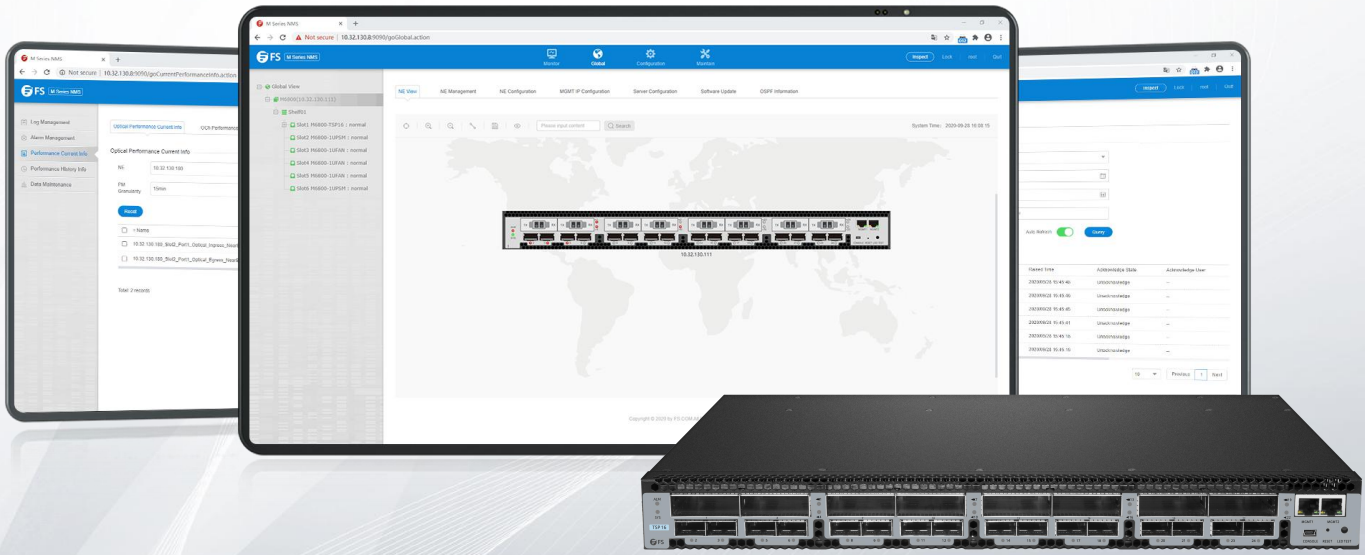
M6800 Series

NE Configuration Manual



Contents

Preface

Overview

Chapter	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 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 Alarm Management	This chapter introduces the current alarms and history alarms of NE and NMS system.
Chapter 7 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
M Series NMS-M6800 Series	R6.3.31

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
	Special attention should be paid to the content. If the operation is improper, it may cause serious injury to the person.
	It reminds the matters for attention. Improper operation may cause loss of data or damage to the device.
	It represents the operation or information that requires special attention to ensure the success of the operation or the normal work of the device.
	A skill or a knack which helps to solve a problem and save time.
	The necessary supplement and explanation for the description of the text.

1. It is not allowed to make modification if the input box or the drop-down box is grayed out.
2. The add, delete, modify and refresh buttons are all on the toolbar.
3. One and only one data in the table must be selected first while doing the modification operation.
4. At least one data in the table must be selected while doing the deletion operation.
5. The refresh button is used to refresh the table and the form. There are two refresh operations on the toolbar. When it shows "Refresh Table" on icon, it will refresh the table. When it shows "Refresh Form" on icon, it will refresh the form.

1. Preparation Before Configuration

1.1. Configuration Process

When configuring M6800-TSP16 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 Figure 1-1 to complete the operation. If the project has been created, only the configuration of one NE or single disk needs to be changed, please perform the operation according to relevant content of chapters in Figure 1-1.

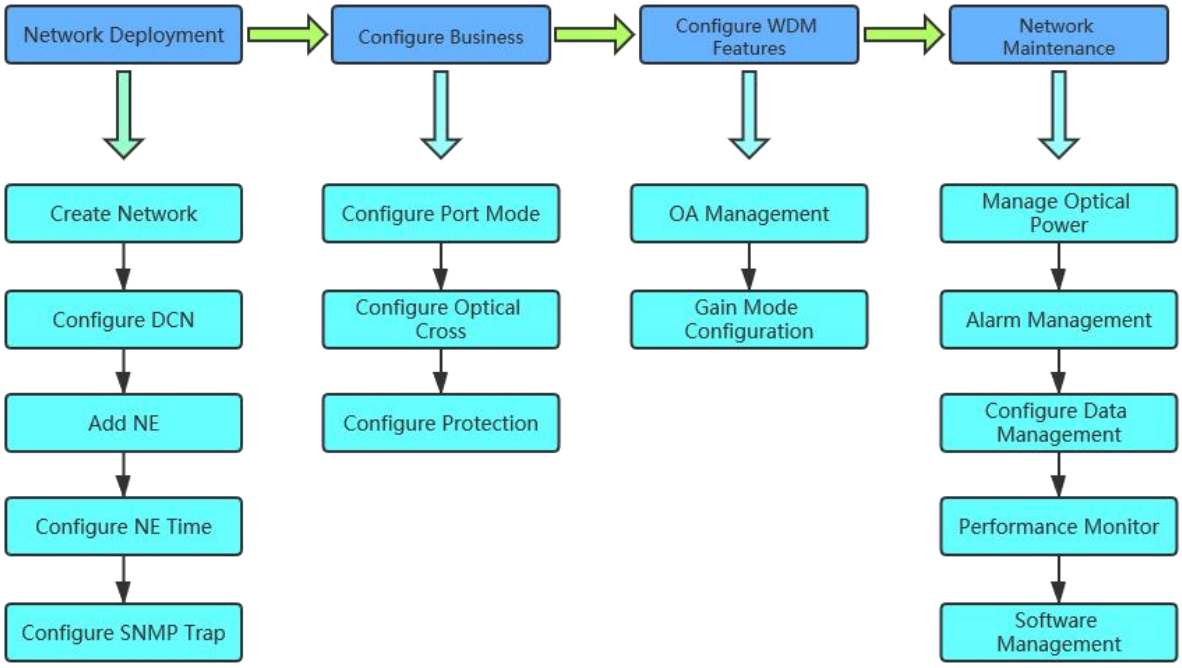


Figure 1-1 M6800-TSP16 Service Configuration Process

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

It is recommended that the configurations of M Series NMS equipment be completed according to the sequence of operation in the flowchart (Figure 1-1).

1.2. Connect NMS System & NE

For different network connection components, there are multiple connection modes between M Series NMS network management computer and M6800-TSP16 network elements. The connection mode of “directly connected network line+HUB+directly connected network line” is the most commonly used. You can also directly connect M Series NMS network management computer with M6800-TSP16 network elements by using cross network cable or directly connected network cable.

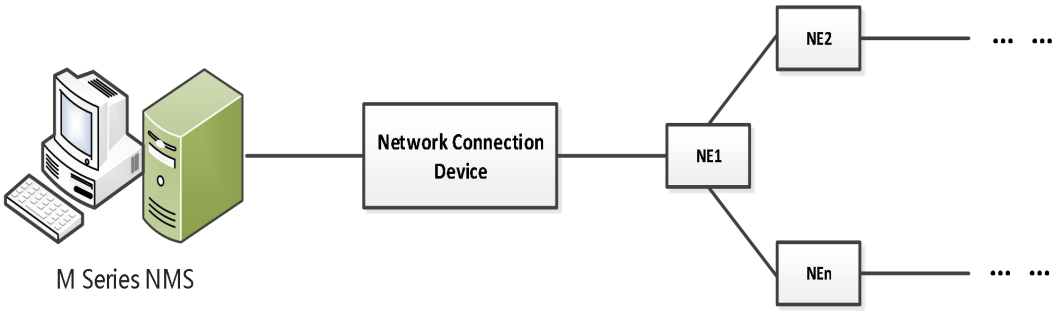


Figure 1-2 Schematic Diagram of Connection Between Network Management System and Network Elements

Prerequisite

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

Steps

Here we take the connection mode of "directly connected network cable+HUB+directly connected network cable" 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 End 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:

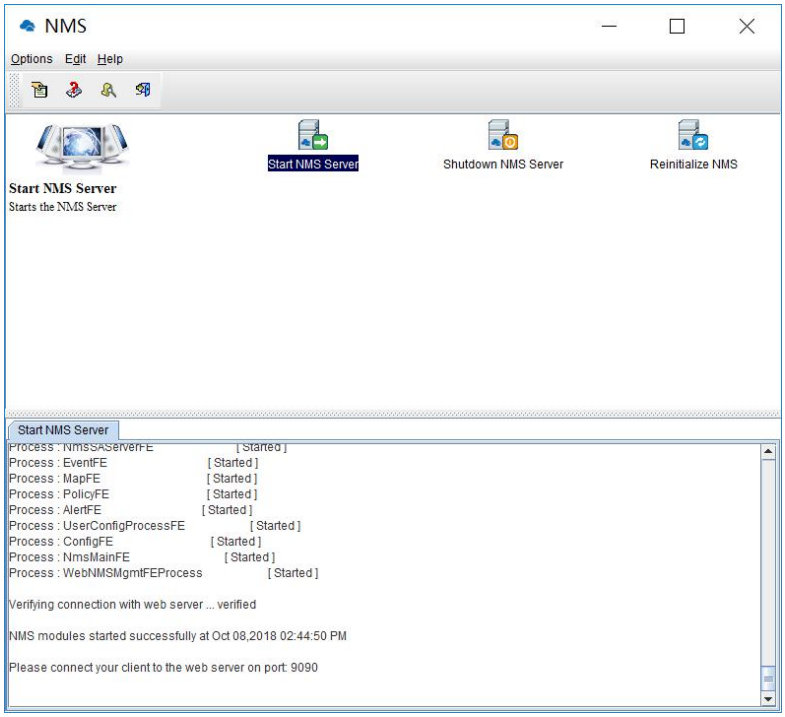


Figure 1-3 Start NMS Server

Note: In log of “Start NMS Server”, when it shows “NMS module has successfully started at XXXX, please start the client application. The port of web server is 9090”, it indicates that the NMS server has successfully started.

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 disk 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 M6800-TSP16 in each step, and only the sections of the reference book will be provided for the common configuration steps for each device. M Series NM-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;
- Management of NE IP;
- 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:

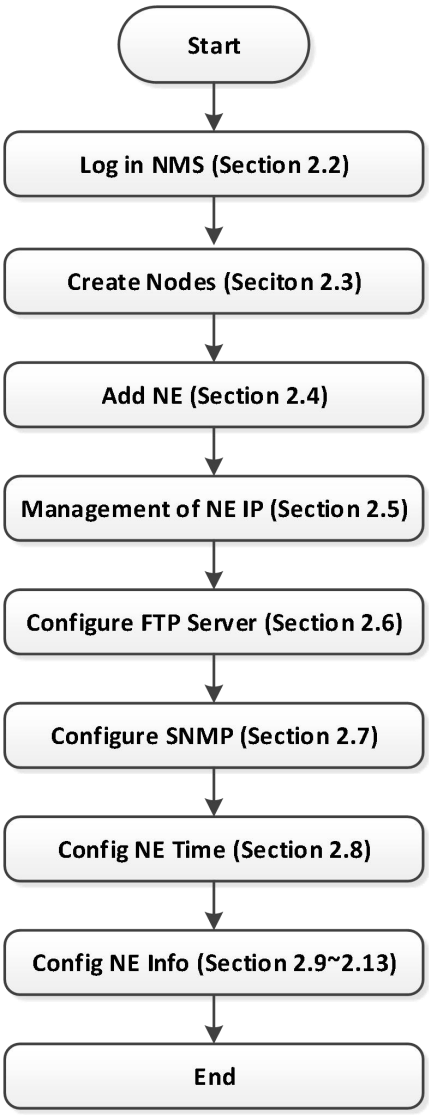


Figure 2-1 Create Flow Chart of Network Topology

2.2. Login NMS Interface

Prerequisite

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

Steps

Open the Google Chrome browser and enter localhost:9090 in the address bar (If you log on to the NMS host, you can use this address.) or xxx.xxx.xxx.xxx:9090 (for remote NMS host). Enter your user name and password to login. The user name is root, and the password is public.

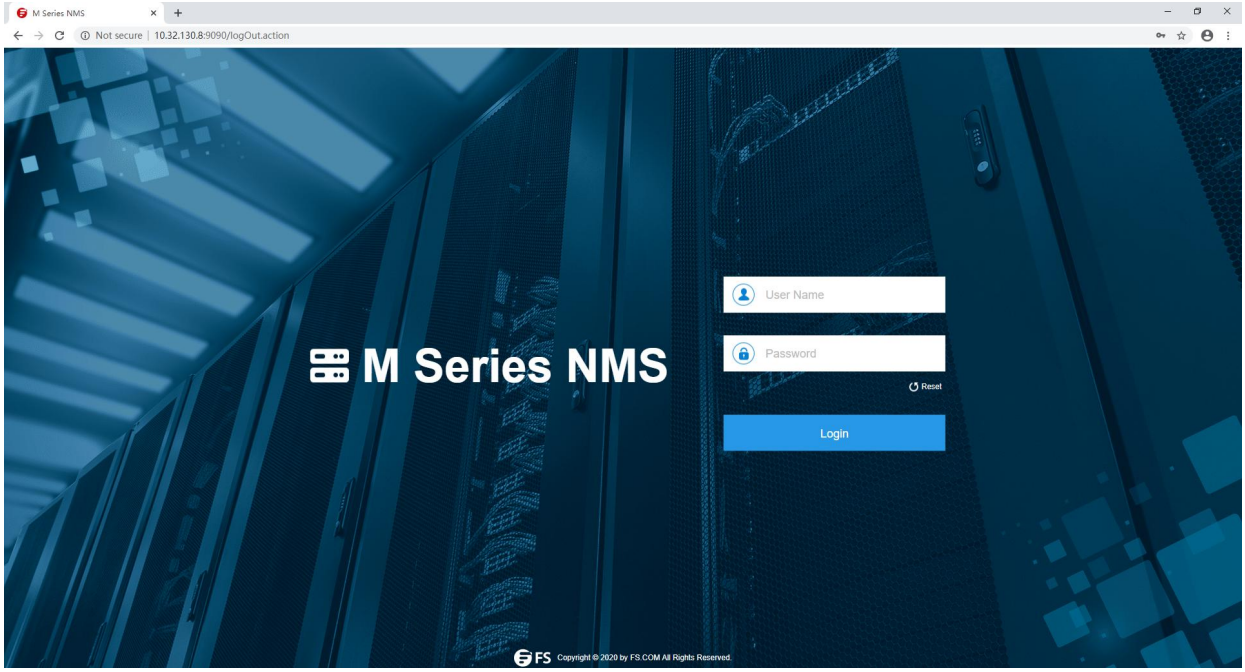


Figure 2-2 Login NMS System

2.3. Create Node

Click on"*Global View*" , and then click on"*Global Configuration*". Enter node name and description information. The description information can be blank. After that, click on "*Apply*".

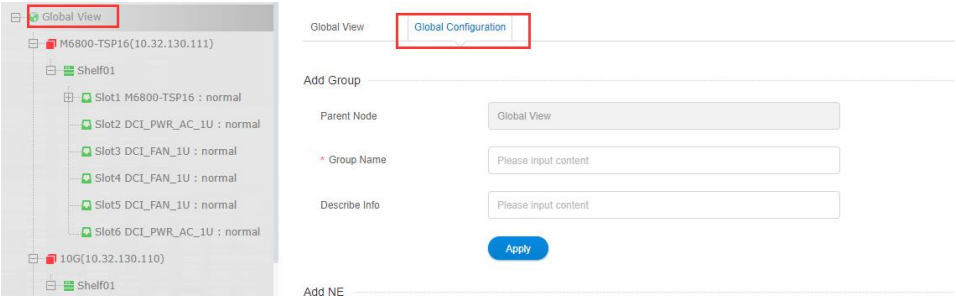


Figure 2-3 Add Node

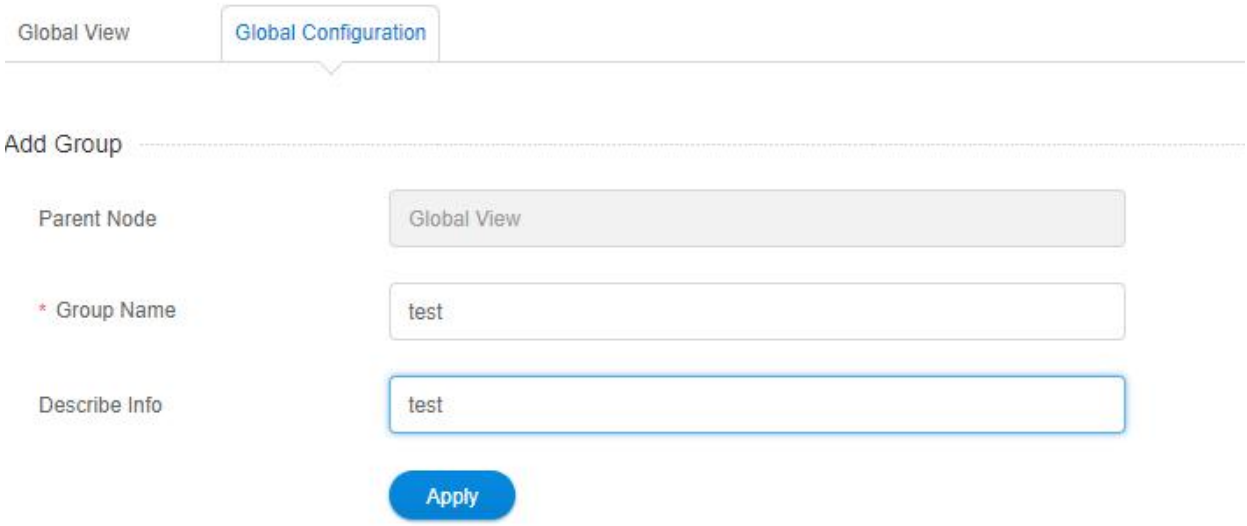


Figure 2-4 Add Node Info

2.4. Add NE

2.4.1. Add NE

Click on the node which has been added, then click on"*Group Configuration*". Enter the NE name, NE IP address, subnet mask, Trap host name, Trap host IP address, and click on"*Apply*".

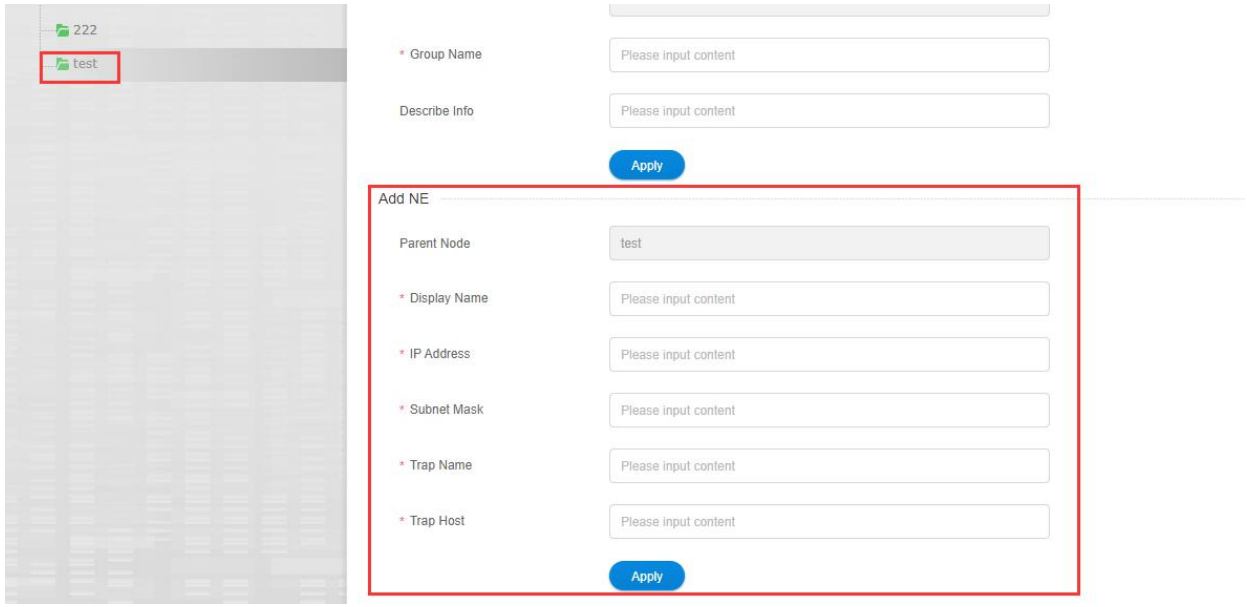


Figure 2-5 Add NE

2.4.2. Modify NE

Click on the NE which has been added，then click "*NE Management*". Here you can only modify the displayed name of the NE.

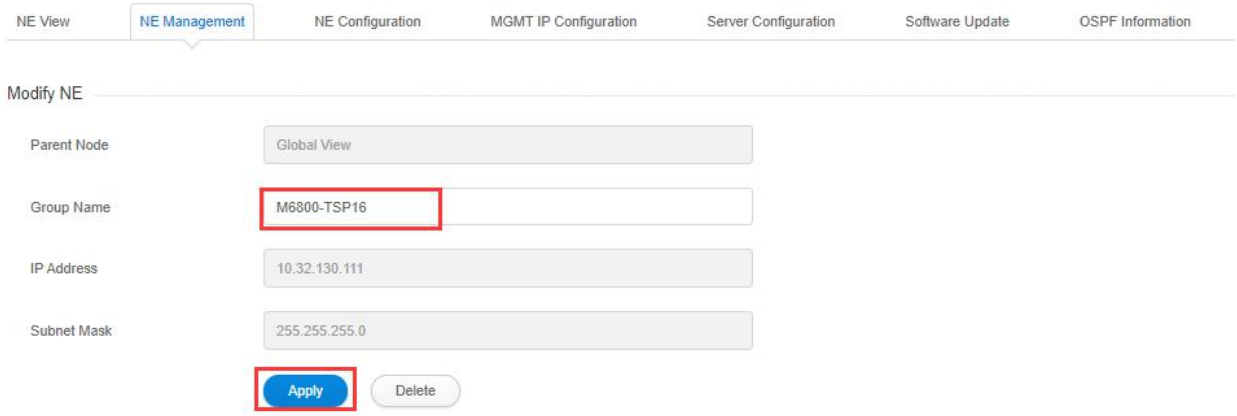


Figure 2-6 Modify NE Name

2.4.3. Delete NE

Click on the NE which has been added, then click "*NE Management*",and click on"*Delete*".

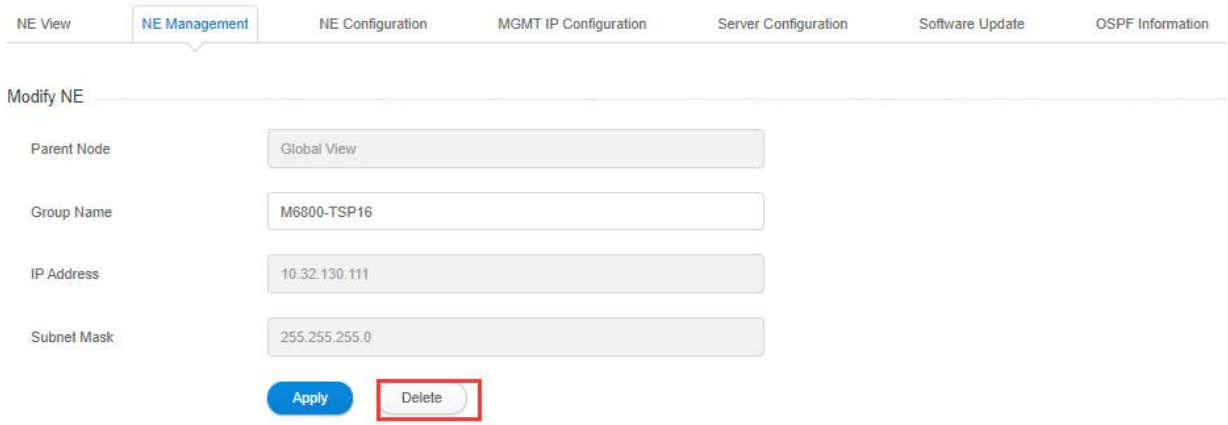


Figure 2-7 Delete NE

2.5. Manage NE IP

There are three types of IP addresses of NE:

- Node IP address: in-band management IP address which is suitable for DCN transmission.
- IP1/IP2 address: out-band management IP address which can be modified by the client.
- Local NMS IP address: It is the default IP address which is 192.168.126.2.

DCN purpose: 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

Click on the NE which has been added, then click on"*MGMT IP Configuration*"on the top.

Figure 2-8 MGMT IP Configuration

Input the IP address of the node, and then click on"*Apply*".

