the monitoring data, and the abscissa represents the time. Data which has been read for more than 15 minutes will be automatically transferred from current statistics to history statistics.

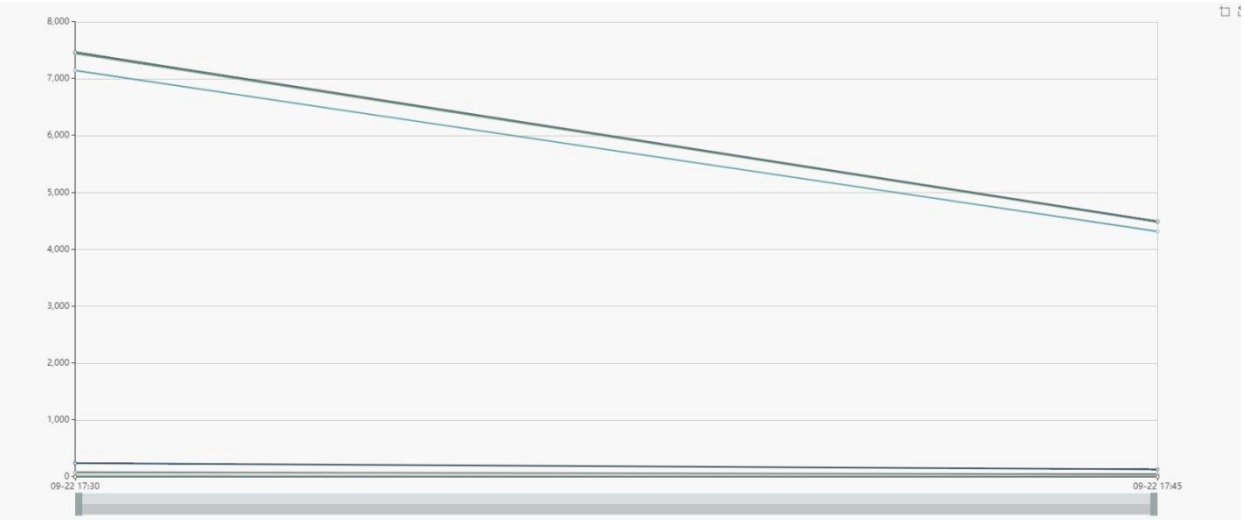



Figure9-93 15-Minute Chart Data of Ethernet

History performance statistics of Ethernet also show history data in tabular form. Click on the table, the interface as shown in the figure below appears:

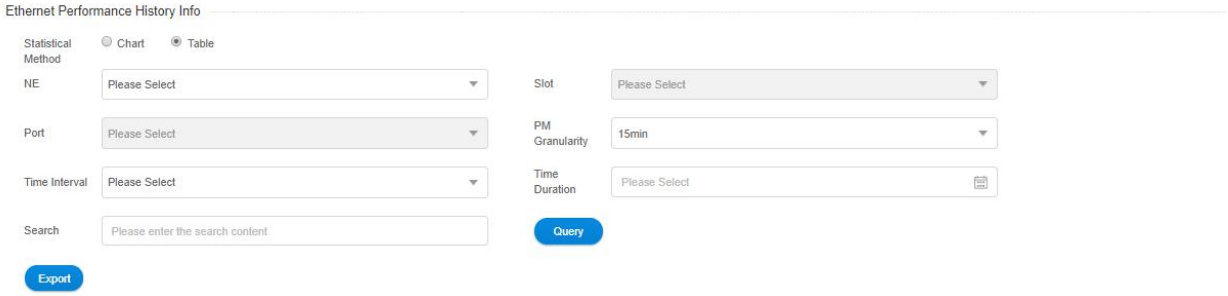



Figure9-94 15-Minute Tabular Interface of Ethernet

Click the time interval shortcut in the right menu or select the required time interval in Duration, and then click on Apply button in the lower right corner, the history data of all Ethernet monitoring points on this port will be displayed, as shown in the figure below:

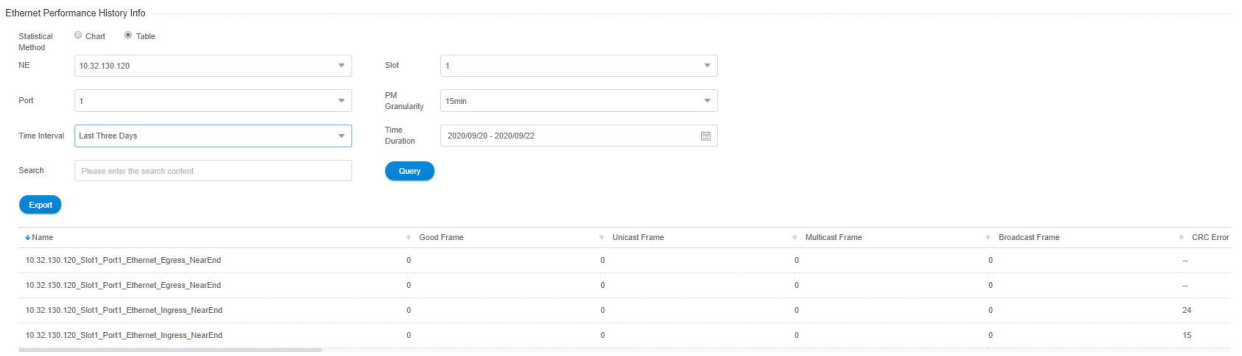



Figure9-95 15-Minute Tabular History Data of Ethernet

### 9.3.6.3. Export Ethernet History Monitoring Information

To save the history data, you can click on the upper Export button, and an interface will pop up, as shown in the figure below:

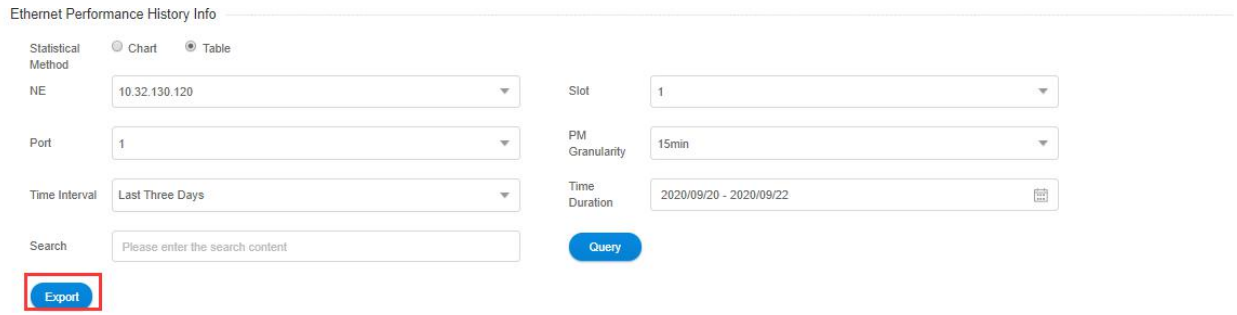



Figure9-96 Export History Data of Ethernet

Any character such as English, Chinese, alphabet or number can be entered as the file name, and then click on Apply button, it will prompt that the export is successful, as shown in the figure below:

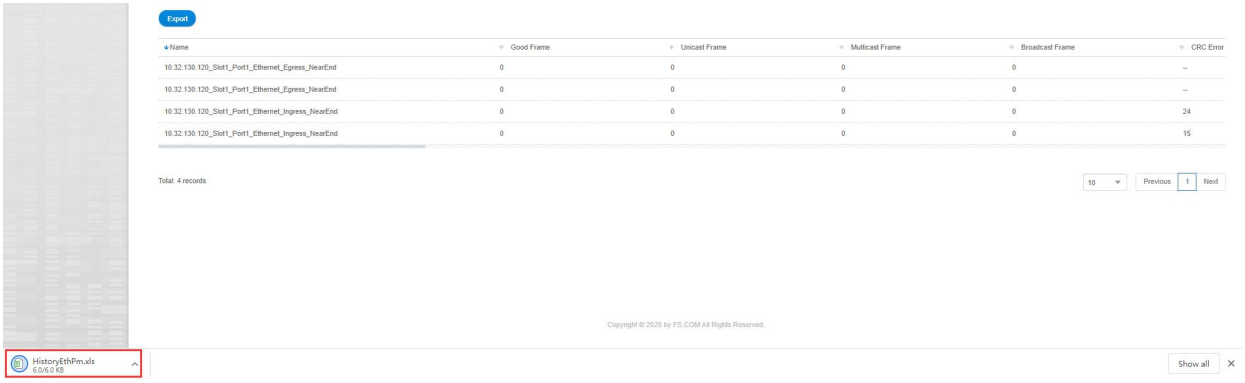



Figure9-97 Successfully Export Data of Ethernet

# 10. Abbreviation

| Abbreviation | Description |
|---|---|
| **AIS** | Alarm Indication Signal |
| **AMP** | Asynchronous Mapping Procedure |
| **BDI** | Backward Defect Indication |
| **BEI** | Backward Error Indication |
| **BER** | Bit Error Ratio |
| **BIP** | Bit Interleaved Parity |
| **BMP** | Bit-synchronous Mapping Procedure |
| **BSP** | Board Support Package |
| **DAPI** | Destination Access Point Identifier |
| **DCM** | Dispersion Compensation Module |
| **DCN** | Data Communication Network |
| **DWDM** | Dense Wavelength Division Multiplexing |
| **EDFA** | Erbium-Doped Fiber Amplifier |
| **FEC** | Forward Error Correction |
| **GCC** | General Communication Channel |
| **GE** | Gigabit Ethernet |
| **GFP** | Generic Framing Procedure |
| **GMP** | Generic Mapping Procedure |
| **IP** | Internet Protocol |
| **NE** | Network Element |
| **NTP** | Network Time Protocol |
| **OA** | Optical Amplifier |
| **OCh** | Optical Channel |
| **ODU** | Optical Demultiplexer Unit |
| **OLA** | Optical Line Amplifier |
| **OLP** | Optical Line Protection |
| **OMU** | Optical Multiplexer Unit |
| **OPA** | Optical Pre-Amplifier |

| | |
|---|---|
| **OPU** | Optical Channel Payload Unit |
| **OSC** | Optical Supervisory Channel |
| **OSNR** | Optical Signal-to-Noise Ratio |
| **OSPF** | Optical Signal-to-Noise Ratio |
| **OTN** | Optical Transport Network |
| **OTU** | Optical Transponder Unit |
| **PM** | Path Monitoring |
| **PT** | Payload Type |
| **SM** | Section Monitoring |
| **SNMP** | Simple Network Management Protocol |
| **TTI** | Trail Trace Identifier |