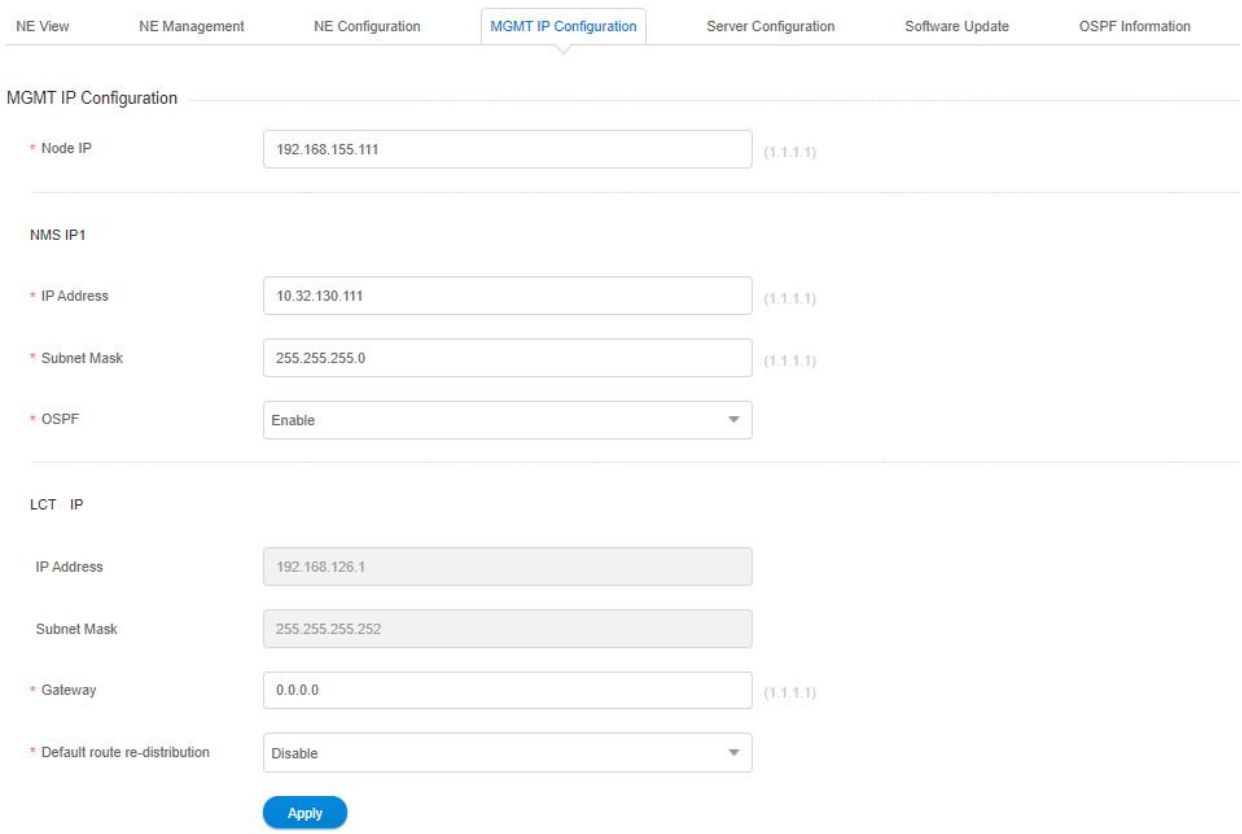


Figure 2-9 MGMT IP Configuration

2.5.2. NMS IP1 Configuration

Click on the NE which has been added→Click on"*MGMT IP Configuration*"on the top. Input the IP address, and then click on"*Apply*".

Figure 2-10 NMS IP1 Configuration

2.5.3. Local NMS IP Configuration

The default IP address of local NMS is 192.168.126.1, and the default subnet mask is 255.255.255.252.

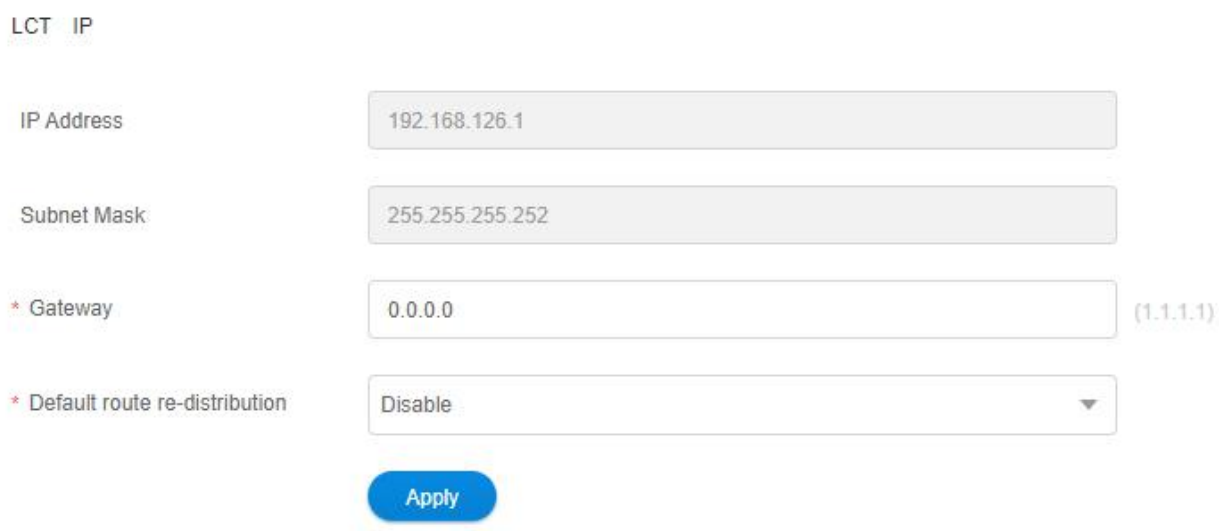


Figure 2-11 Local NMS IP Configuration

2.5.4. Gateway Configuration

Click on the NE which has been added→Click on"*MGMT IP Configuration*". Input gateway IP address, and click on"*Apply*".

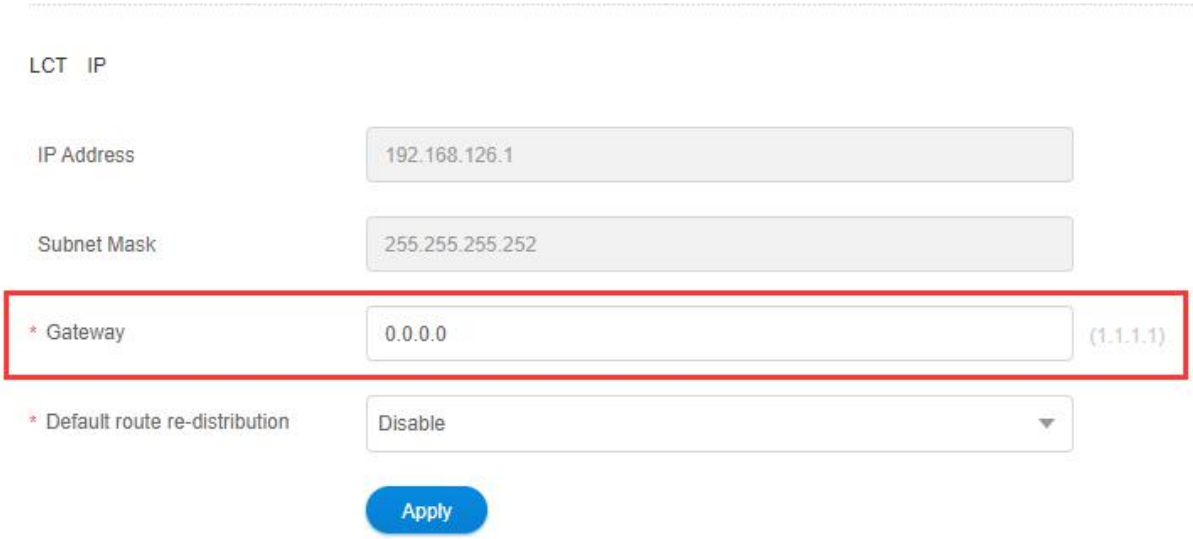


Figure 2-12 Gateway Configuration

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

Click on the NE which has been added→Click on"*Server Configuration*"on the top, and input the IP address of the FTP server, then click on"*Apply*".

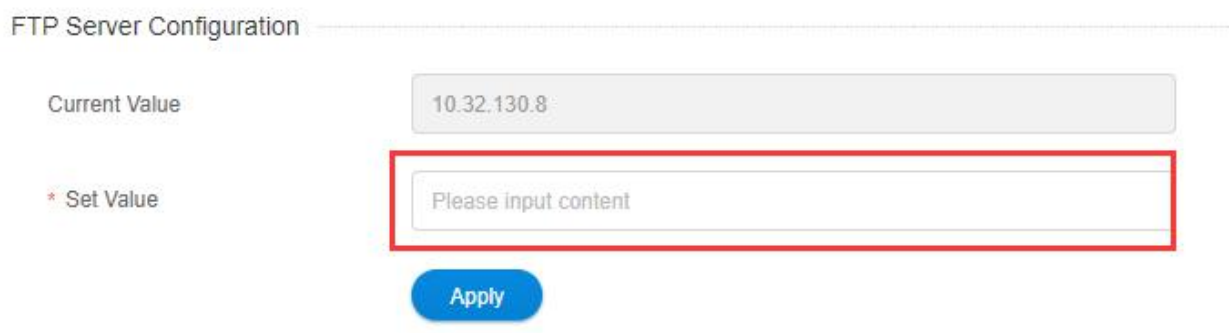


Figure 2-13 Configure FTP Server

2.7. SNMP Configuration

Click on the NE which has been added→Click on"*Server Configuration*"on the top→Click "*Add*". Enter SNMP Trap configuration interface, click on"*Apply*".

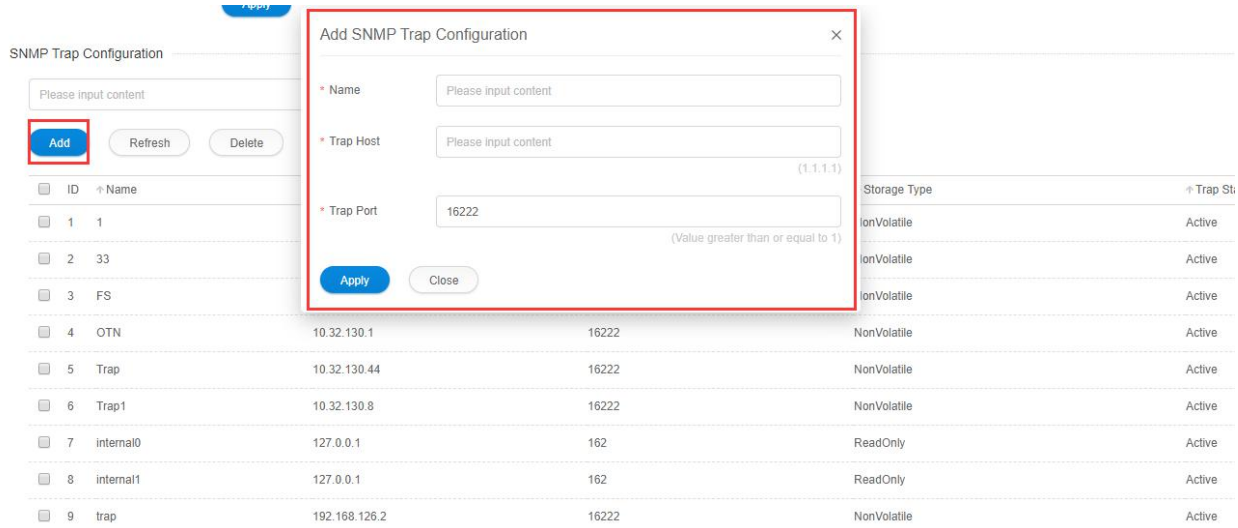


Figure 2-14 SNMP Configuration

Click on"*Apply*" button in the pop-up window to add trap address. The default port number of trap is 16222. It is not recommended to modify this port number.

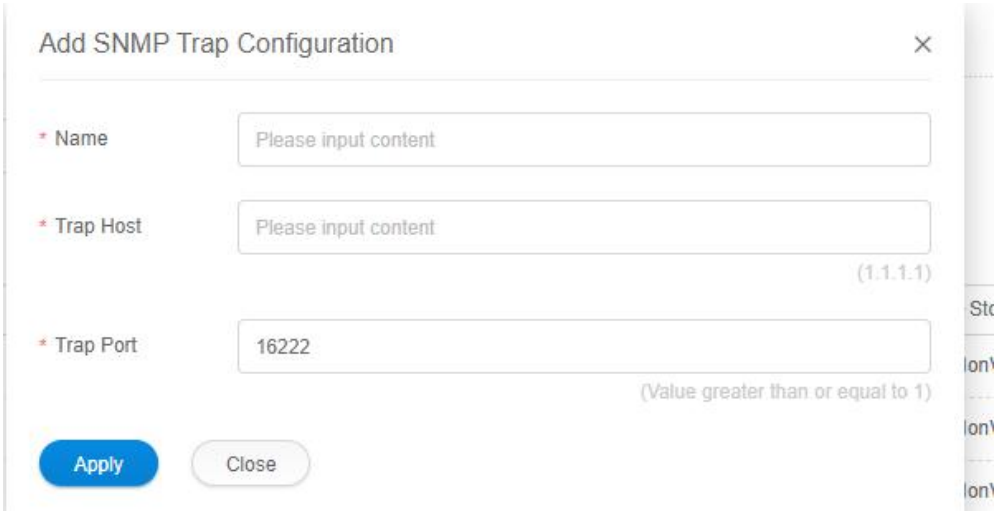


Figure 2-15 Add Trap Address

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 top.

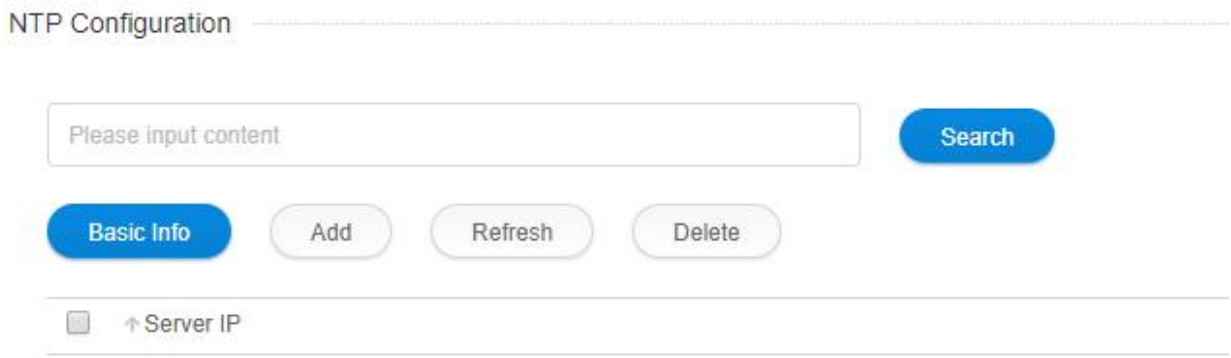


Figure 2-16 NTP Configuration

Input the IP address of NTP server, and click on "*Apply*", the configuration succeeds.

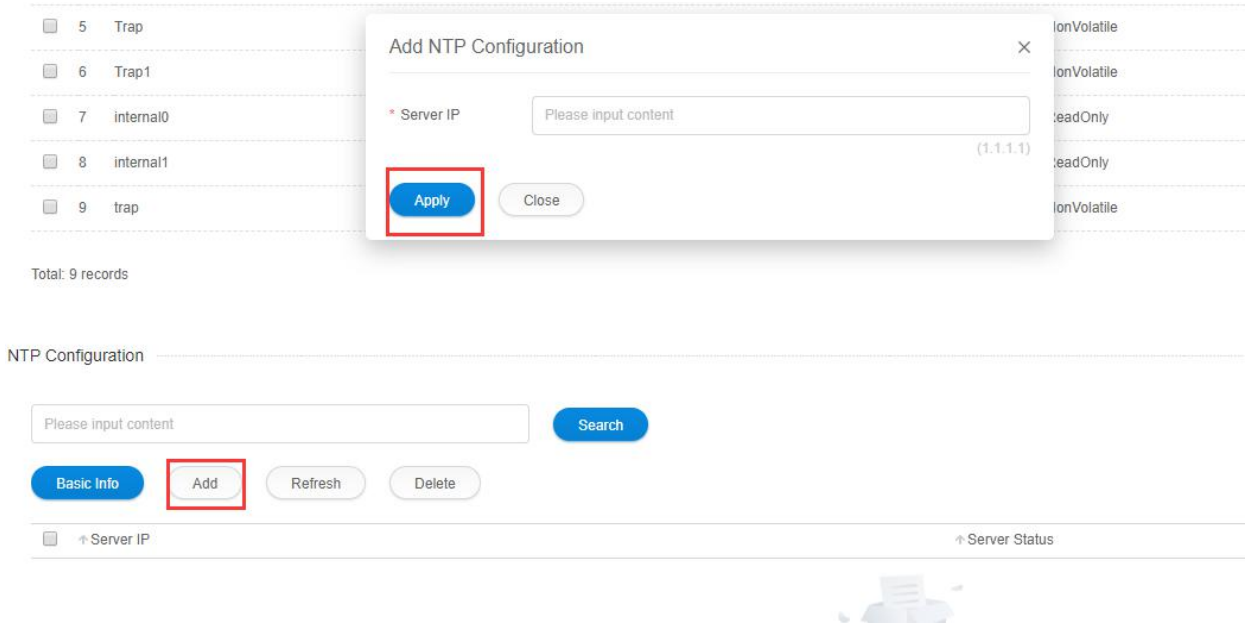


Figure 2-17 Configure NTP Server

2.8.2. Configure NE Time

Click on the NE which has been added→Click on"*NE Configuration*"on the top menu.

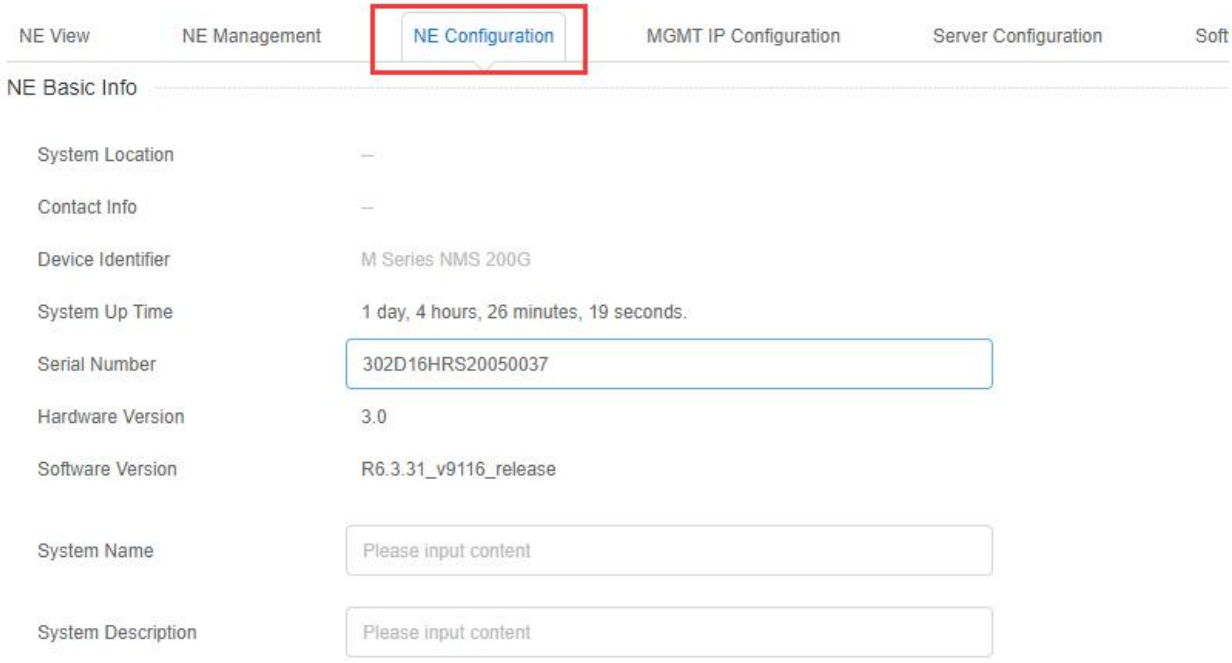


Figure 2-18 NE Time Configuration

Configure the current time of NE , and click on "*Apply*".

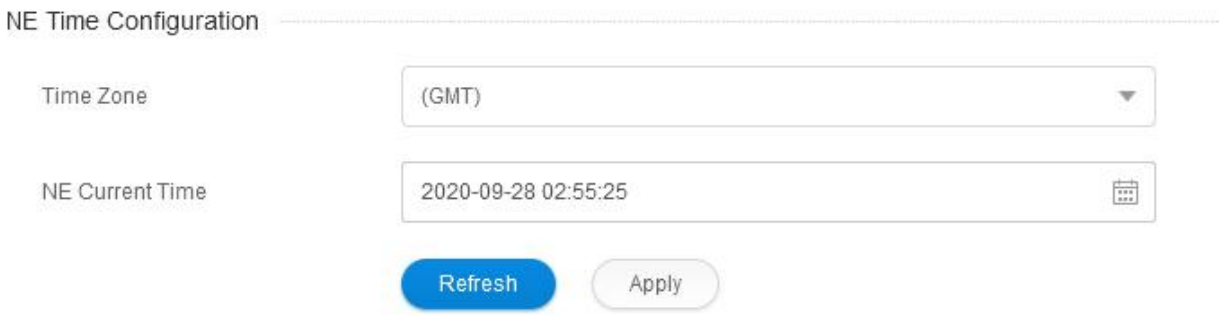


Figure 2-19 Set NE Time

2.9. Upgrade NE

Upgrade NE:

- NE Software Upgrade: When the NE software is not the latest version but it needs to support the new function, you need to upgrade the NE software.
- BSP Upgrade of SC Card: When the NE BSP is not the latest version but it needs to support the new BSP function, you need to upgrade the NE BSP.

2.9.1. NE Software Upgrade

Click on the NE which has been added→Click on"*Software Update*"on the top.

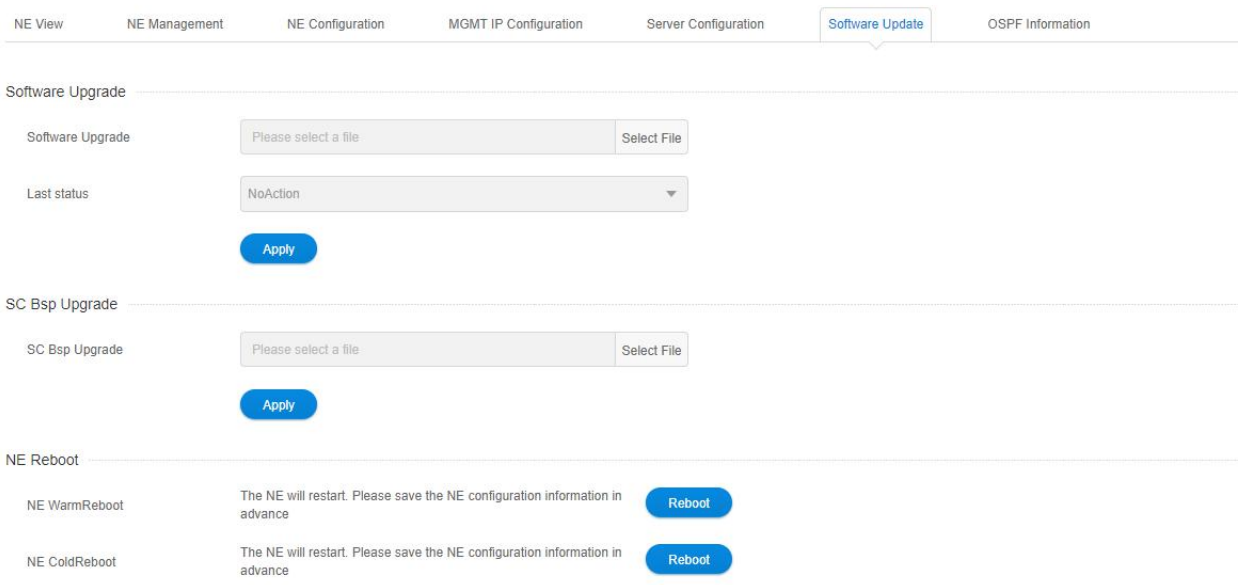


Figure 2-20 NE Software Upgrade

Select the NE load which needs to be upgraded, and click on "*Apply*" to upgrade the NE.

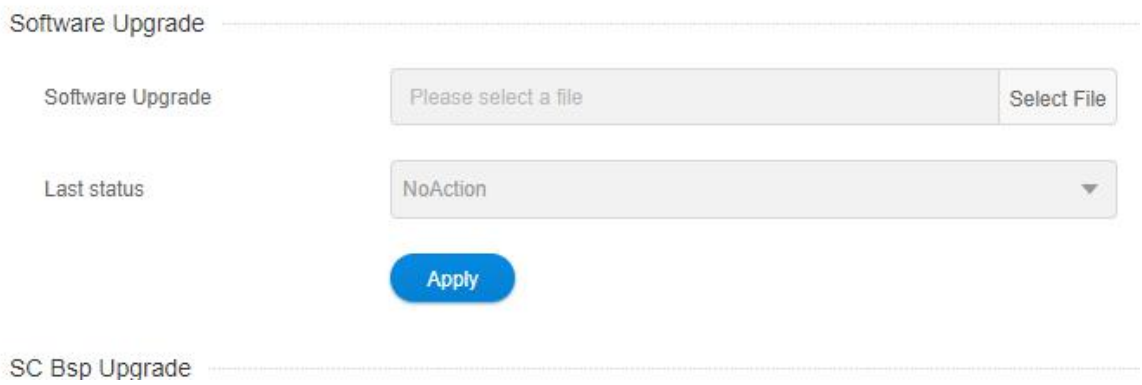


Figure 2-21 Select NE File Name

Note: The software upgrade file and MD5 validating file should be placed in the following directory at the same time: server installation root NMS --->TFTP---> software. Please do not change the file name and release the file by using the official name.

After upgrading the NE, you need to cold start and hot start the NE to make the upgraded load be effective.

Cold Start of NE: It will reboot the NE after cold start of NE, and the service which is being tested will be interrupted. After successful reboot of the NE, the service will recover to normal.

Hot Start of NE: It will reboot the NE after hot start of NE. However, the service will not be interrupted in the reboot process.

2.9.2. BSP Upgrade of SC Card (NMU Module)

Click on the NE which has been added→Click on"*Software Update*"on the top.

Select the BSP file which needs to be upgraded and click on"*Apply*" , you can upgrade BSP of NMU card.

Figure 2-22 Select BSP File Name

Note: BSP upgrade file and MD5 verification file need to be simultaneously placed in the following directory: server installation root NMS --->TFTP---> bsp (firmware_update upgrade tool is simultaneously placed in this root directory). Users can locally modify the upgrade file name and MD5 verification file name. The names of the two files must be the same (except for the suffix), and Chinese or special characters are not allowed for the file names.

2.10. Configure NE Data

Configure NE Data:

- Save NE Configuration: Abnormal power failure of the network element may cause configuration loss and affect the service. The configuration data of M6800-TSP16 network elements will be saved automatically at a certain time interval (1-3 minutes). In this option, it manually triggers the saving of configuration. With this function, the NE configuration will be saved immediately.
- 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.

2.10.1. Save NE Configuration

Click on the NE which has been added→Click on"*NE Configuration*"on the top.

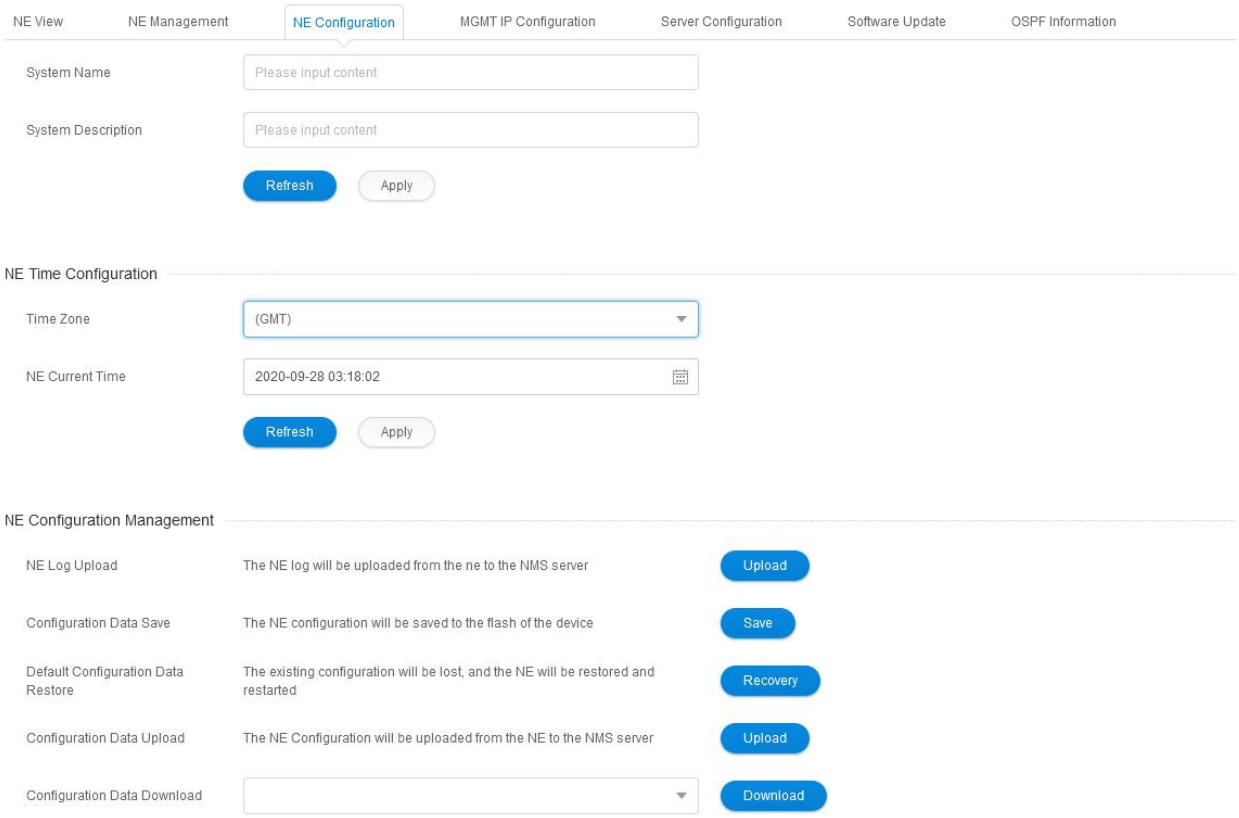


Figure 2-23 Save NE Configuration

2.10.2. Upload NE Configuration

Click on the NE which has been added→Click on"*NE Configuration*"on the top.

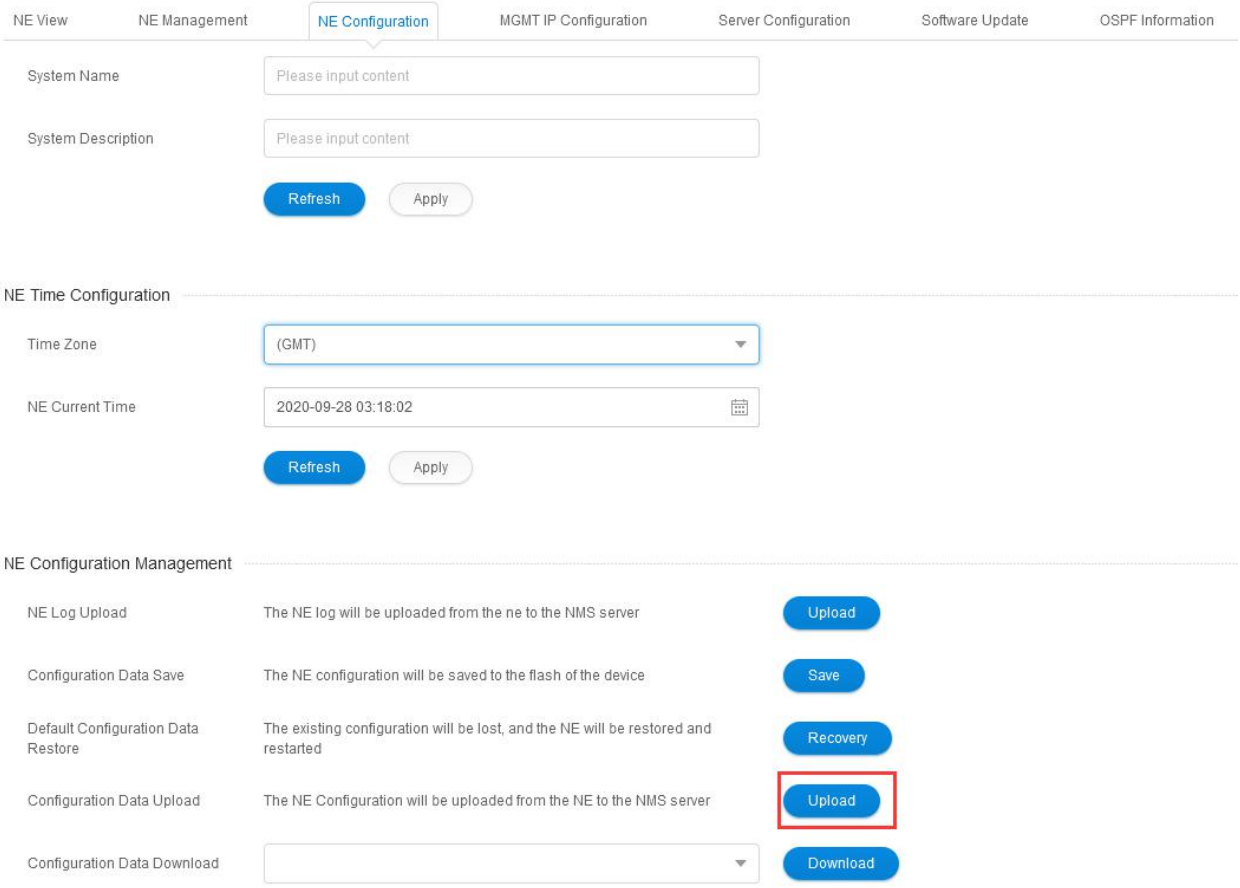


Figure 2-24 Upload NE Configuration

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

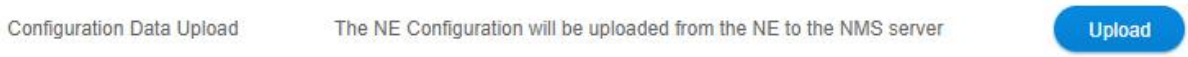


Figure 2-25 Enter NE Configuration File Name

The path to upload network element configuration is: the NMS installation directory --->TFTP--->config folder.

2.10.3. Download NE Configuration

Click on the NE which has been added→Click on"*NE Configuration*"on the top.

Figure 2-26 Download NE Configuration

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

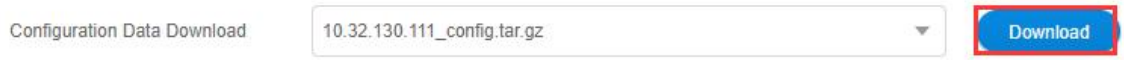


Figure 2-27 Select Configuration File To Be Downloaded

2.10.4. Restore NE Default Configuration

Click on the NE which has been added→Click on"*NE Configuration*"on the top.

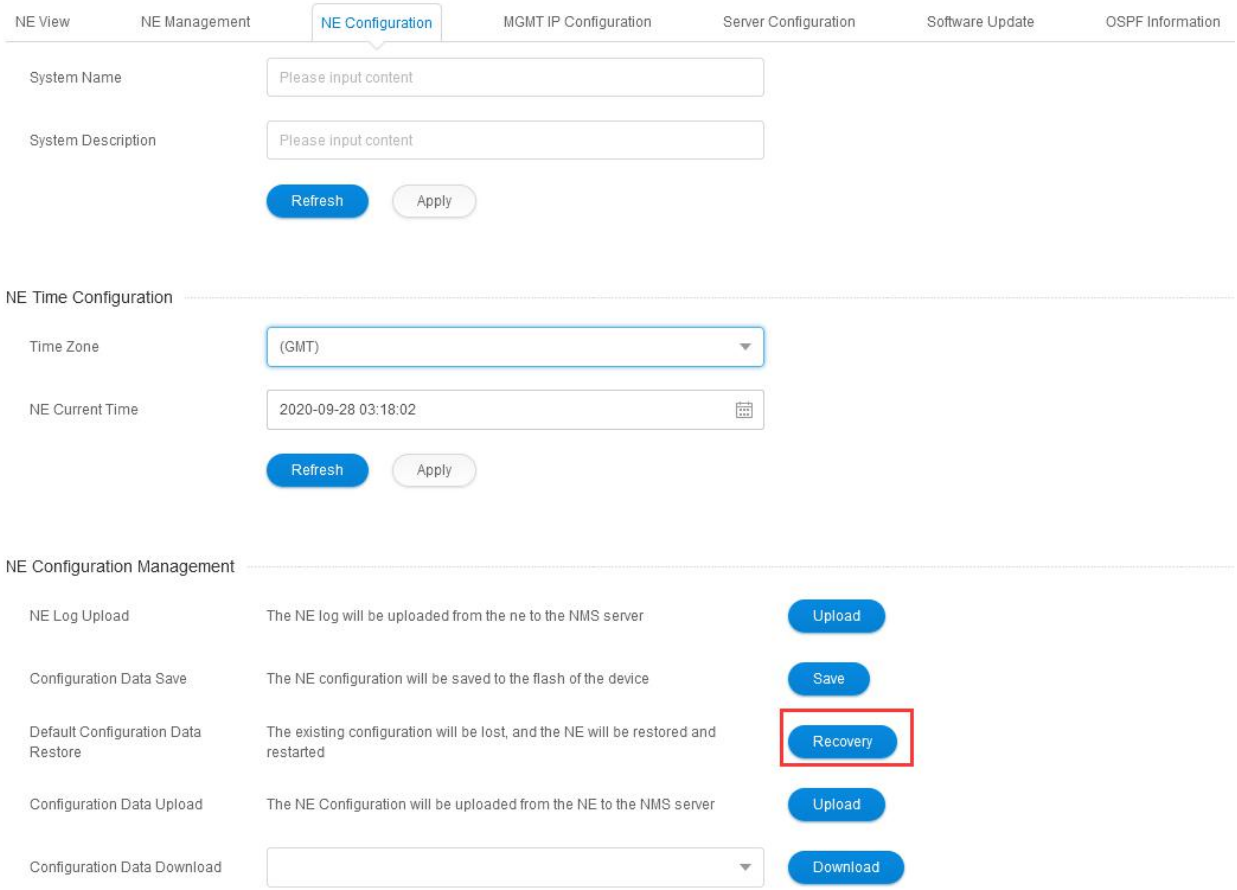


Figure 2-28 Restore NE Default Configuration

2.11. Upload NE Log

2.11.1. Upload NE Log

Click on the NE which has been added→Click on"*NE Configuration*"on the top.

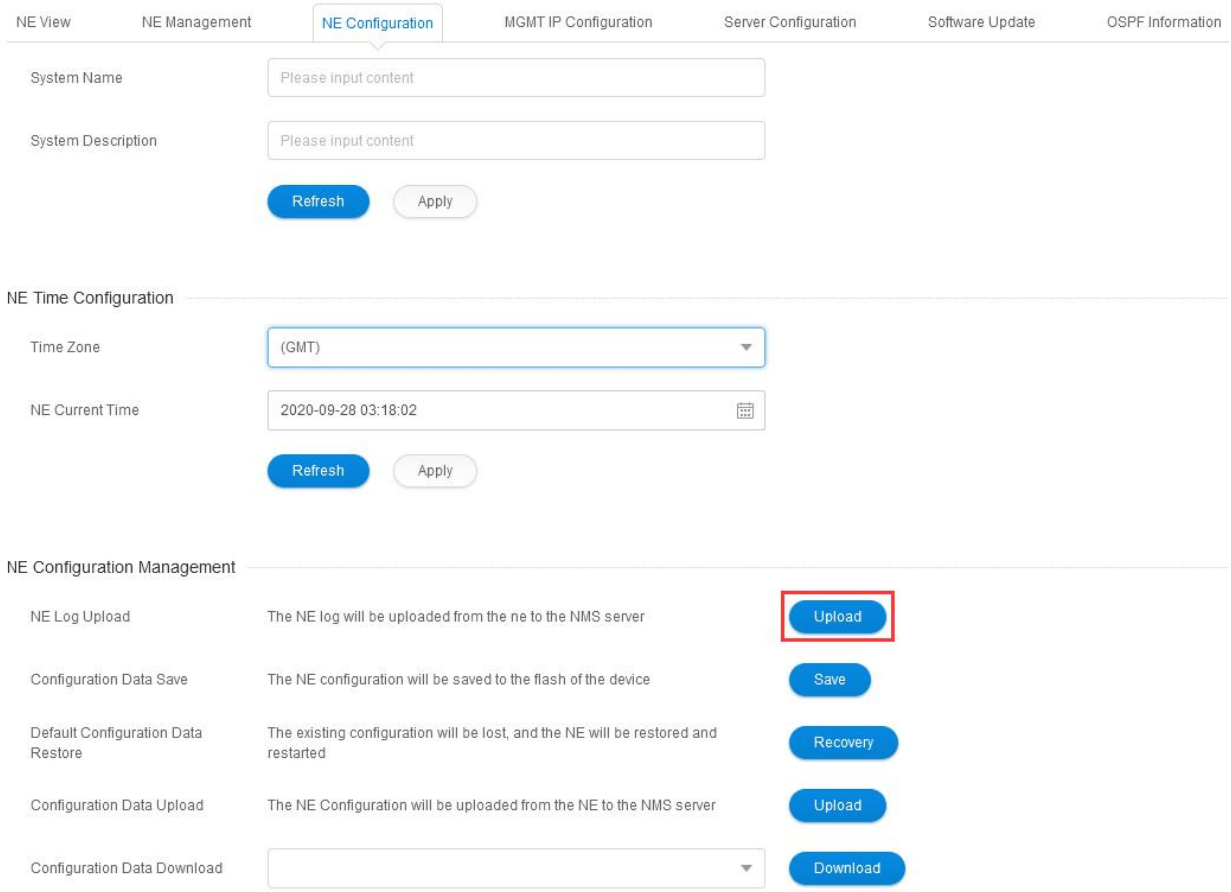


Figure 2-29 Upload NE Log

Enter the file name of the log which needs to be uploaded, and click on " *Apply*".

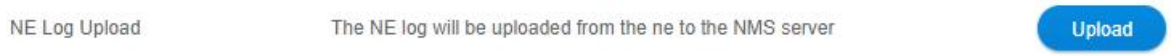


Figure 2-30 Enter File Name of NE Log

The path to upload network element configuration is: the NMS installation directory --->TFTP--->log folder.

2.12. Reboot NE

Reboot NE:

- Hot Reboot of NE: During the hot reboot of NE, the service will not be interrupted.
- Cold Reboot of NE: During the cold reboot of NE, the service will be interrupted. The service will be recovered to normal after the start of the equipment is completed.

2.12.1. NE Hot Reboot

Click on the NE which has been added→Click on"*Software Update*"on the top.

Figure 2-31 NE Hot Reboot

If you are sure to make hot reboot of NE, then click on"*OK*".

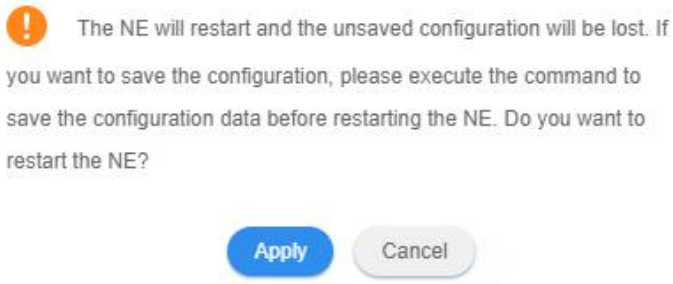


Figure 2-32 Confirm Hot Reboot

2.12.2. NE Cold Reboot

Click on the NE which has been added→Click on"*Software Update*"on the top.

Figure 2-33 NE Cold Reboot

If you are sure to make cold reboot of NE, then click on"*OK*".

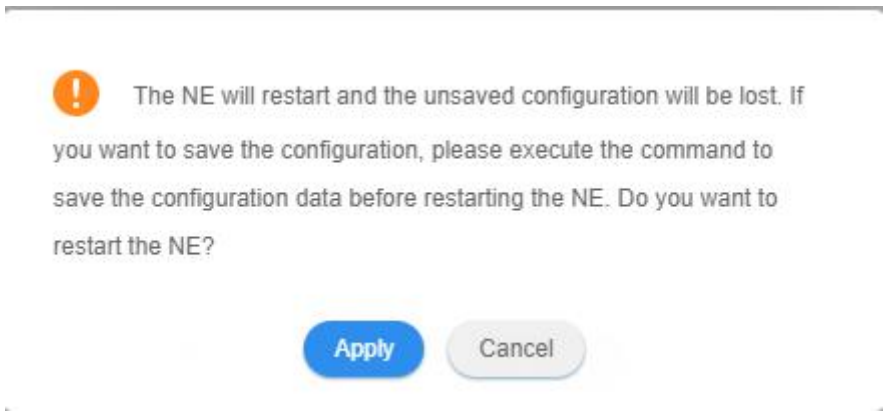


Figure 2-34 Confirm Cold Reboot

2.13. Display and Operate Device Panel

2.13.1. 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.

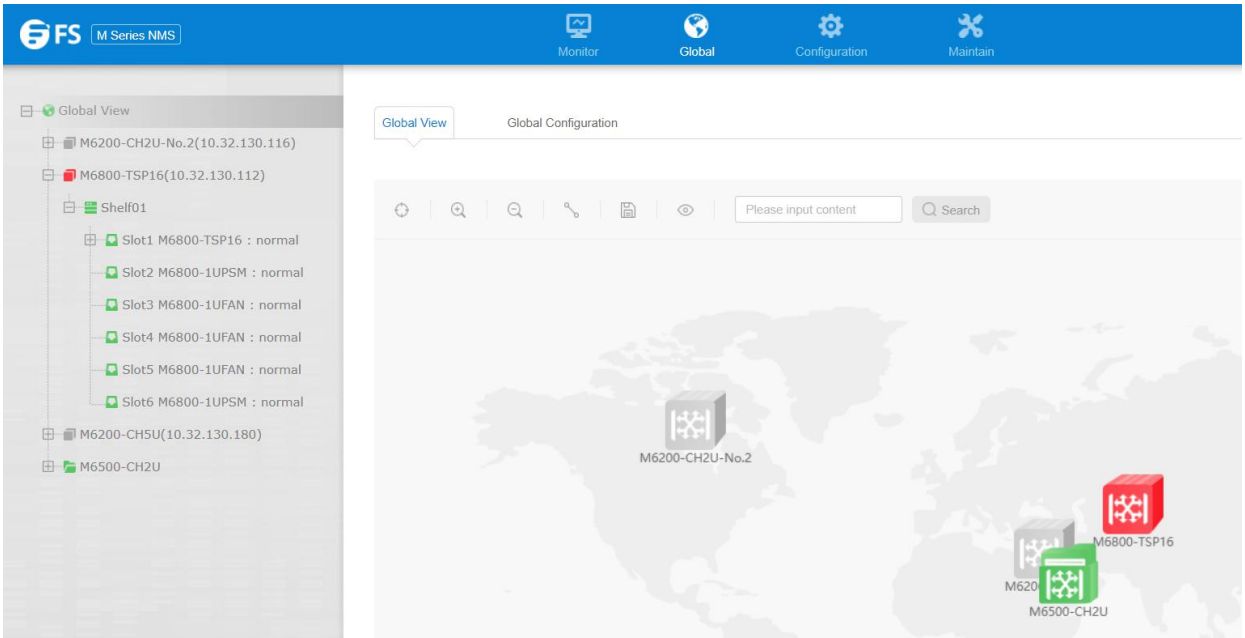


Figure 2-35 Adjust NE Layout

2.13.2. Create Connection between NEs

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

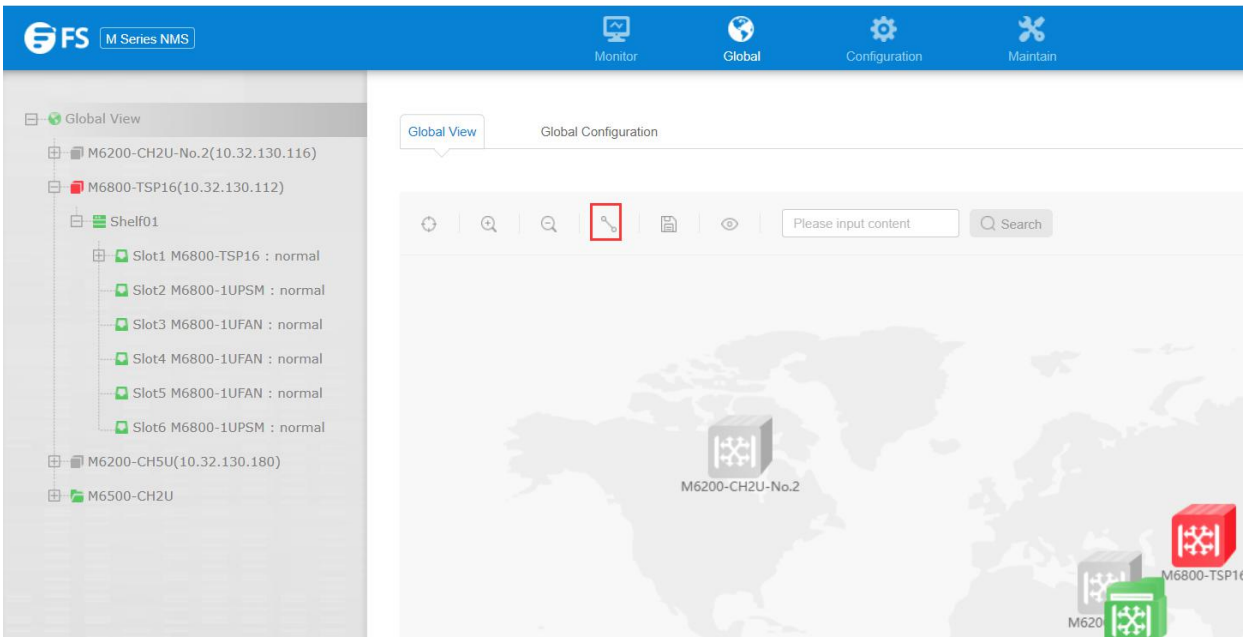


Figure 2-36 Click"Connect"Button

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

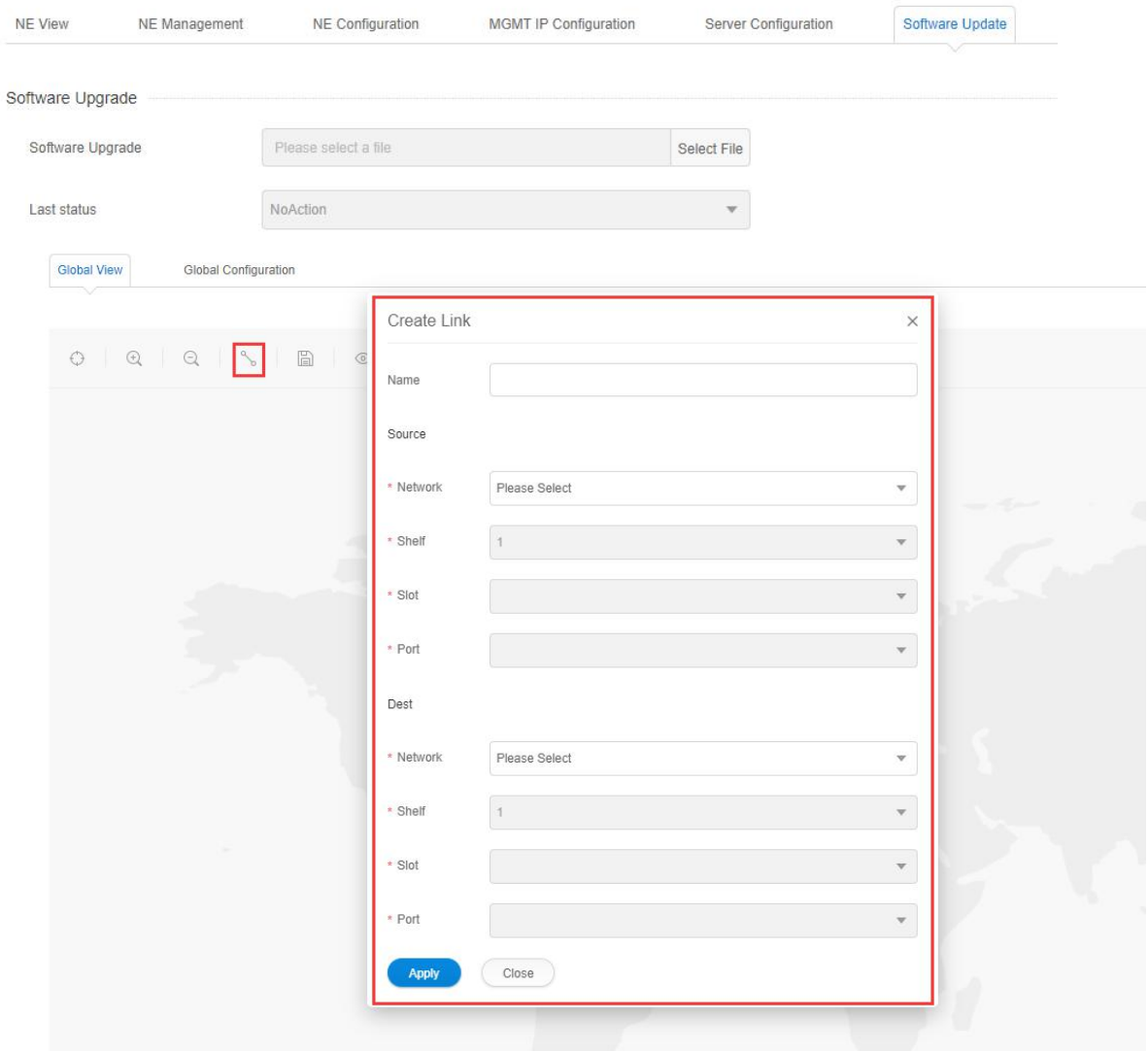


Figure 2-37 Create Connection between NEs

2.13.3. Display Panel Diagram

Click on the NE which has been added, then click on"*NE View*".

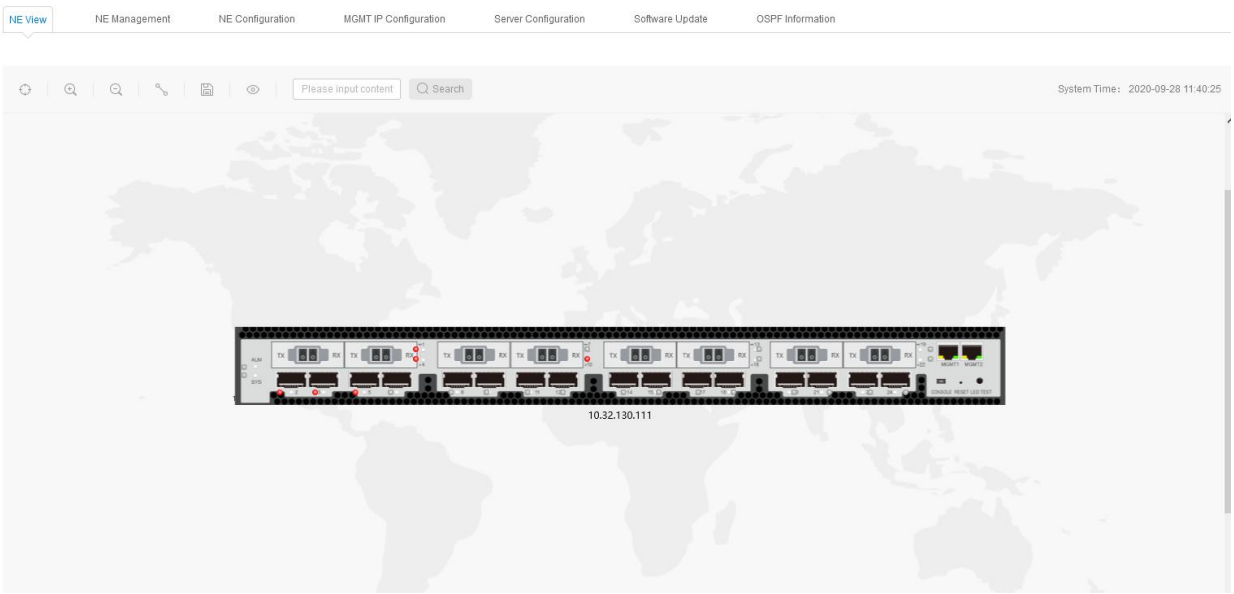


Figure 2-38 NE View

2.13.4. Save Layout

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

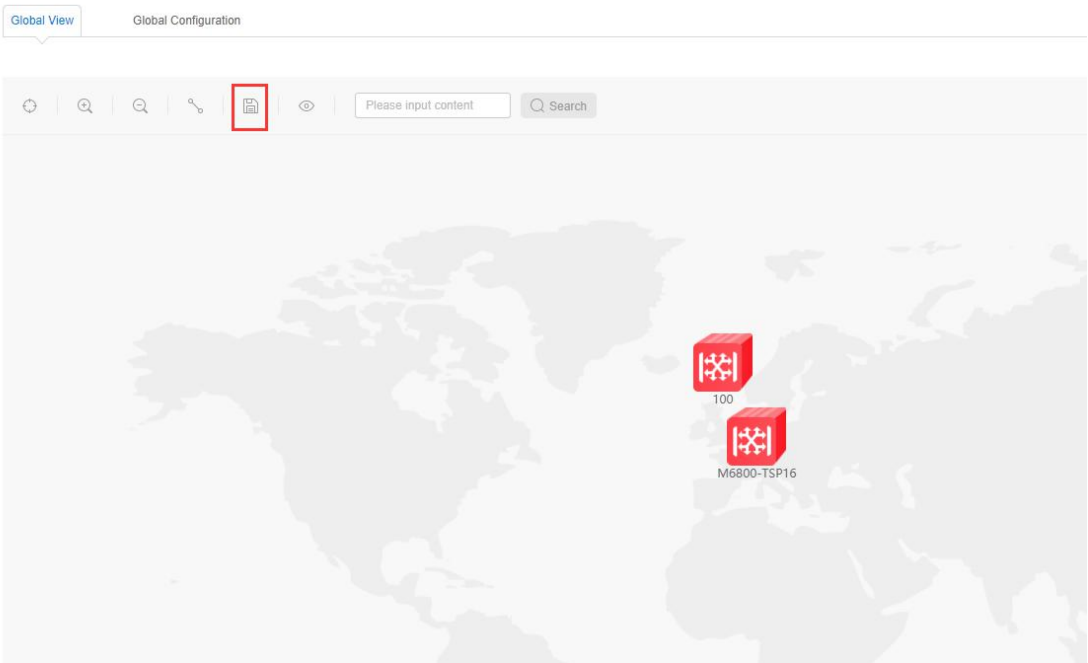


Figure 2-39 Save Layout

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:

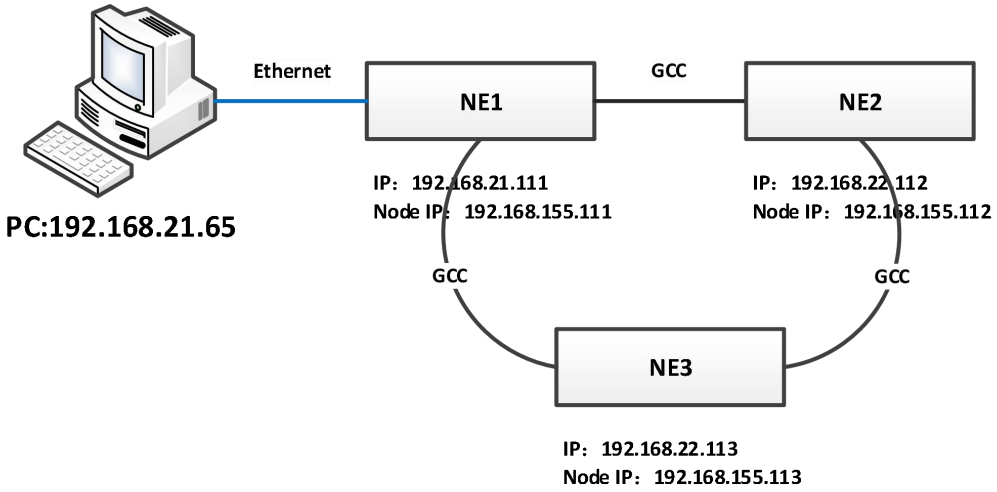


Figure 3-1 Basic Environment Map of PC Direct Connection

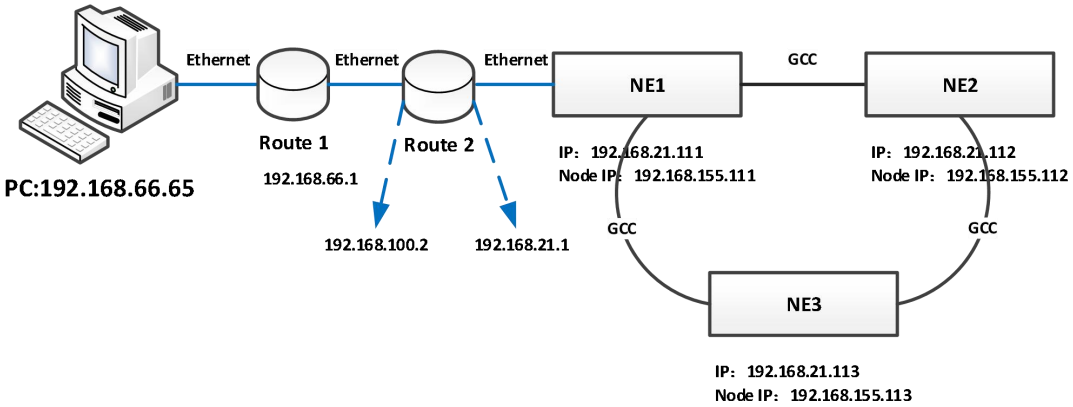


Figure 3-2 Basic Environment Map of Connection between PC and Router

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

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 MGMT1 port of the device. Add the IP of 192.168.126.1 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 OCh (OTU4)/OCh (OTUC2).

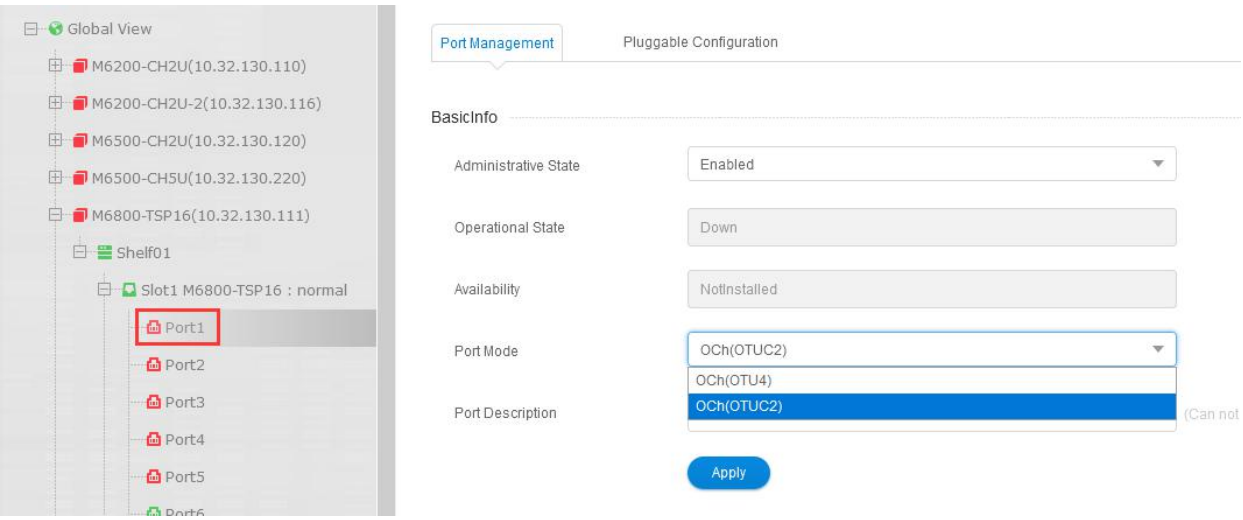


Figure 3-3 Enable OCh (OTU4) Port

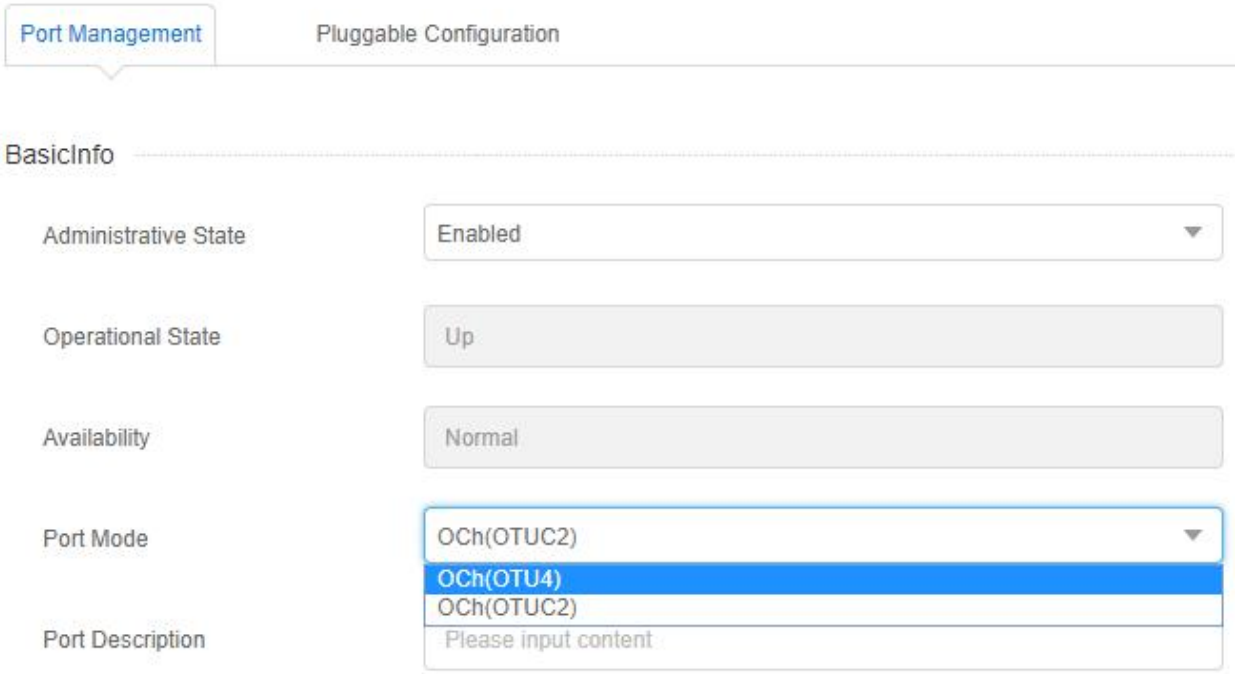


Figure 3-4 Enable OCh (OTUC2) Port

Click on OTU4.

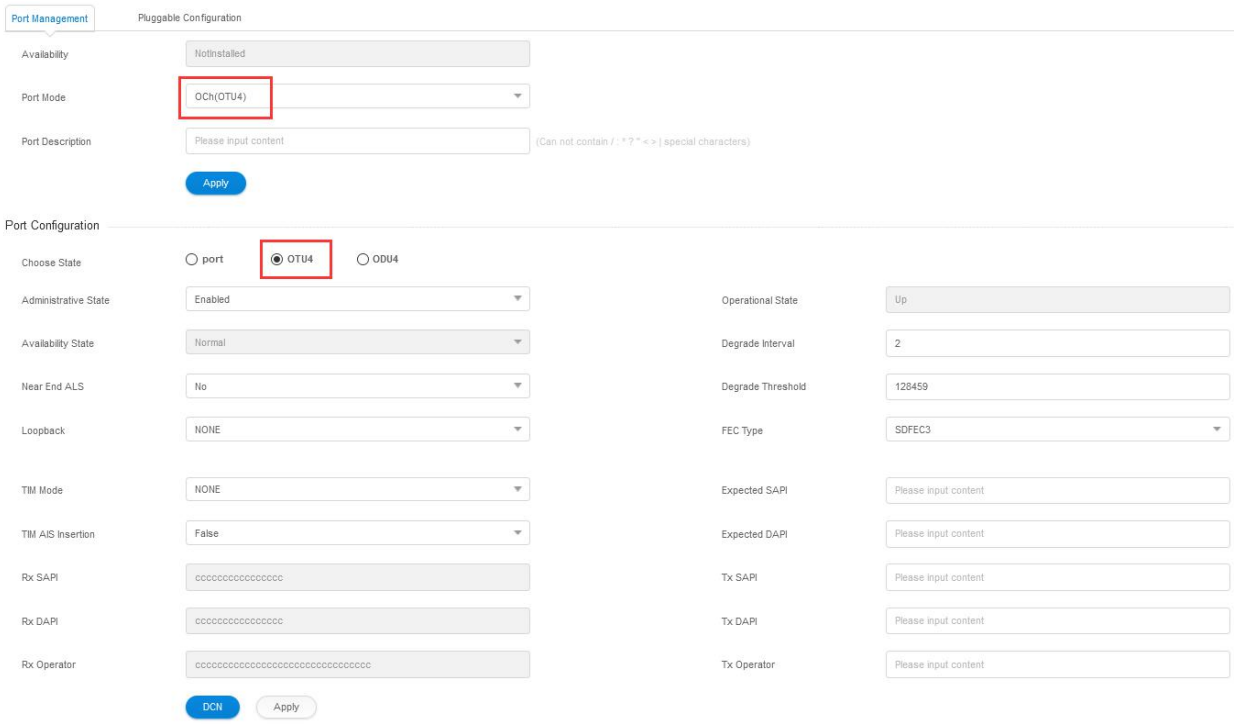


Figure 3-5 Preparation before Opening GCC Channel of OCh (OTU4)

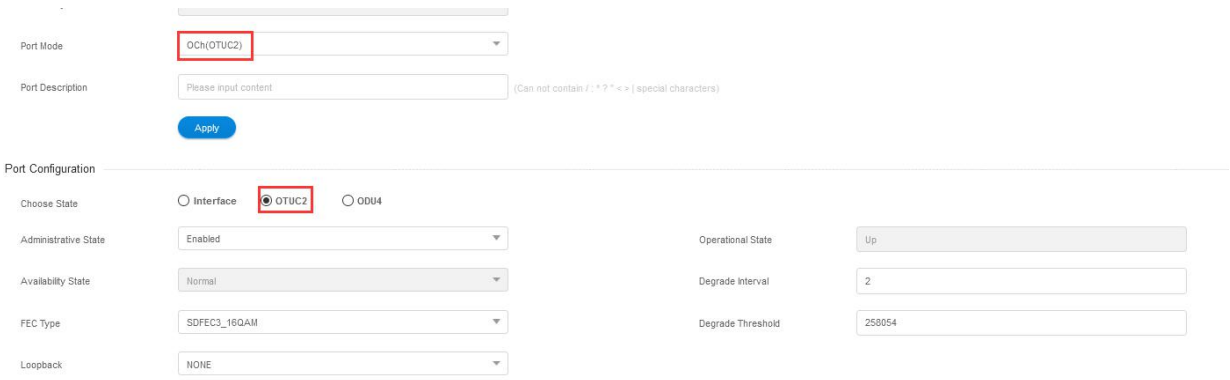


Figure 3-6 Preparation before Opening GCC Channel of OCh (OTUC2)

Then click on DCN in the lower right corner to enter DCN configuration interface. Select GCC type (The GCC type of ODU4 layer is GCC1 and GCC1+2), as shown in the figure below:

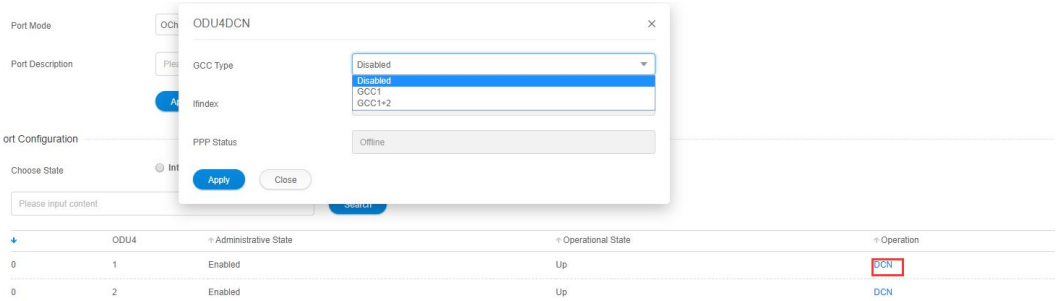


Figure 3-7 Open GCC Channel of ODU4 Layer

It needs to set the same GCC types of the occupied ports for adjacent NE.

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 "MGMT IP Configuration".

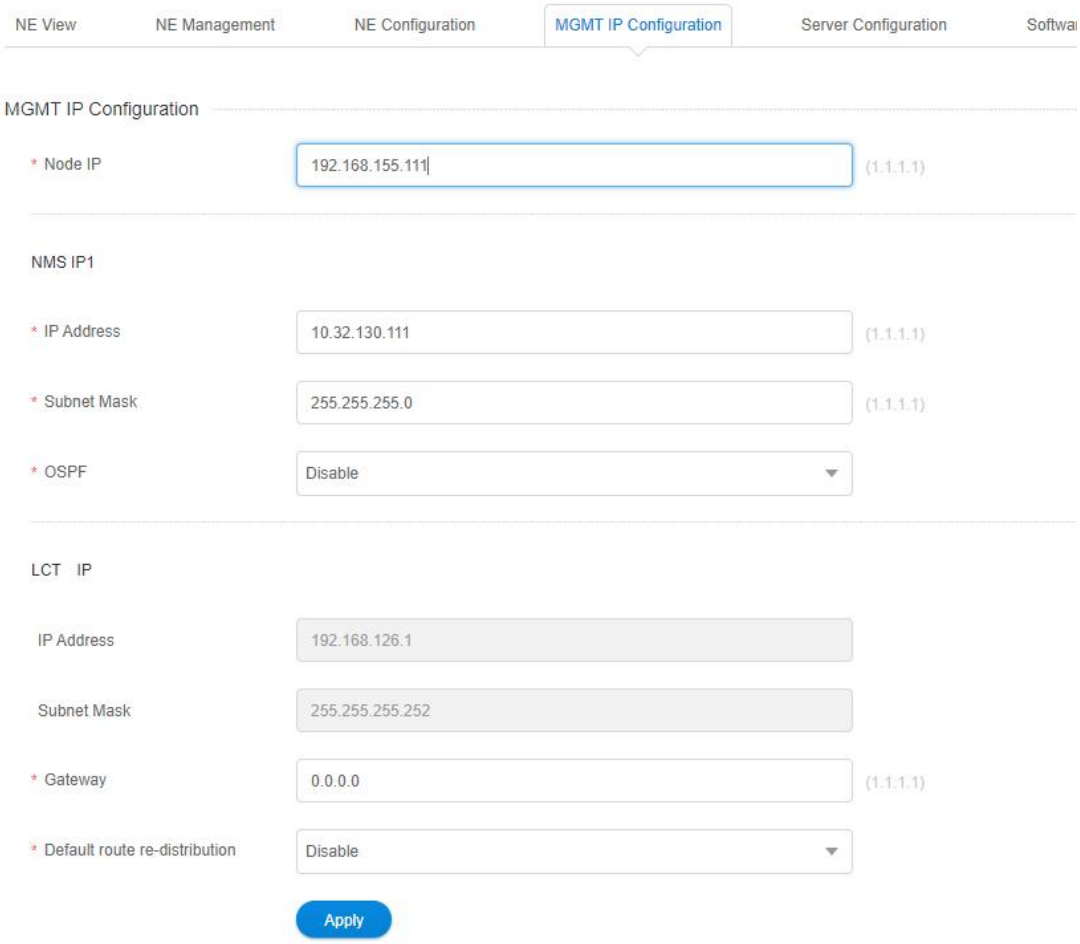


Figure 3-8 Select NE and MGMT IP Configuration

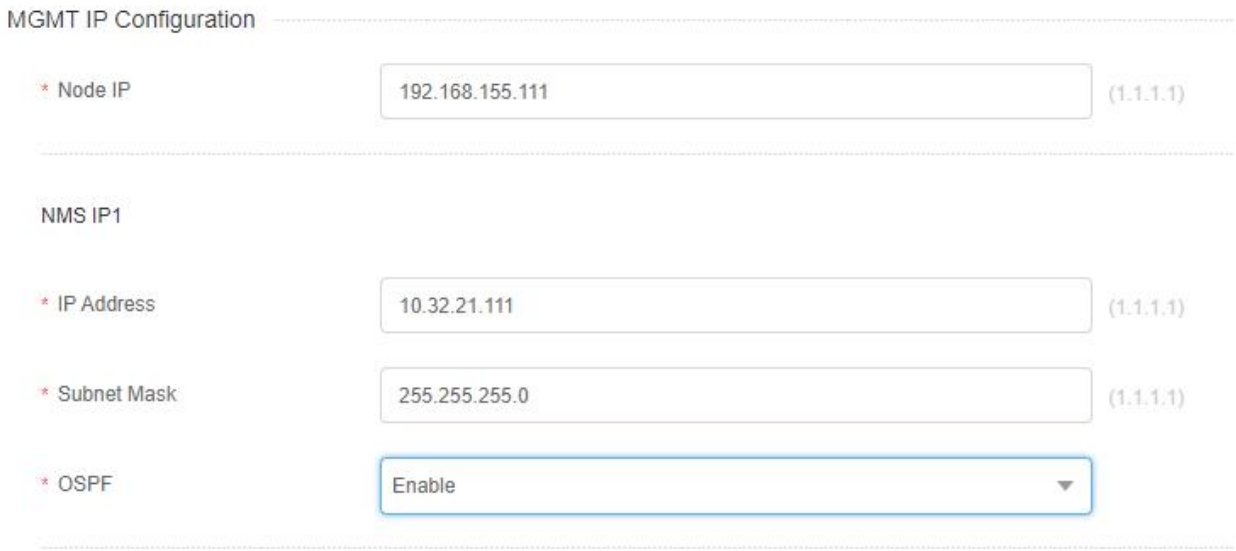


Figure 3-9 Open MGMT IP Configuration Interface

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.

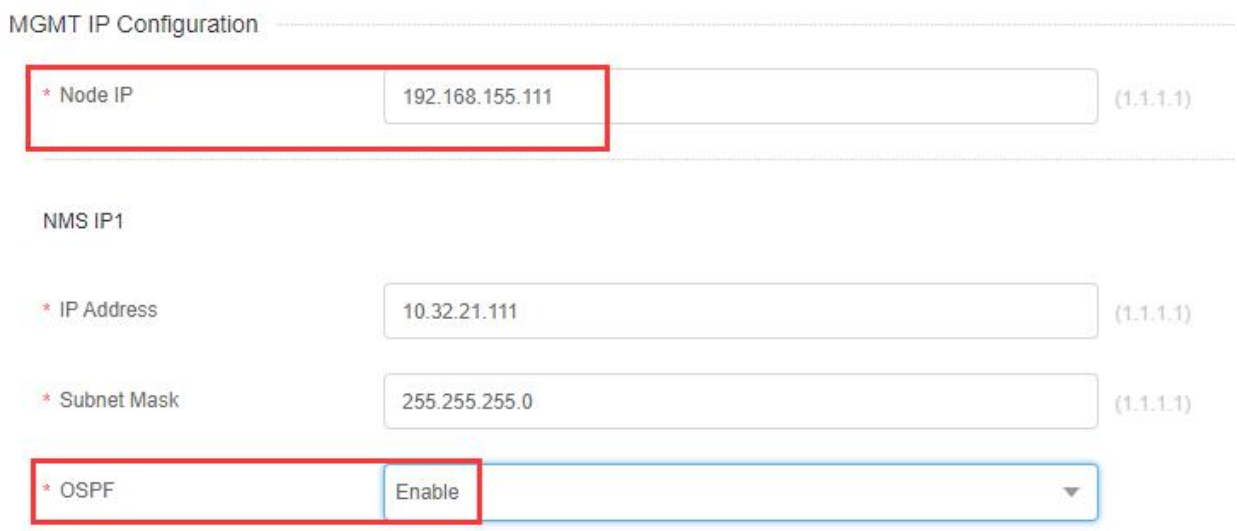


Figure 3-10 Configure Gateway NE IP

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.

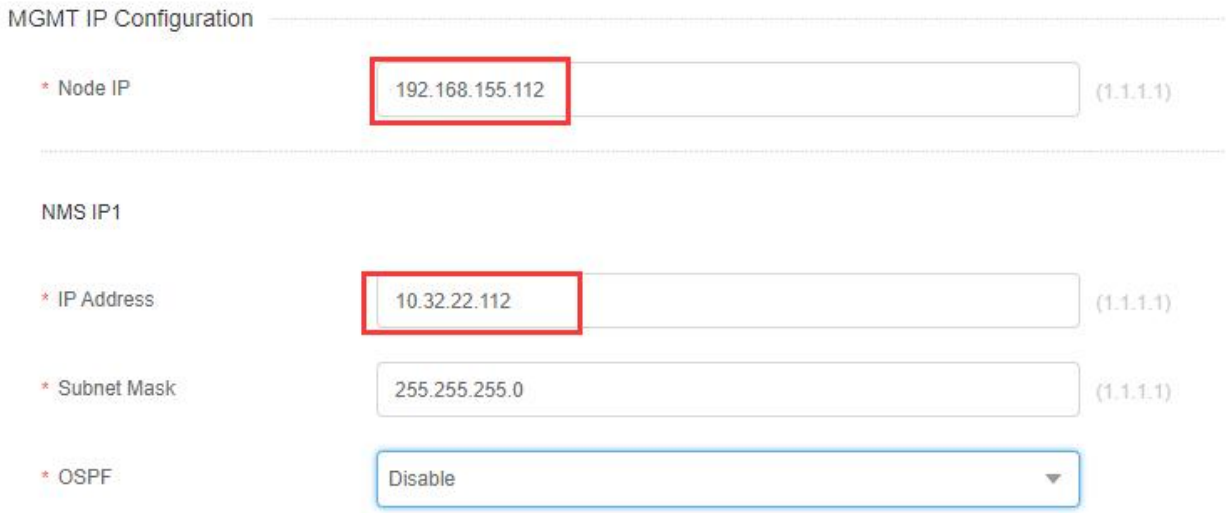


Figure 3-11 Configure Remote NE IP

Step 3:

Configure the route on the computer to run CMD as an administrator and enter the 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.

```
C:\WINDOWS\system32>route add 192.168.155.111 mask 255.255.255.255 192.168.21.111

C:\WINDOWS\system32>route add 192.168.155.112 mask 255.255.255.255 192.168.21.111
```

Figure 3-12 Add Local Route

Check the input route through route print command.

```
192.168.155.111   255.255.255.255   192.168.21.111   172.100.10.44   36
192.168.155.112   255.255.255.255   192.168.21.111   172.100.10.44   36
```

Figure 3-13 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:

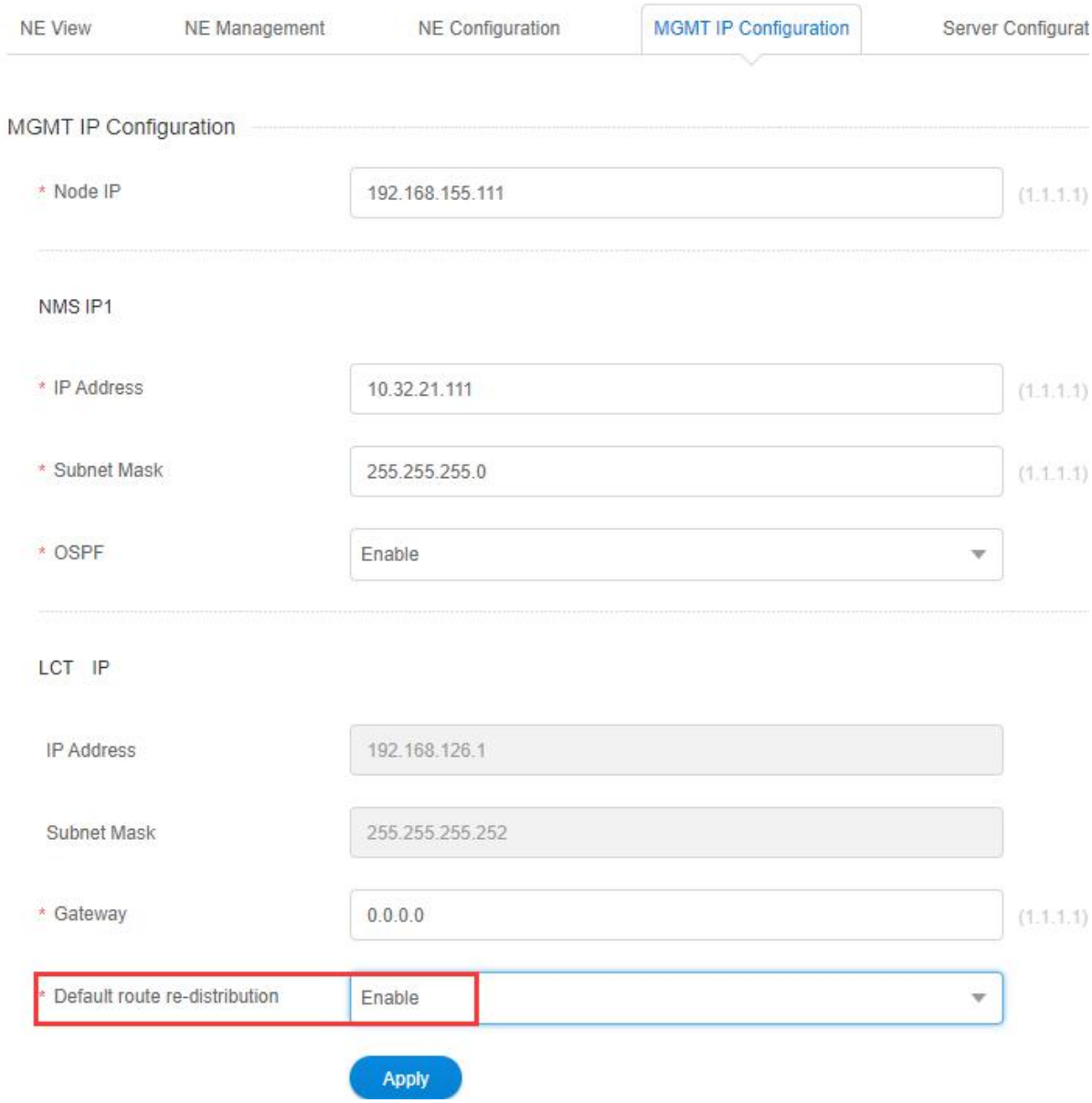


Figure 3-14 Enable Default Route Redistribution Function of the Gateway NE

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

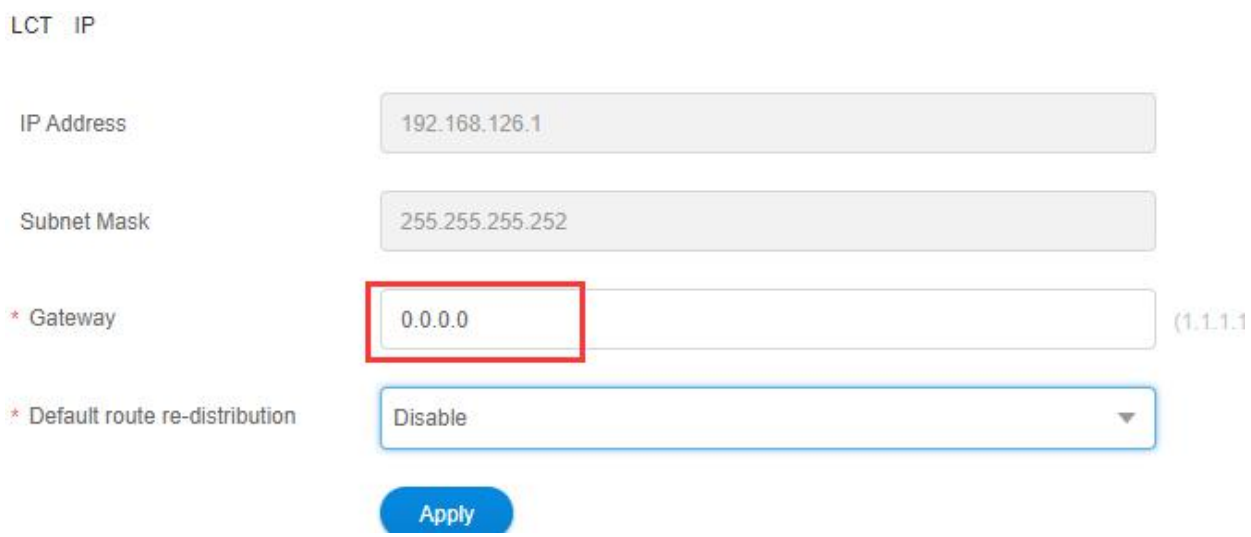


Figure 3-15 Modify Gateway

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.)

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 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 "*Shelf 01*", then select "*Shelf Information*"to open the Shelf information interface. Information such as Shelf type and temperature is displayed in this interface, as shown in Figure 4-1:

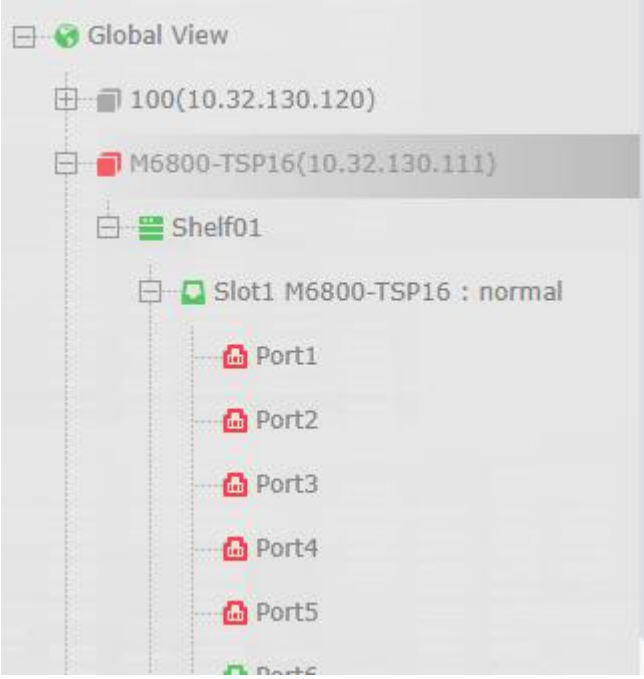


Figure 4-1 Operation Steps to View Shelf Information

4.1.1. M6800-TSP16 Shelf Information

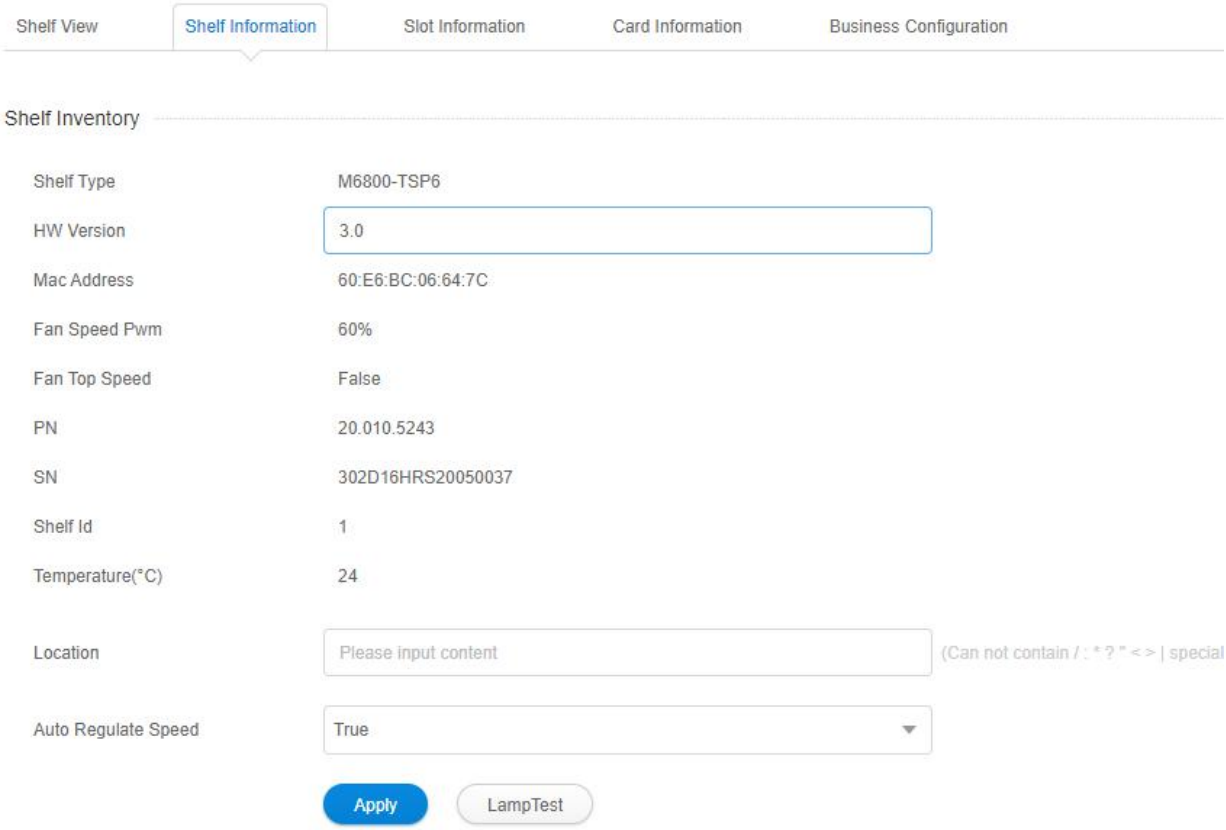


Figure 4-2 M6800-TSP16 Shelf Information

4.2. Indicator Light Information

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

4.2.1. NMU Module

Table 4-1 Indicator Light Status of Integrated NMU Module

		M6800-TSP16
NMU Control System Indicator Light (NMU Board, Service Board Integration)	SYS	Green Light Slow Flash: The system has successfully started. Green Light Always Off: The system has not started.
	ALM	Red Light Quick Flash: There is Critical alarm. Red Light Slow Flash: There is Major alarm of the device. Red Light Always ON: There is Minor alarm of the device. Red Light Off: There is no alarm of the device.

4.2.2. Fan Tray Indicator Light

Table 4-2 Fan Tray Indicator Light Status

		M6800-TSP16
Fan Tray Indicator Light	FAN (Two Colors)	Green Light Always ON: There is no alarm of the fan. Red Light Always ON: There is alarm of the fan.

4.2.3. Port Indicator Light of Service Board

Table 4-3 Port Indicator Light Status of Service Board

		M6800-TSP16
Service Board Port Indicator Light	Bi-Color Indicator Light	Always OFF: The port is disabled. Red Light Quick Flash: There is mismatch alarm of the port. Red Light Always On: There is los alarm of the port. Green Light Always On: There is no los and mismatch alarm of the port.

4.2.4. Power Tray Indicator Light

Table 4-4 Power Tray Indicator Light Status

		M6800-TSP16
Power Tray Indicator Light	PWR (Bi-Color Indicator Light)	Red Light Always ON: The power tray is not powered or there is failure of the power tray. Green Light Always ON: Normal power supply and there is no alarm of the power tray.

4.3. View Single Board Information

Select NE and click on "*Shelf 01*", and then select "*Card Information*".

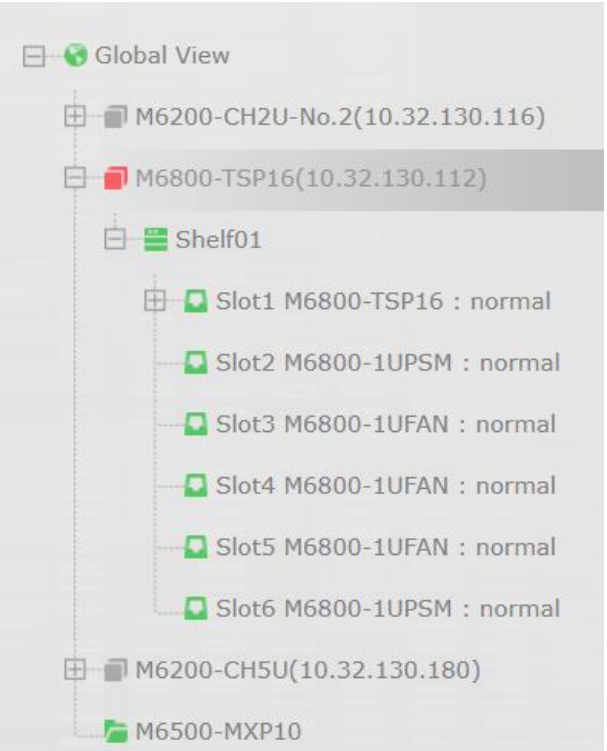
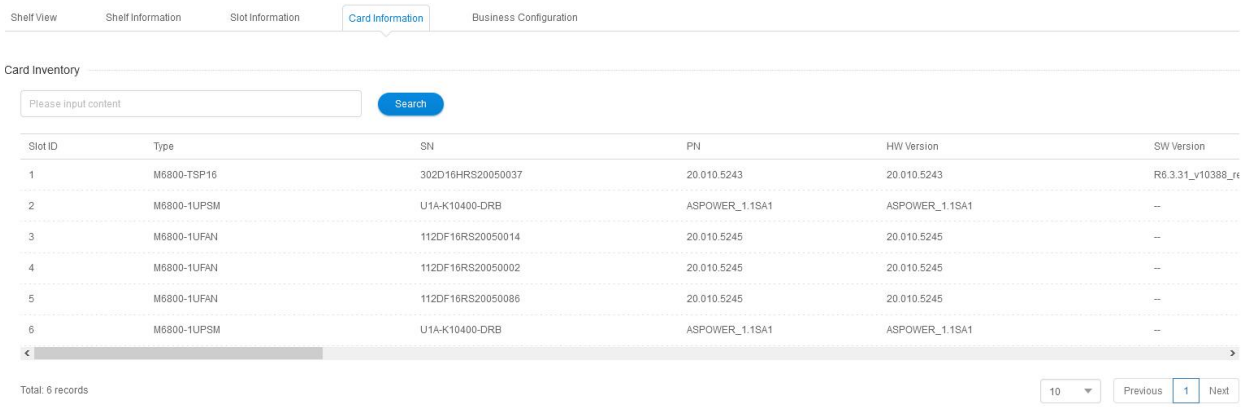


Figure 4-3 View Single Card Information

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



Slot ID	Type	SN	PN	HW Version	SW Version
1	M6800-TSP16	302D16HRS20050037	20.010.5243	20.010.5243	R6.3.31_v10388_re
2	M6800-1UPSM	U1A-K10400-DRB	ASPOWER_1.1SA1	ASPOWER_1.1SA1	--
3	M6800-1UFAN	112DF16RS20050014	20.010.5245	20.010.5245	--
4	M6800-1UFAN	112DF16RS20050002	20.010.5245	20.010.5245	--
5	M6800-1UFAN	112DF16RS20050086	20.010.5245	20.010.5245	--
6	M6800-1UPSM	U1A-K10400-DRB	ASPOWER_1.1SA1	ASPOWER_1.1SA1	--

Figure 4-4 Board Information Interface

4.4. View Slot Information

Select NE and click on “*Shelf 01*”, and then select “*Slot Information*”.

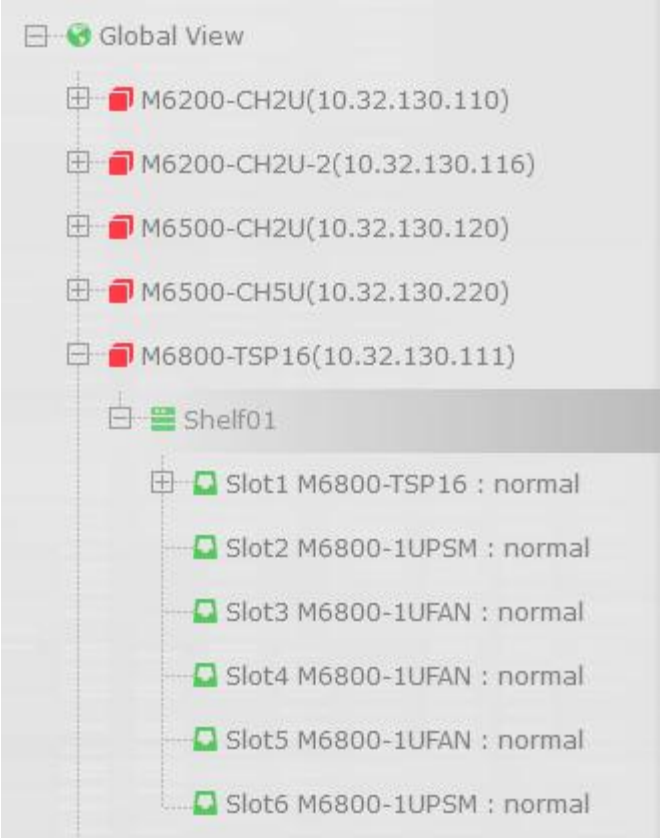


Figure 4-5 View Slot Information

After selecting “Slot Information”, the interface as shown in the figure below pops up. Information of every slot, pre-configured board, actual board, board status and board description can be checked in this interface.

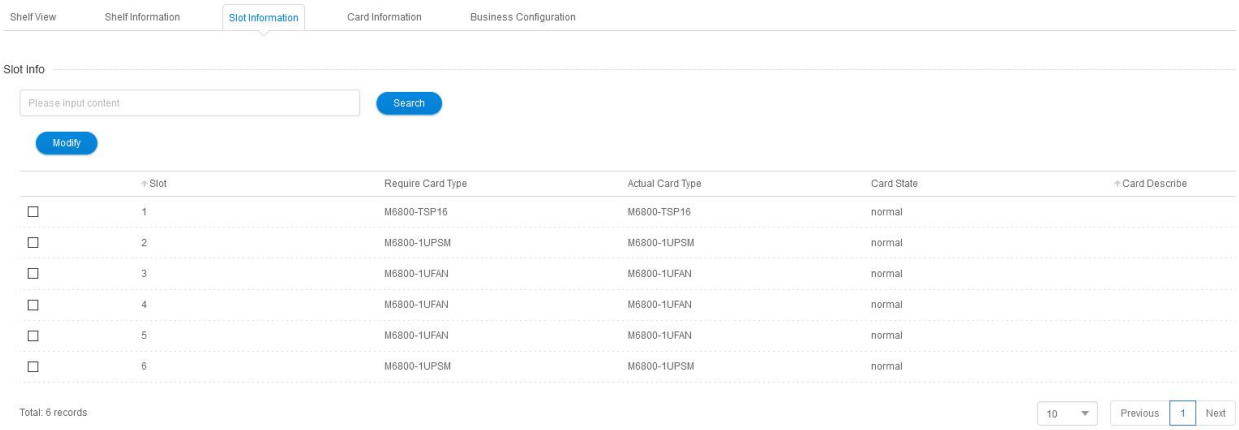


Figure 4-6 Slot Information Interface

4.5. Port Configuration

Select NE-Slot 1, Cick on"*Port 1*",as shown in the figure below:

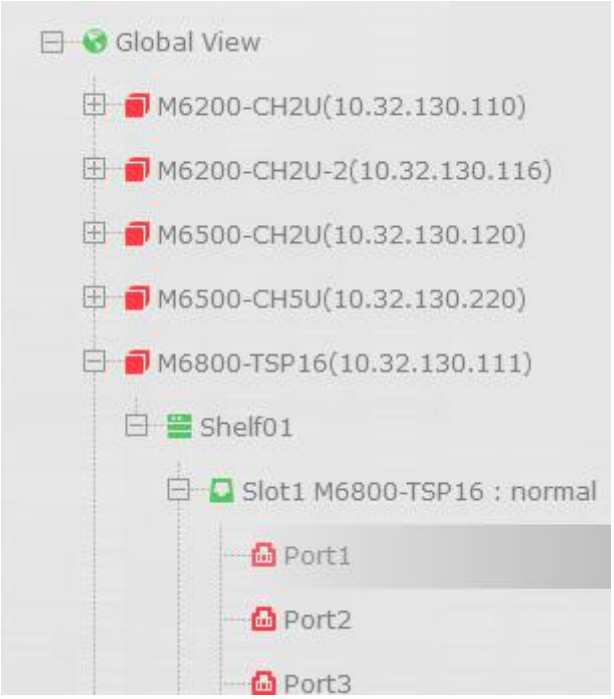


Figure 4-7 View Port Configuration Information

4.5.1. Basic Information

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

The client side port type supports: HGE_GMP.

The line side (system side) port type supports: OCh (OTU4), OCh (OTUC2).

Select NE-Slot 1, click on"*Port 3*", and select"*Port Configuration*", the interface as shown in the figure below pops up. The configuration status, port mode and port description can be modified in basic information.

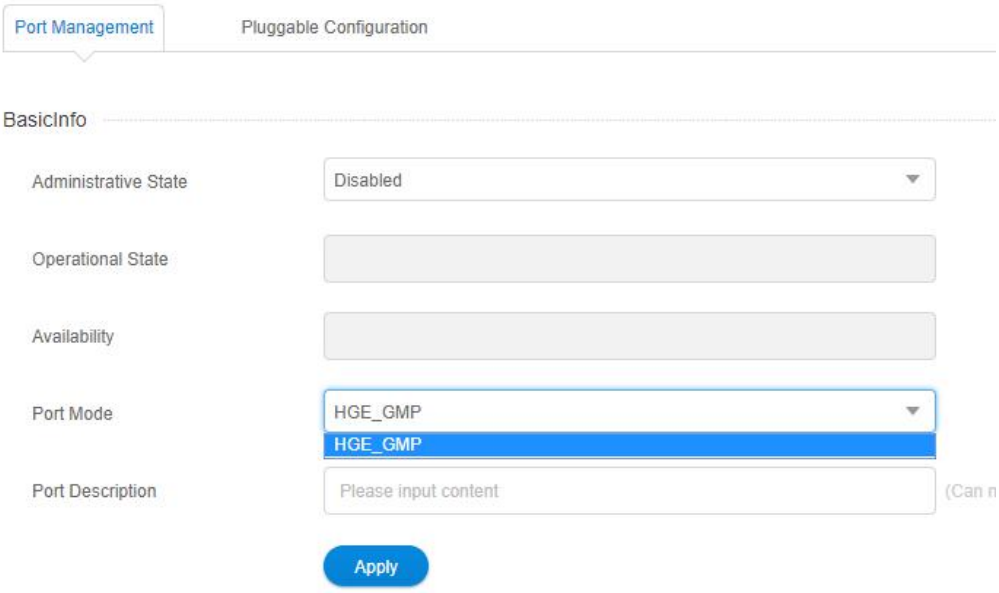


Figure 4-8 Port Management Interface

4.5.1.1. Interface Configuration

Select NE-Slot 1, click on"*Port 3*" and select"*Port Management*" , the port management interface pops up.

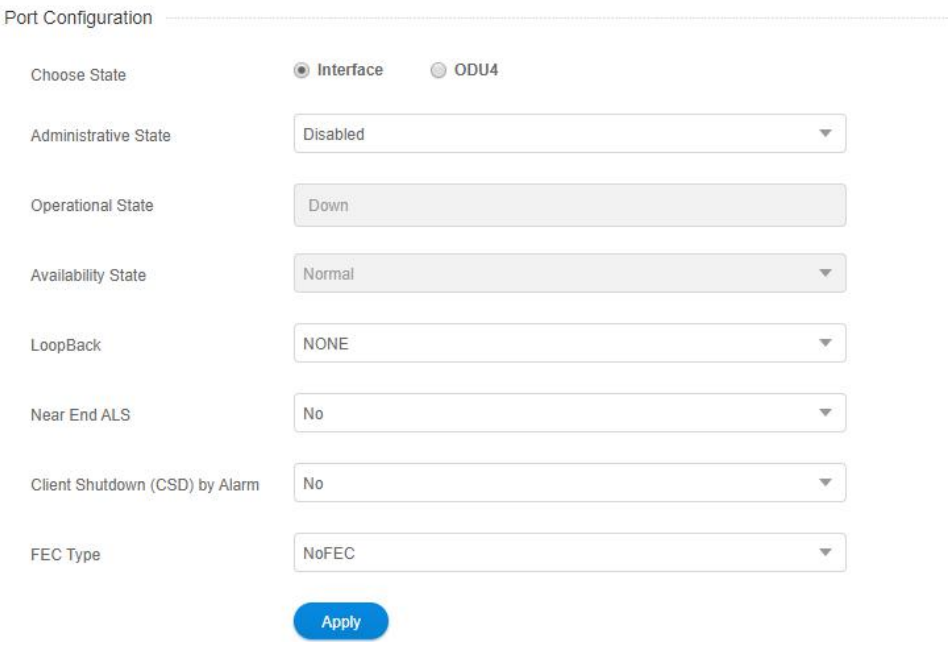


Figure 4-9 Port Management-Interface Information

4.5.1.2. OTU4 Configuration

Select NE-Slot 1, click on"*Port 1*"and select "*Port Management*", 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.

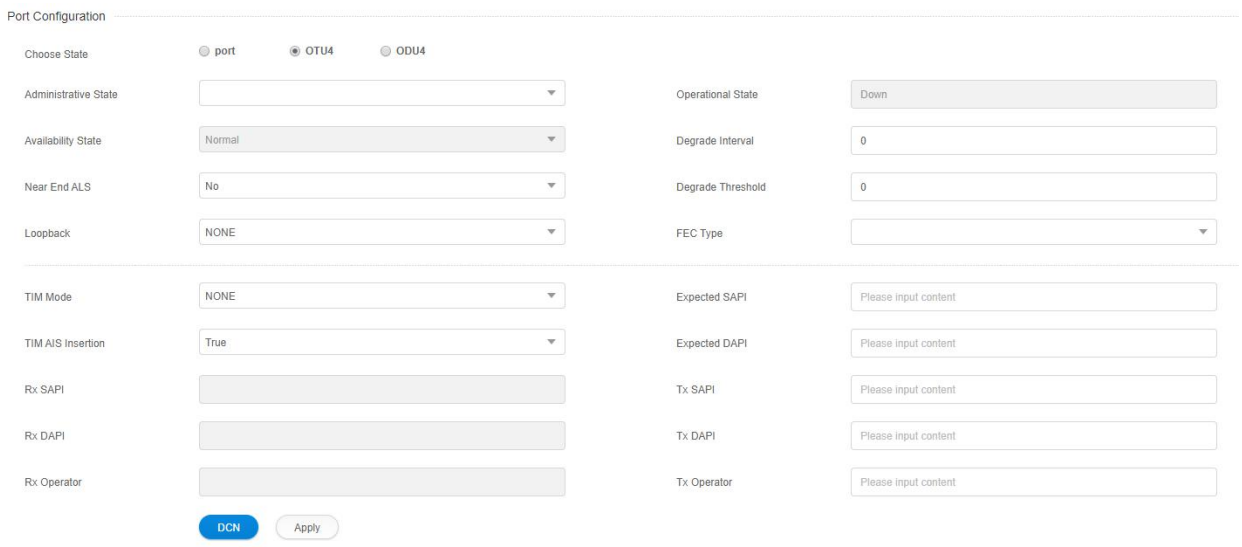


Figure 4-10 OTU4 Toolbar Interface

4.5.1.3. ODU4 Configuration

Select NE-Slot 1, click on"*Port 3*" and select"*Port Management*"(here we take ODU4 corresponding to HE_GMP port mode as an example), the port management interface pops up. Click on ODU4 option from"*Port Configuration*"in this interface, as shown in the figure below. It shows ODU4 toolbar interface.

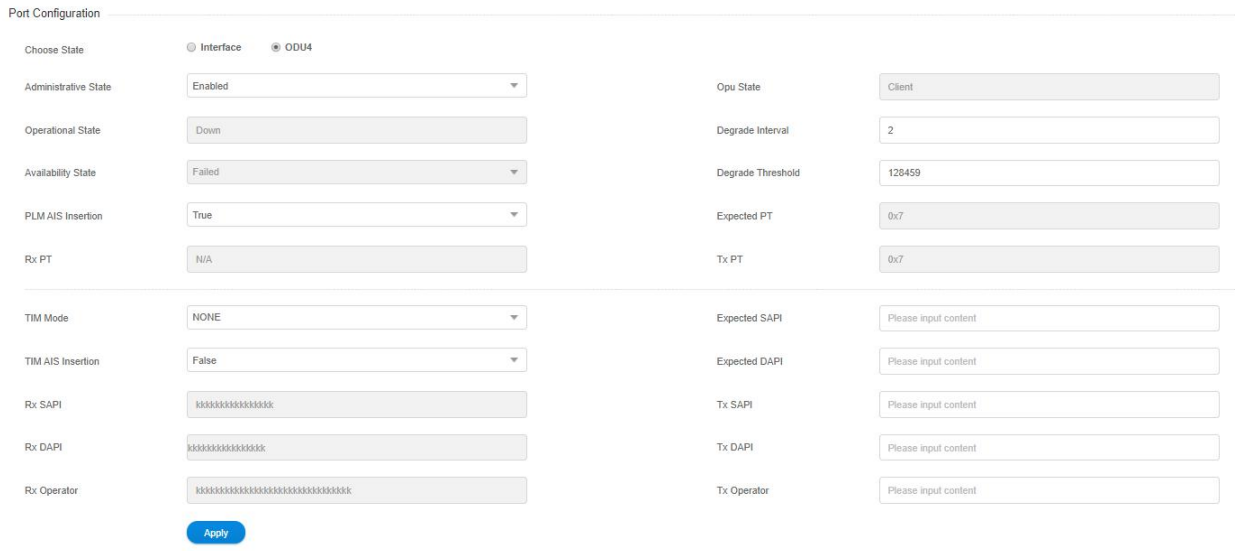


Figure 4-11 ODU4 Toolbar Interface

4.5.1.4. OTUC2 Configuration

Select NE-Slot 1, click on"*Port 1*"and select "*Port Management*", the port management interface pops 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.

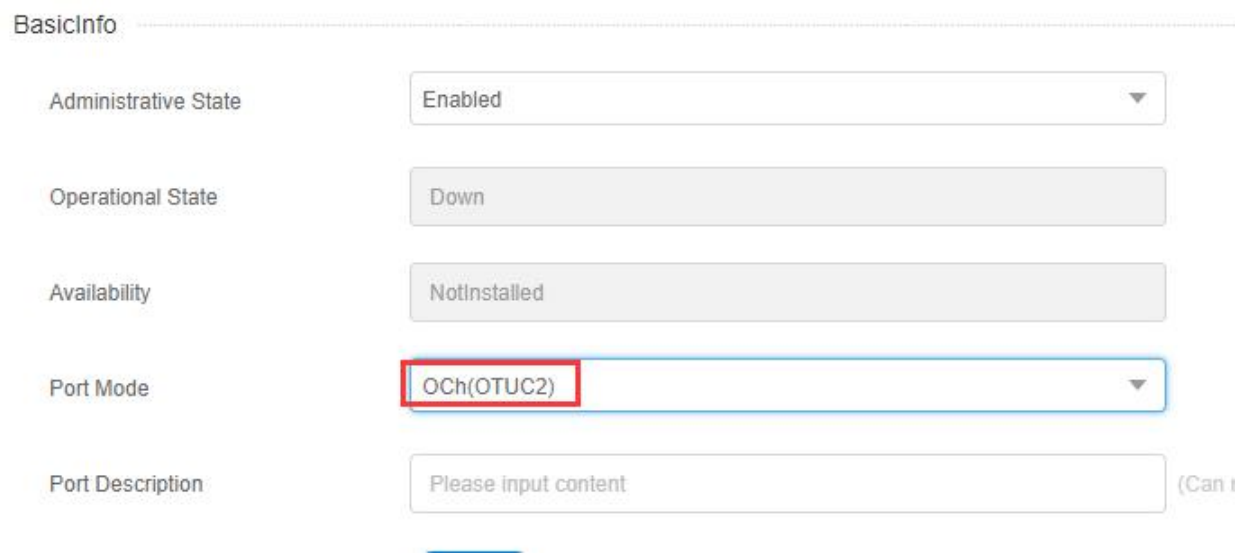


Figure 4-12 OTUC2 Toolbar Interface

4.5.1.5. ODUC2 Configuration

Select NE-Slot 1, click on"*Port 1*"and select "*Port Management*", the port management interface pops up （here we take ODUC2 corresponding to OCh (OTUC2) port mode as an example）. Click on ODUC2 option from"*Port Configuration*"in this interface, as shown in the figure below. It shows ODUC2 toolbar interface.

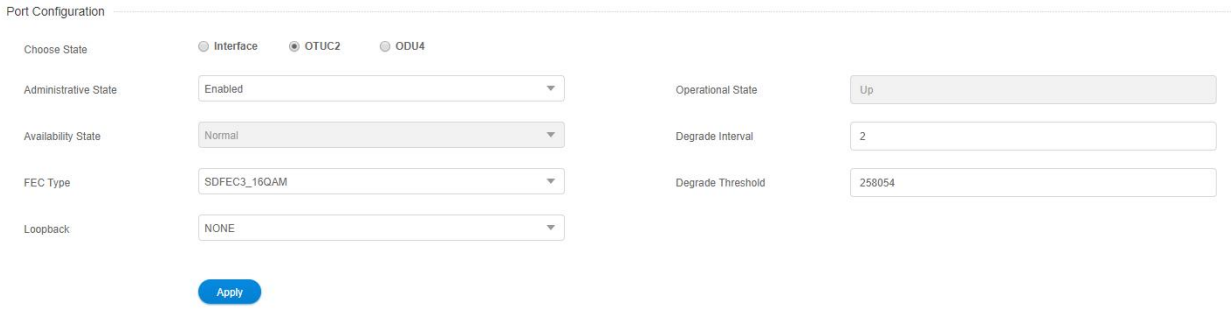


Figure 4-13 ODUC2 Toolbar Interface

4.5.2. Parameter Description

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

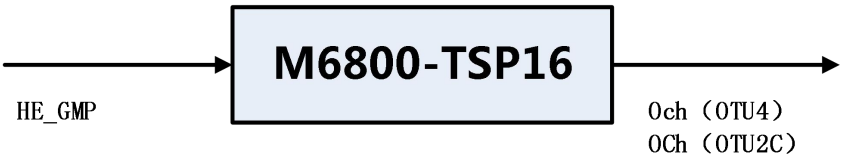


Figure 4-14 M6800-TSP16 Port Mode

Table 4-5 M6800-TSP16 Parameter Description

Item	Description
Maximum Capacity	1.6Tbit/s
Client Side Interface	16x QSFP28-based 100G interfaces

System Side Interface	8x CFP2-based 200G interfaces
Encryption Algorithm	AES-256 (In Developing)
Management Interface	2xRJ45 Ethernet port, 1 mini USB serial port
Management	Supports WEB/SNMP v2
In-band Management	Supports GCC0/1/2.

4.6. Configuration of Optical Module Information

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

Select NE-Slot, click on "*Port 1*"->"*Pluggable Configuration*",and select "*Pluggable BasicInfo*", as shown in the figure below:

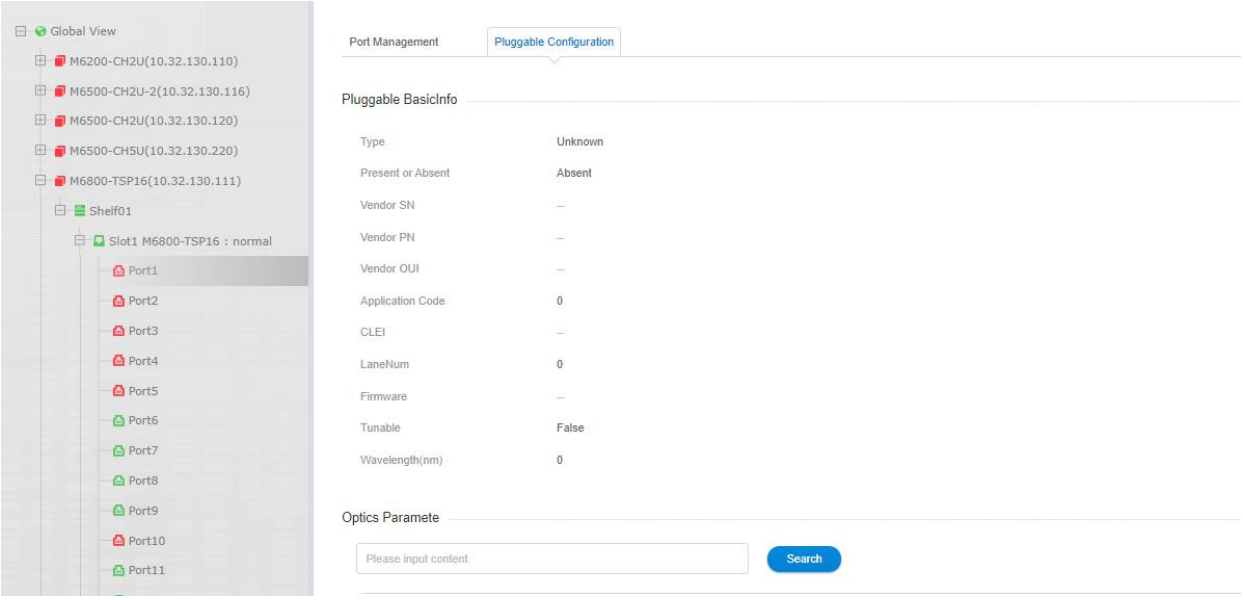


Figure 4-15 View Optical Module Information

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.

4.6.1. QSFP28 Optical Module Information

Figure 4-16 Basic Information of QSFP28 Optical Module

Figure 4-17 Parameter Information of QSFP28 Optical Module

4.6.2. CFP2 Optical Module Information

Configure the port mode as Och (OTUC2), insert a wavelength division CFP2 optical module, select the interface, and configure the working wavelength and transmit optical power of the optical module, as shown in the following figure.

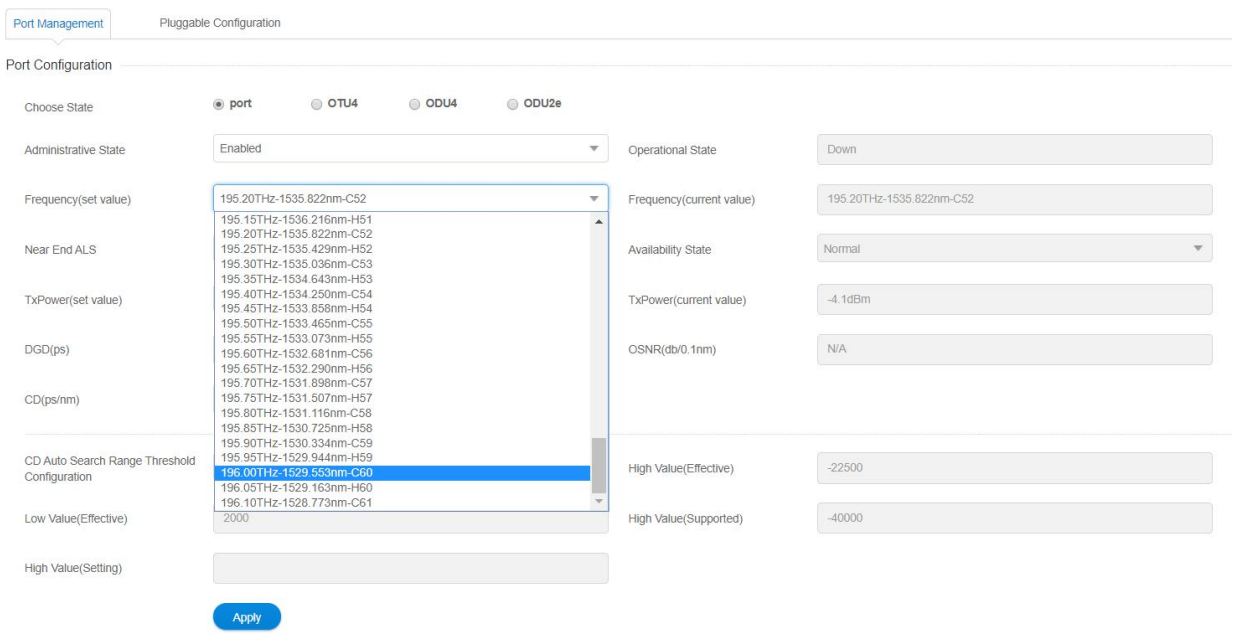


Figure 4-18 Basic Information of QSFP28 Optical Module

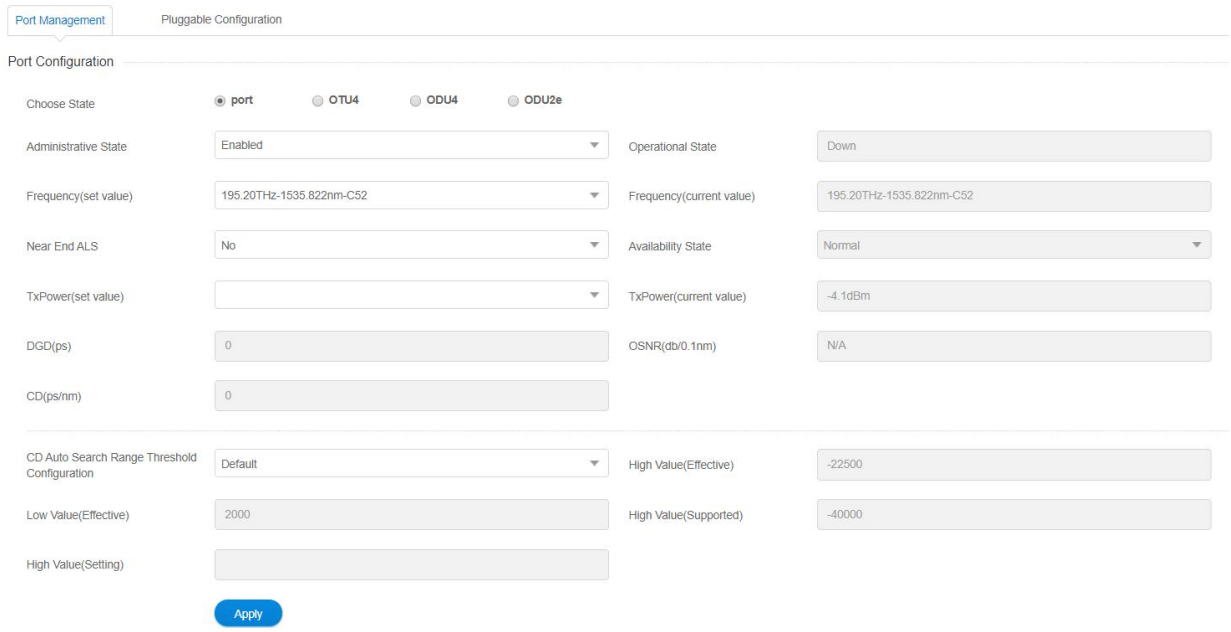


Figure 4-19 Parameter Information of QSFP28 Optical Module

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-connect. 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-connect without protection: one-way cross-connect, that is, the service is transmitted from site A--->site Z without line protection.
- Bidirectional cross-connect without protection: bidirectional cross-connect, that is, the service is transmitted from site A--->site Z and from site Z--->site A without line protection.
- Unidirectional cross-connect with protection: one-way cross-connect, 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-connect with protection: bidirectional cross-connect, 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').

Our company's M6800-TSP16 equipment temporarily does not support the protection function, so we only need to know unidirectional cross-connect without protection and bidirectional cross-connect without protection. Since the TP multiplexing structure and cross-connect of our M6800-TSP16 equipment are generated by fixed default, and by default it is bidirectional cross-connect without protection, there is no need to configure OTN electric cross-connect.

Configuration Steps

Select NE, click on"*Shelf 01*"and select"*Business Configuration*" , the operation steps are as shown in the figure below:

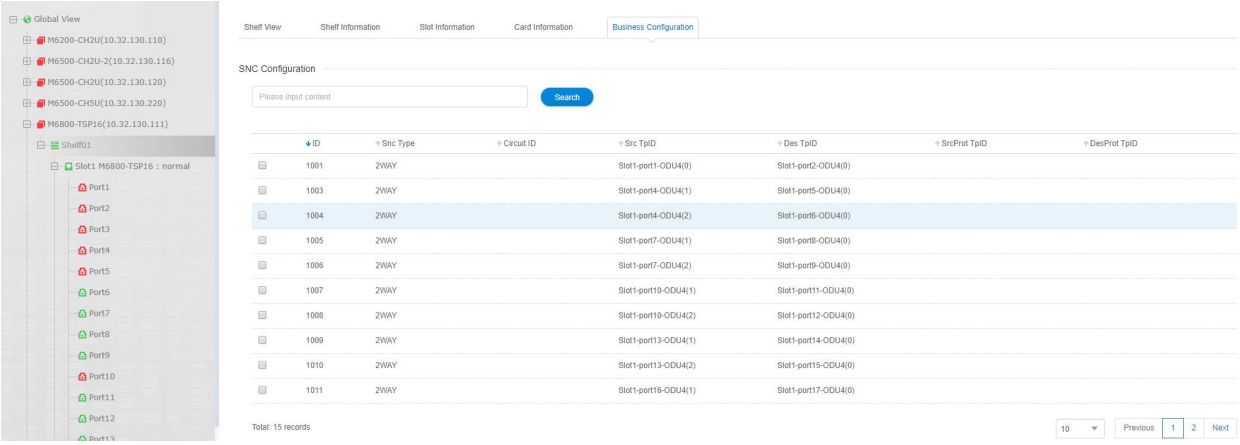


Figure 5-1 Operation Steps of Service Configuration

5.1.1. Bidirectional Cross-Connect without Protection

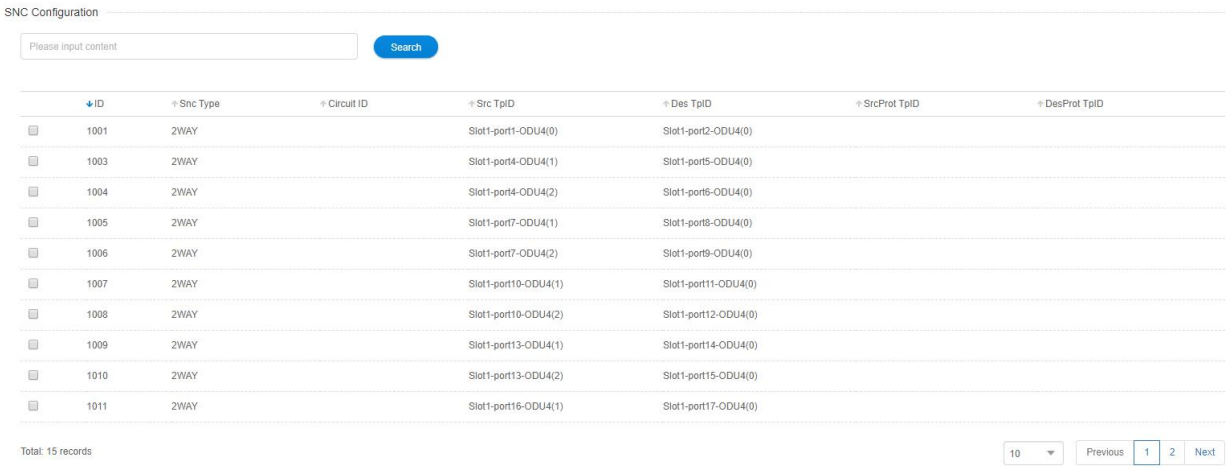


Figure 5-2 Configuration Result of Bidirectional Cross-Connect without Protection

5.2. Service Type

5.2.1. Service Type

Select NE-Slot 1, click on"*Port 2*"and select"*Port Management*", as shown in the figure below:

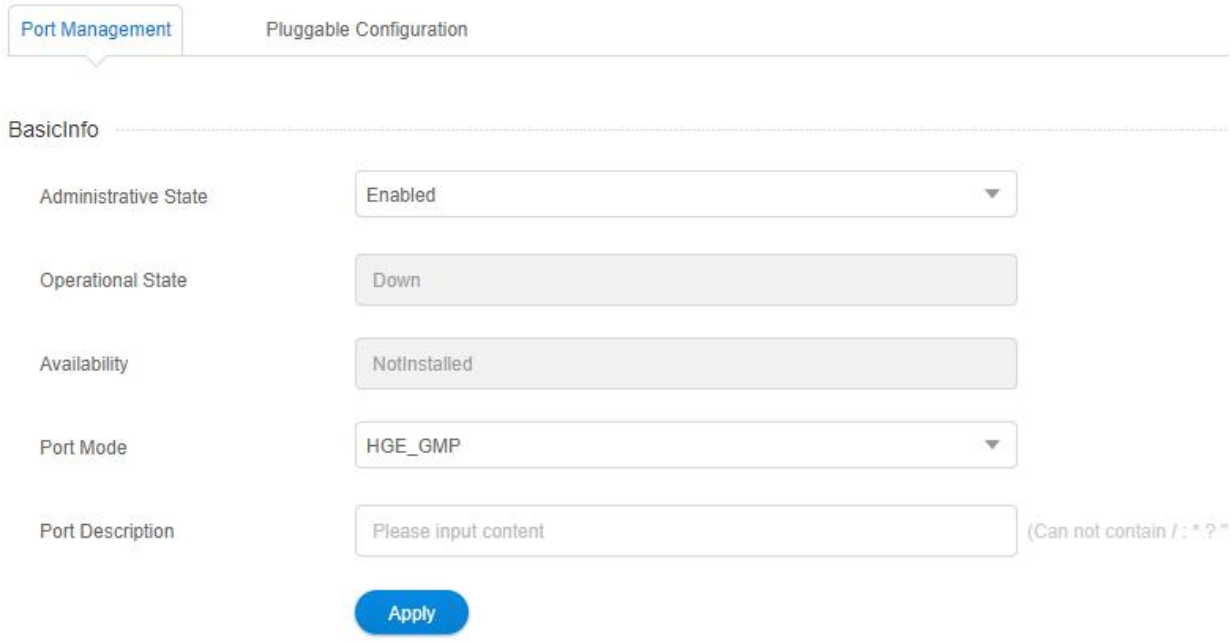


Figure 5-3 Operation Steps of How to View Service Type

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

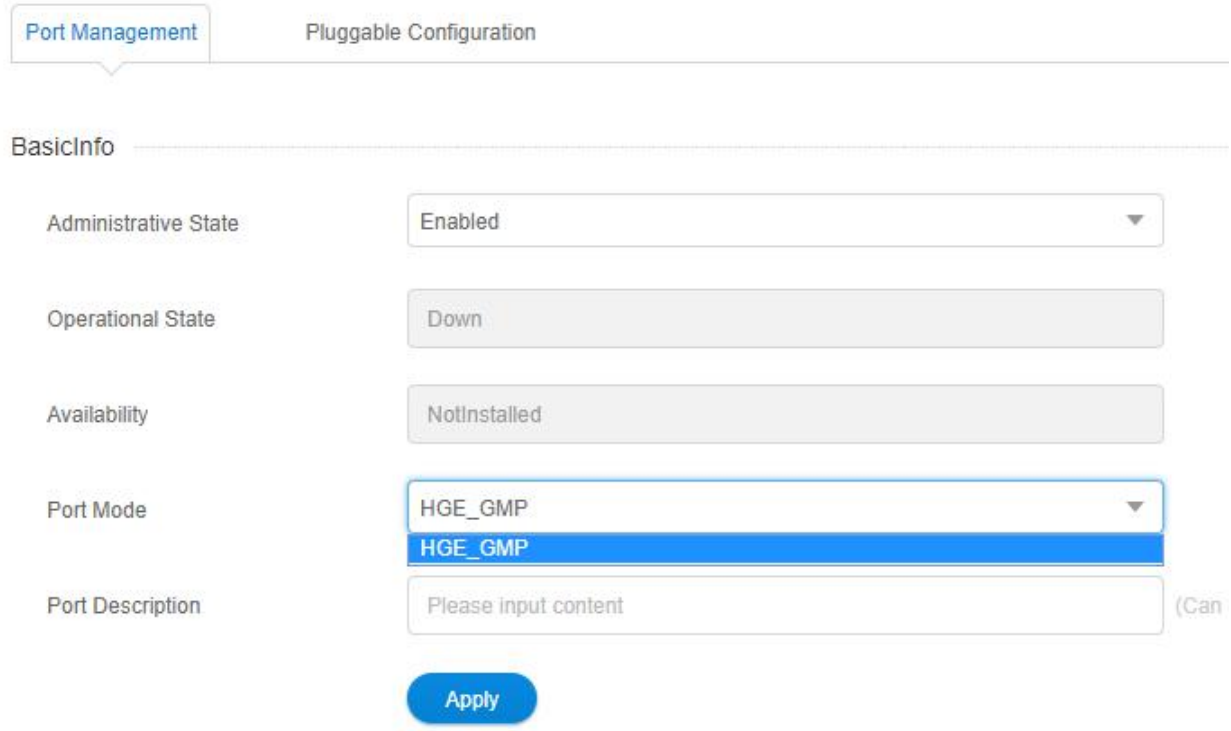


Figure 5-4 Port Mode Type Interface

5.3. Service Configuration Process

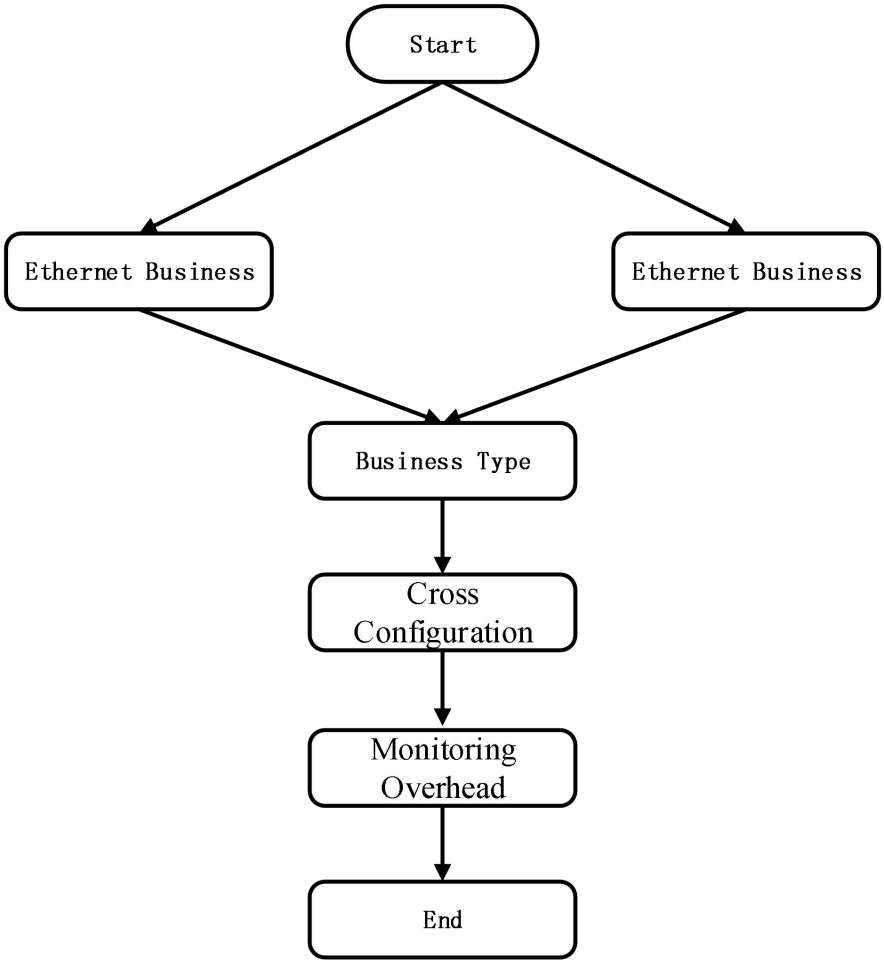


Figure 5-7 Service Configuration Process

5.4. Configuration Instructions

5.4.1. M6800-TSP16

M6800-TSP16 port type includes 1 (port 1)*200G/100G line side interface (CFP2) and 2 (port 2/3)*100G client side interfaces (QSFP28).

5.4.1.1. Service Type

- Line Side Port

Select NE-Slot 1, click on "*Port 1*"and select "*Port Management*", the operation steps are as shown in the figure below:

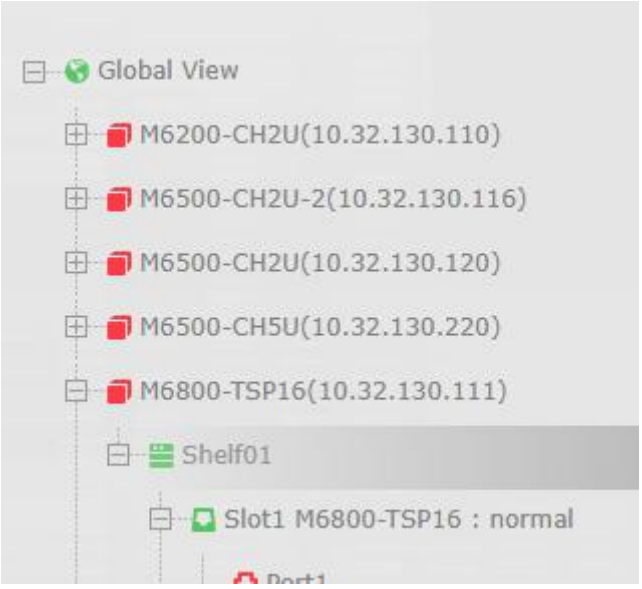


Figure 5-8 Operation Steps of M6800-TSP16 Line Side Port Information

The line side port management interface is as shown in the figure below. You can select the service type in port mode.

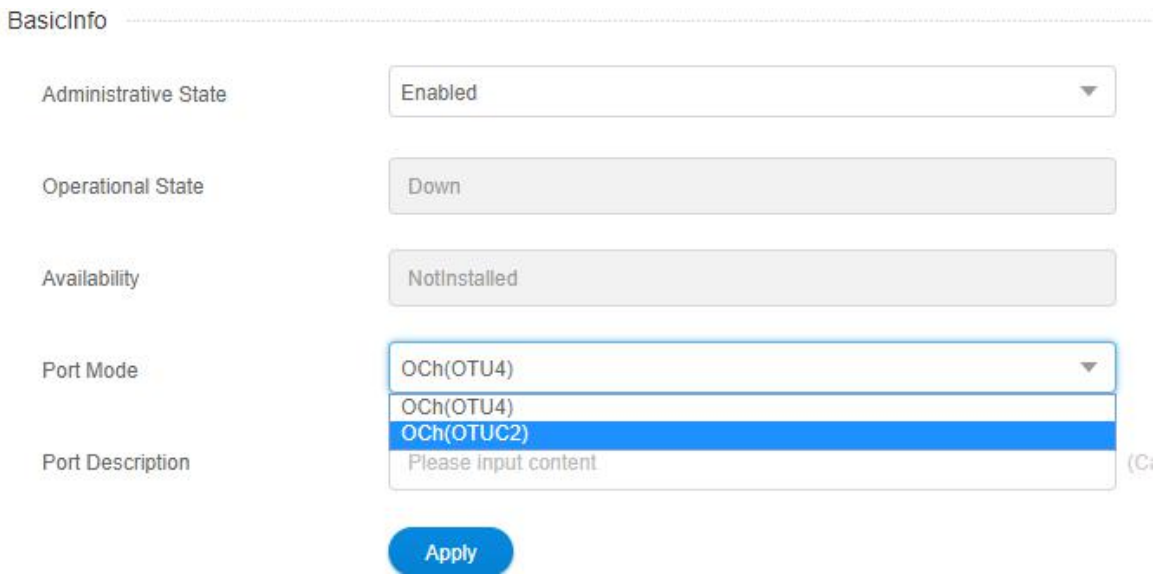


Figure 5-9 M6800-TSP16 Line Side Port Interface

- Client Side 100G Port

Select NE-Slot 1, click on "*Port 2*"and select "*Port Management*" , the operation steps are as shown in the figure below:

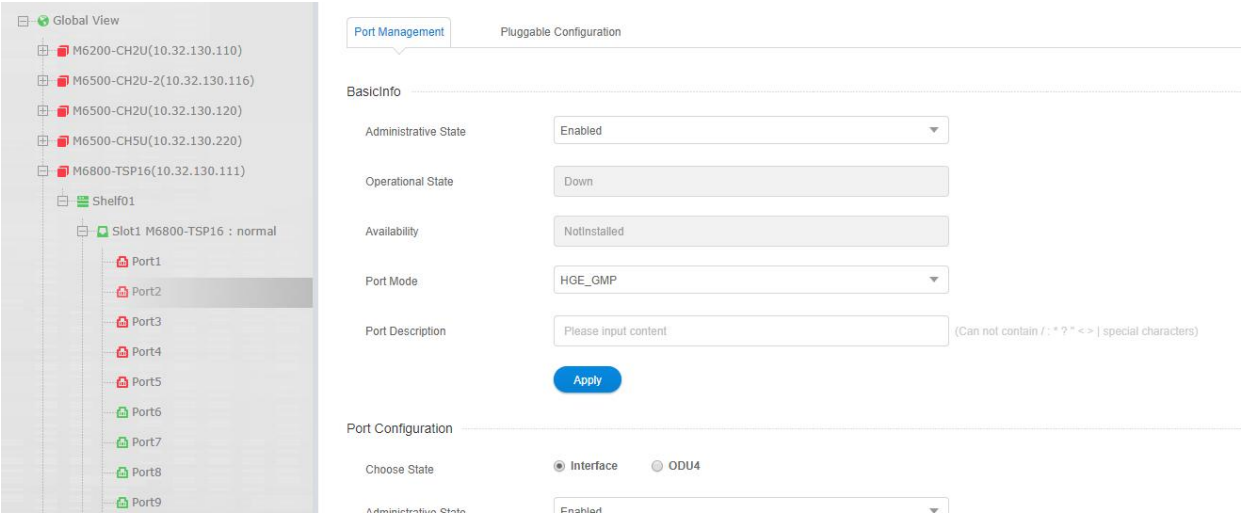


Figure 5-10 Operation Steps of M6800-TSP16 Client Side 100G Port Information

The client side port management interface is as shown in the figure below. You can select the service type in port mode.

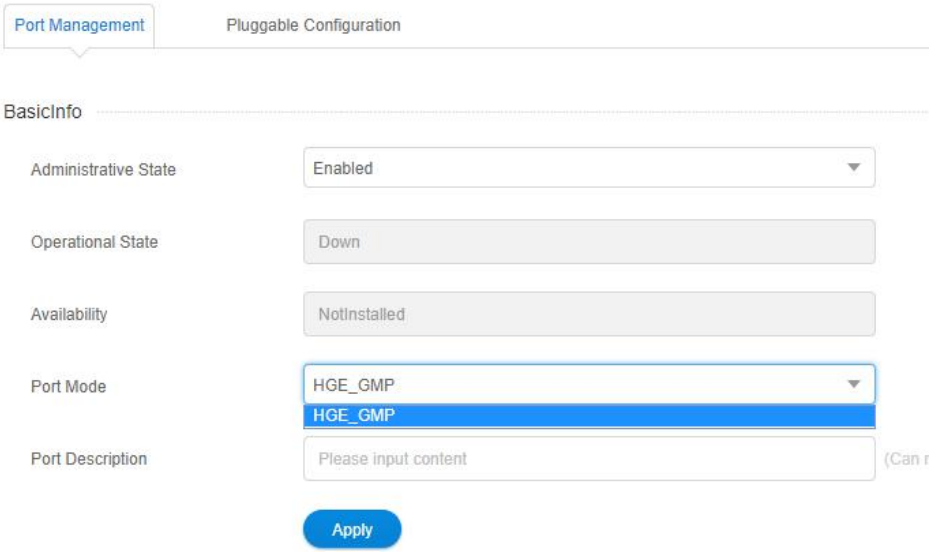


Figure 5-11 M6800-TSP16 Client Side 100G Port Interface

5.4.1.2. FEC Configuration

FEC is configurable only on OTU layer.

- Line Side Port

Select NE-Slot 1, click on"*Port 1*"and select "*Port Management*" to open the port management interface and select OCh (OTU4) as the port mode. Select "*FEC Type*"option in "*OTU4*" interface of "*Port Configuration*" to check the configuration. There are in all 4 FEC modes for the line side, which are respectively G709FEC/SDFEC1/SDFEC2/SDFEC3. SDFEC3 is the default mode. The configuration is as shown in the figure below:

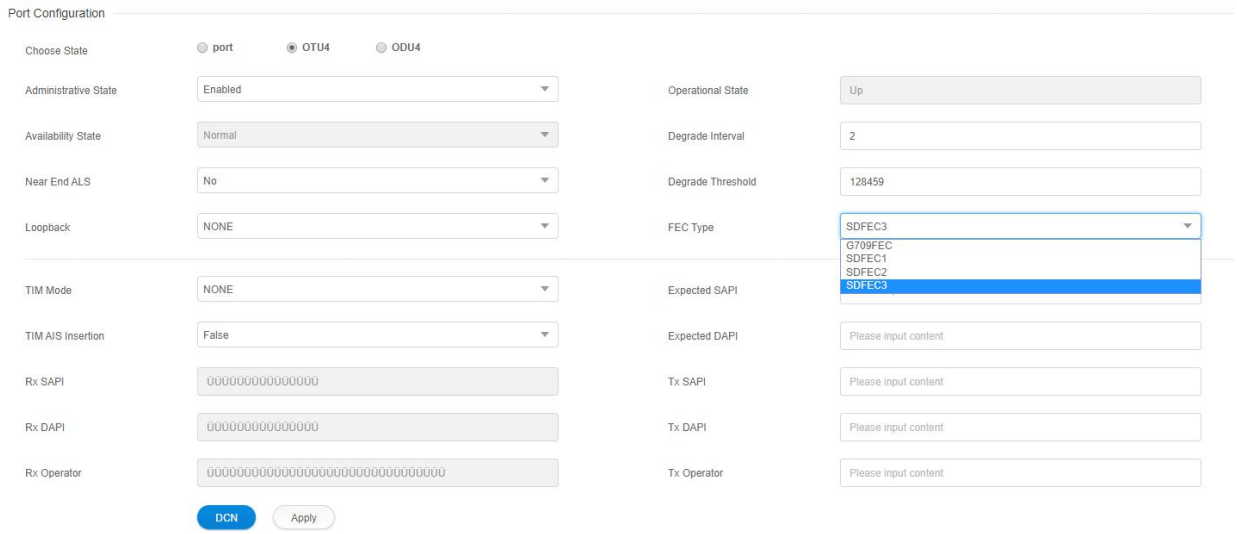


Figure 5-12 FEC Configuration of M6800-TSP16 Line Side Port OTU4

Select NE-Slot 1, click on"*Port 1*"and select "*Port Management*" to open the port management interface and select OCh (OTUC2) as the port mode. Select "*FEC Type*"option in "*OTUC2*" interface of "*Port Configuration*" to check the configuration. There are in all 6 FEC modes for the line side, which are respectively SDFEC1_8QAM/SDFEC2_8QAM/SDFEC3_8QAM/SDFEC1_16QAM/SDFEC2_16QAM/SDFEC3_16QAM. SDFEC3_16QAM is the default mode. The configuration is as shown in the figure below:

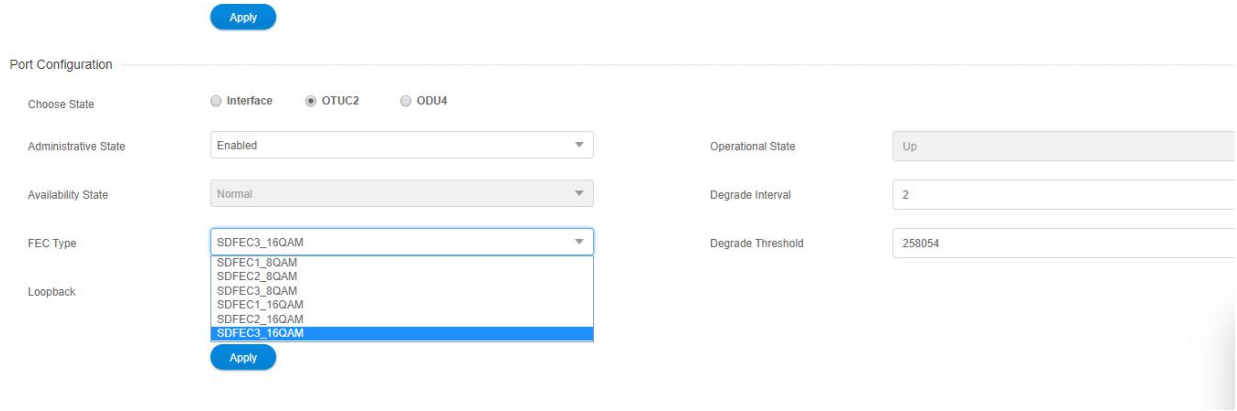


Figure 5-13 FEC Configuration of M6800-TSP16 Line Side Port OTUC2

- Client Side 100G Port

Select NE-Slot 1, click on"*Port 2*"and select "*Port Management*" to open the port management interface and select HE_GMP as the port mode. Select "*FEC Type*"option in "*Interface*" interface of "*Port Configuration*" to check the configuration. There are in all 2 FEC modes for the client side, which are respectively No-FEC and RS_FEC. No-FEC is the default mode. The configuration is as shown in the figure below:

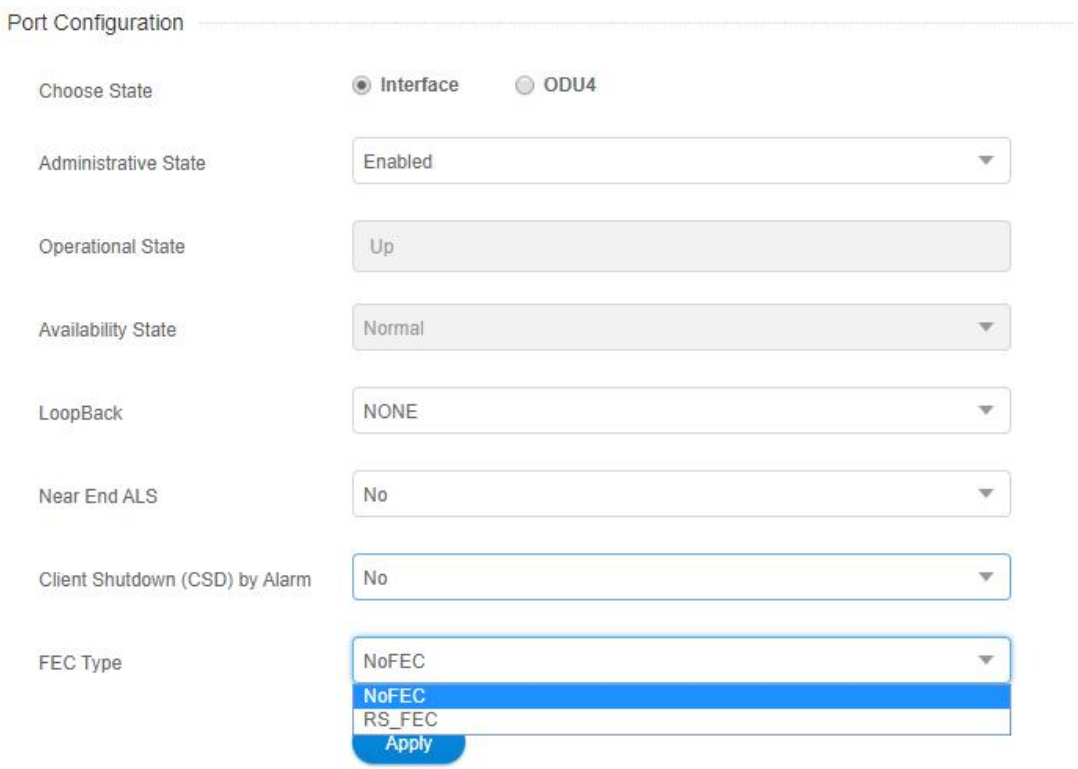


Figure 5-14 FEC Configuration of M6800-TSP16 Client Side 100G Port

Note: When SR4 or CWDM4 optical modules are used at the client side, it needs to enable the RS_FEC function of the port according to actual requirements.

5.5. Configuration Example

5.5.1. Configuration Example of Service Transparent Transmission

Here we take site-to-site transmission between Site A and Site B of LR4 100GE service as an example.

Configure the service type of the client side port2-port3 as HGE_GMP, and configure the mode of the line side port1 as OCh (OTUC2), and then enable the ports at the client side and the line side.

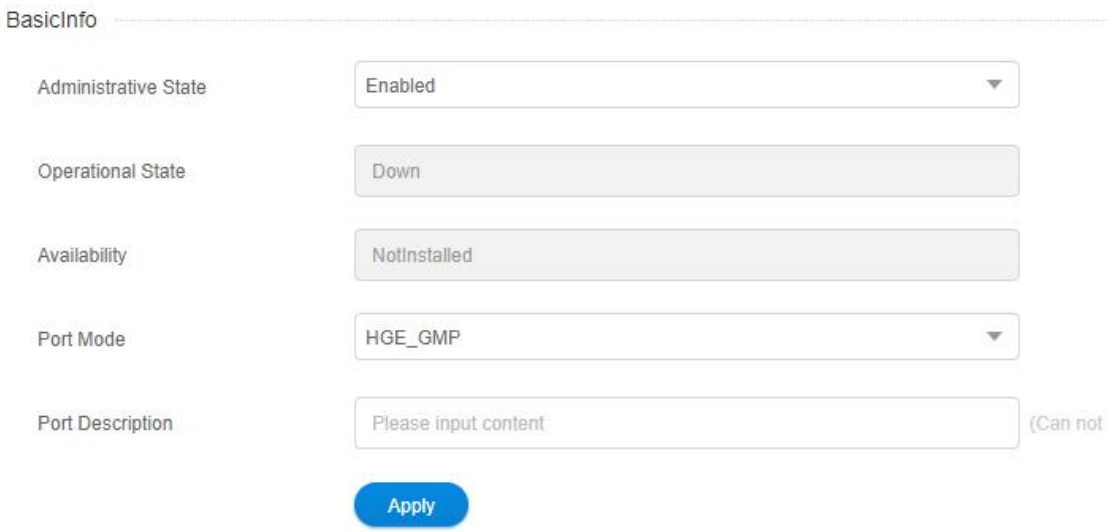


Figure 5-15 Configure Client Side Signal Mode

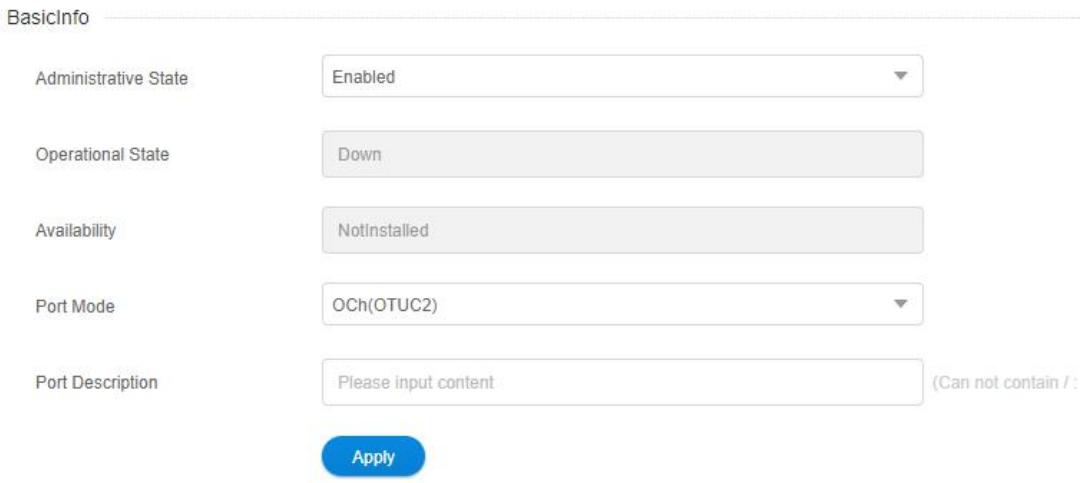


Figure 5-16 Configure Line Side Signal Mode

Build the environment according to the following diagram.

Figure 5-17 Site-to-Site Transmission Environment

Note:

- Ensure that the client side service types including mapping methods of Site A and Site B are the same.
- Ensure that the line side FEC types of Site A and Site B are the same.

6. Alarm Management

6.1. 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 several types and four levels of failures. It includes types such as equipment alarm, communication alarm, service quality alarm, environment alarm and error processing alarm. The four levels are emergency, primary, secondary and warning.

6.2. Main Interface of Alarm Management

After logging in the NMS system, click "*Maintain*"on the top bar –> click on the "*Alarm Management*" menu -- the alarm management sub-menu appears, which includes: current alarm, history alarm and Ethernet events.

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.

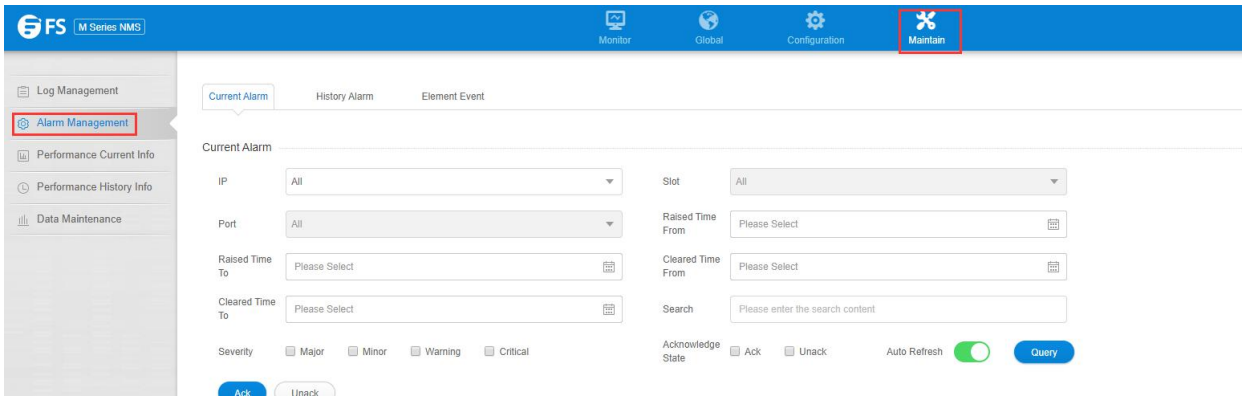


Figure 6-1 Alarm Management

6.2.1. Current Alarm

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

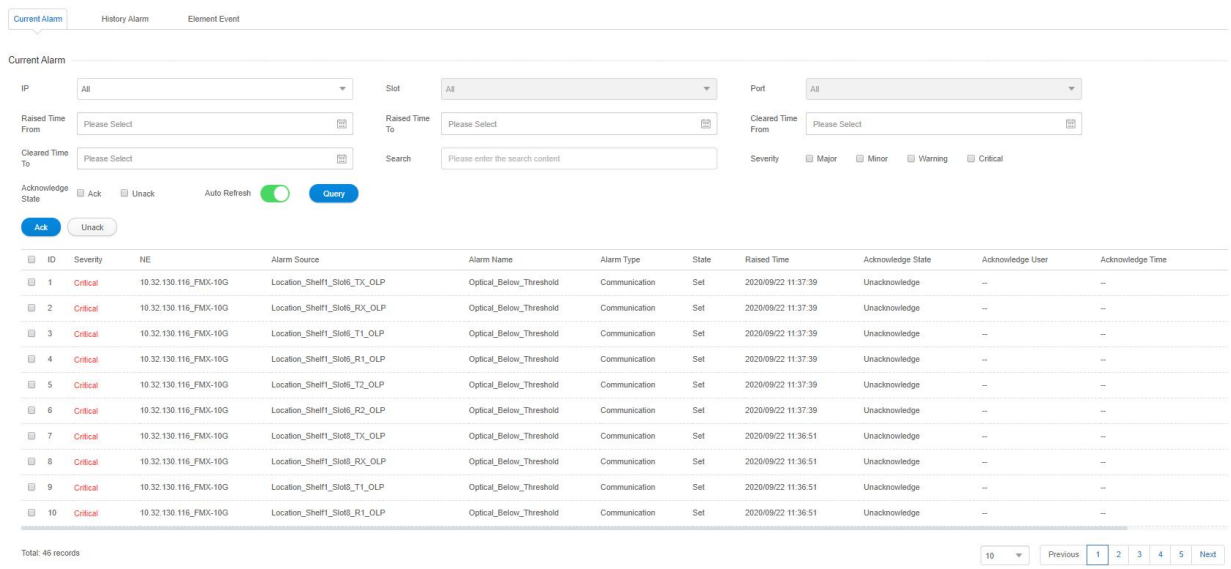


Figure 6-2 Current Alarm

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).

Figure 6-3 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 "Confirm" button, the selected alarms are all in the confirmation state. The confirmation status of the confirmed alarm is "*Ack*" 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.

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

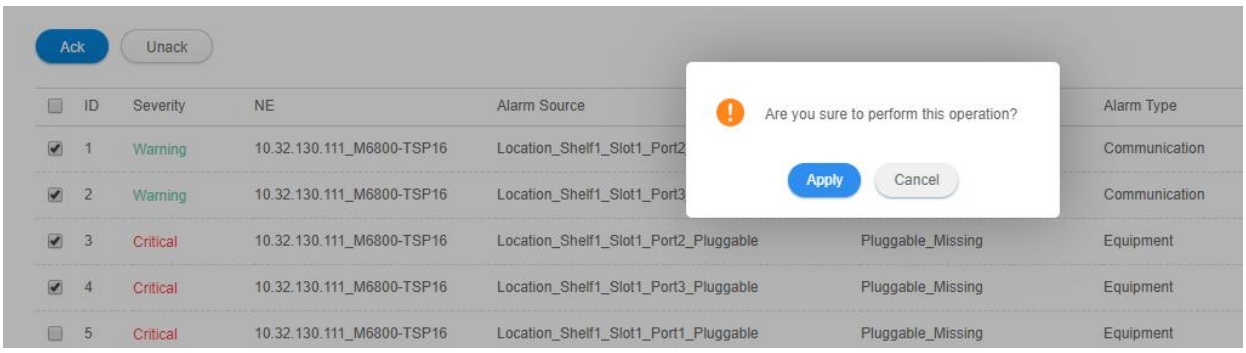


Figure 6-4 Select to Confirm Current Alarm

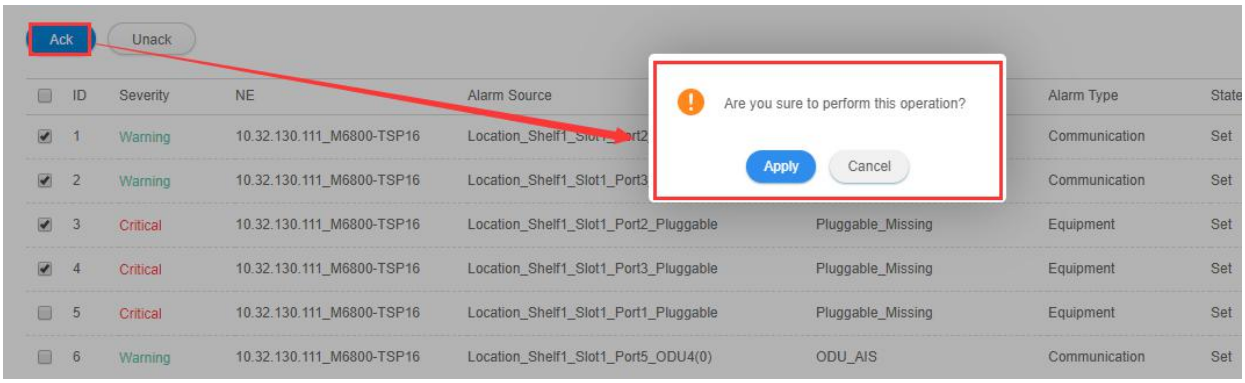


Figure 6-5 Confirm Current Alarm

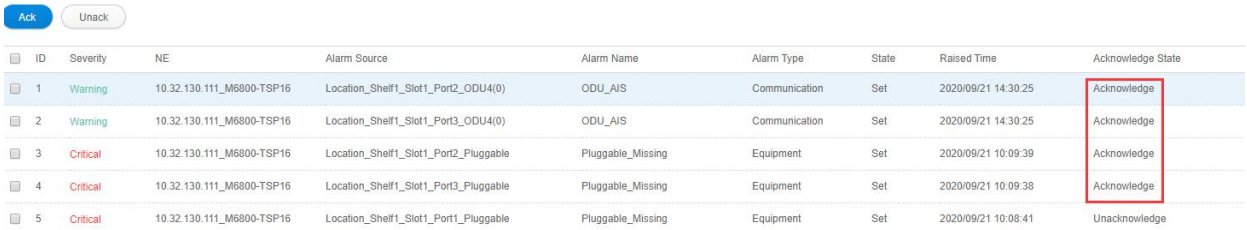


Figure 6-6 Complete Confirmation of Current Alarm

- 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.

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

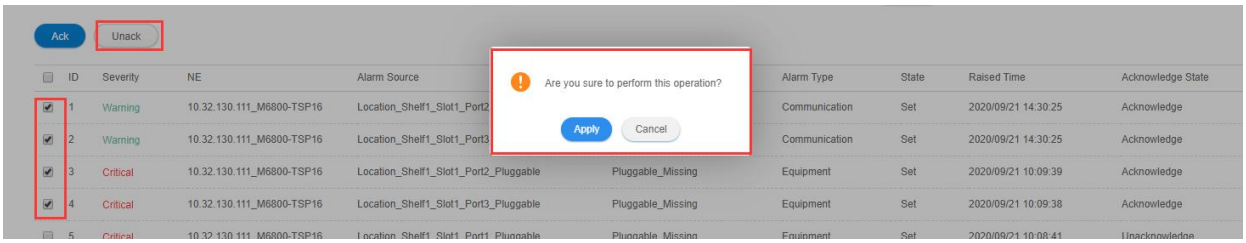


Figure 6-7 Cancel Confirmation of Current Alarm

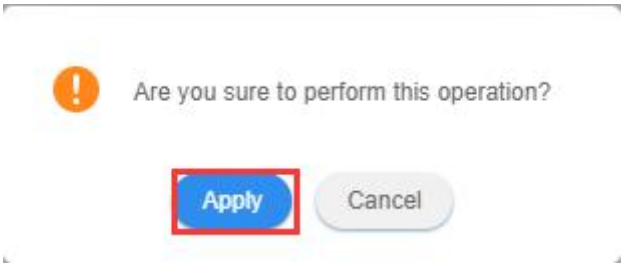


Figure 6-8 Cancel Confirmation

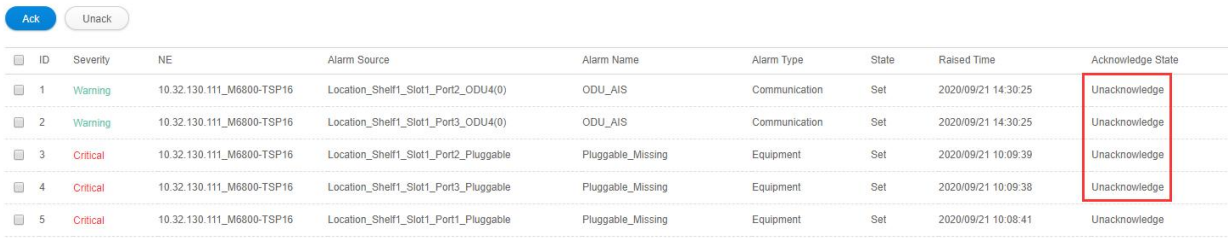


Figure 6-9 Complete Cancellation Confirmation of Current Alarm

- 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.

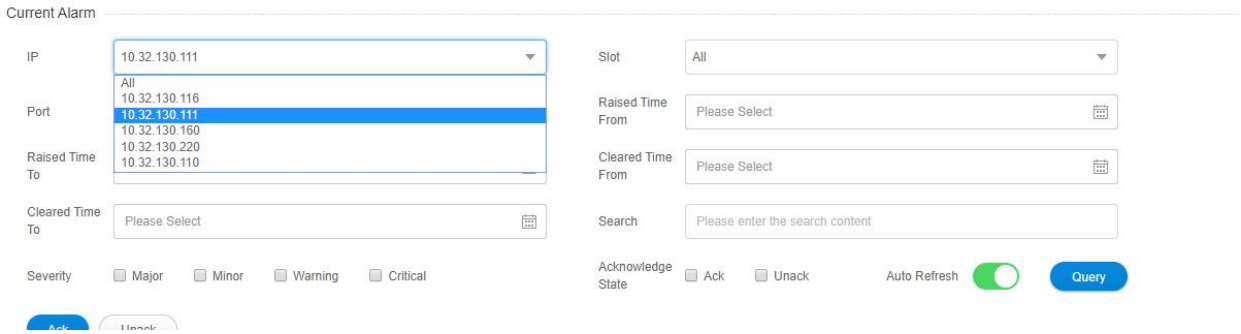


Figure 6-10 IP Filter Current Alarm

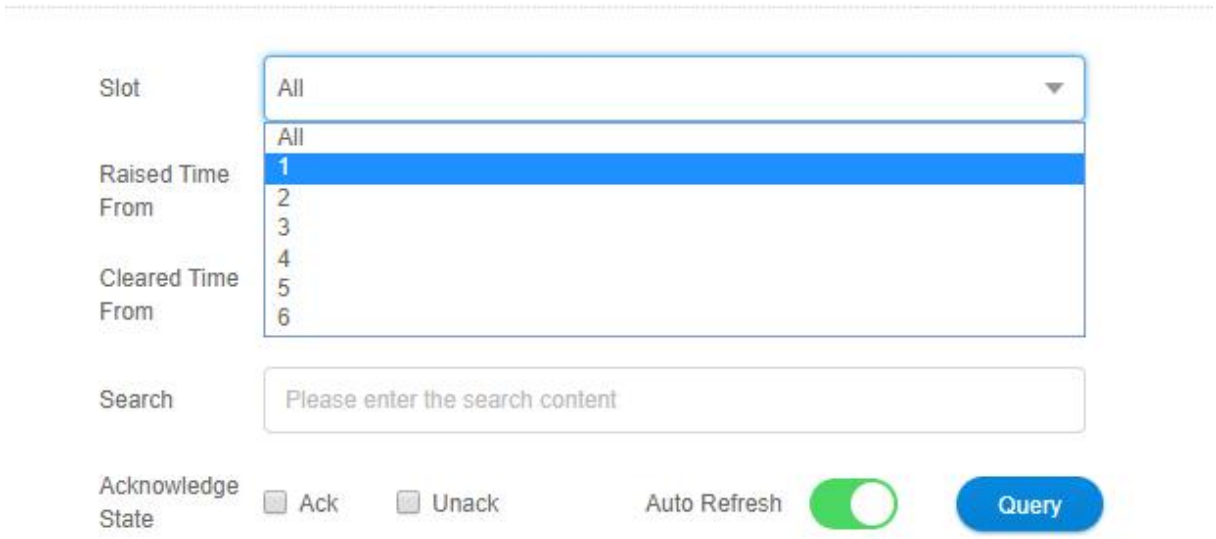


Figure 6-11 Fliter Current Alarm for Slots & Ports

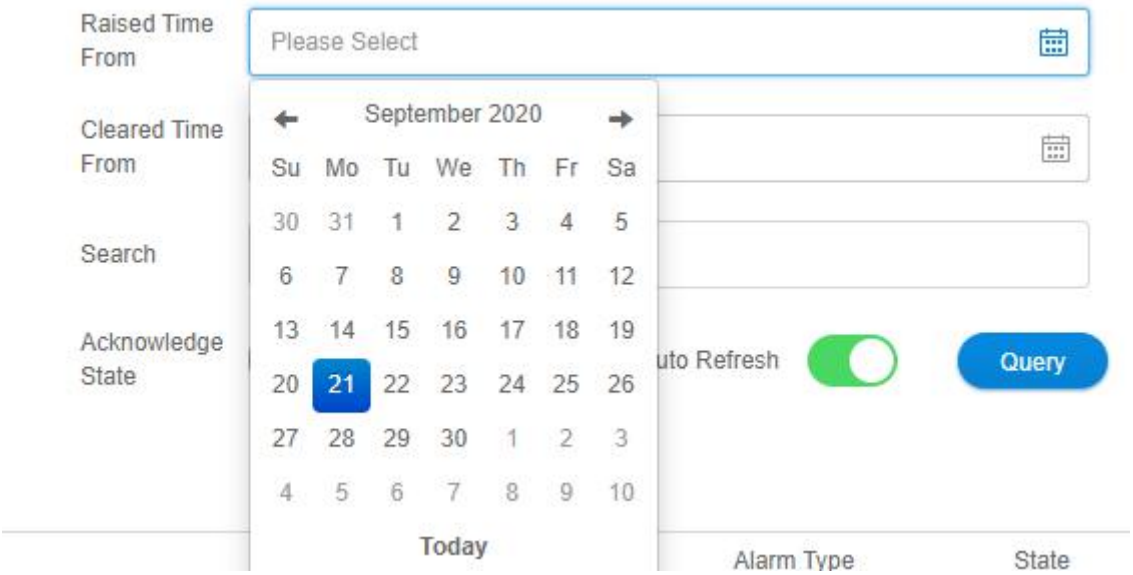


Figure 6-12 Create Time to Filter Current Alarm

Figure 6-13 Filter Current Alarm According to Alarm Level & Confirmation Status

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.

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.

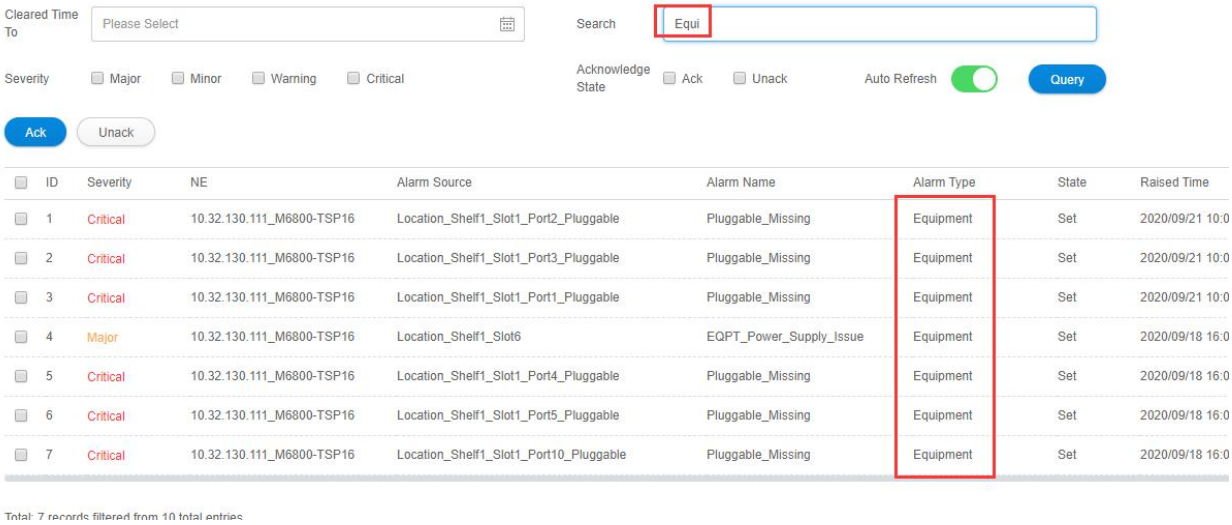


Figure 6-14 Search Current Alarm

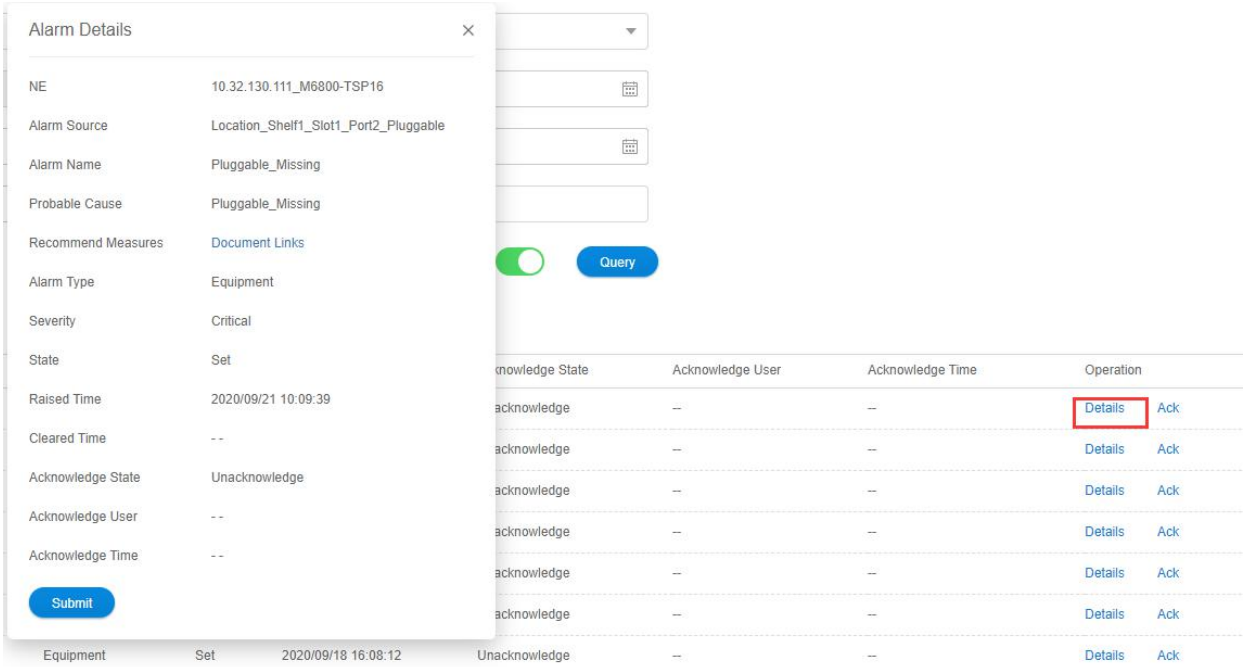
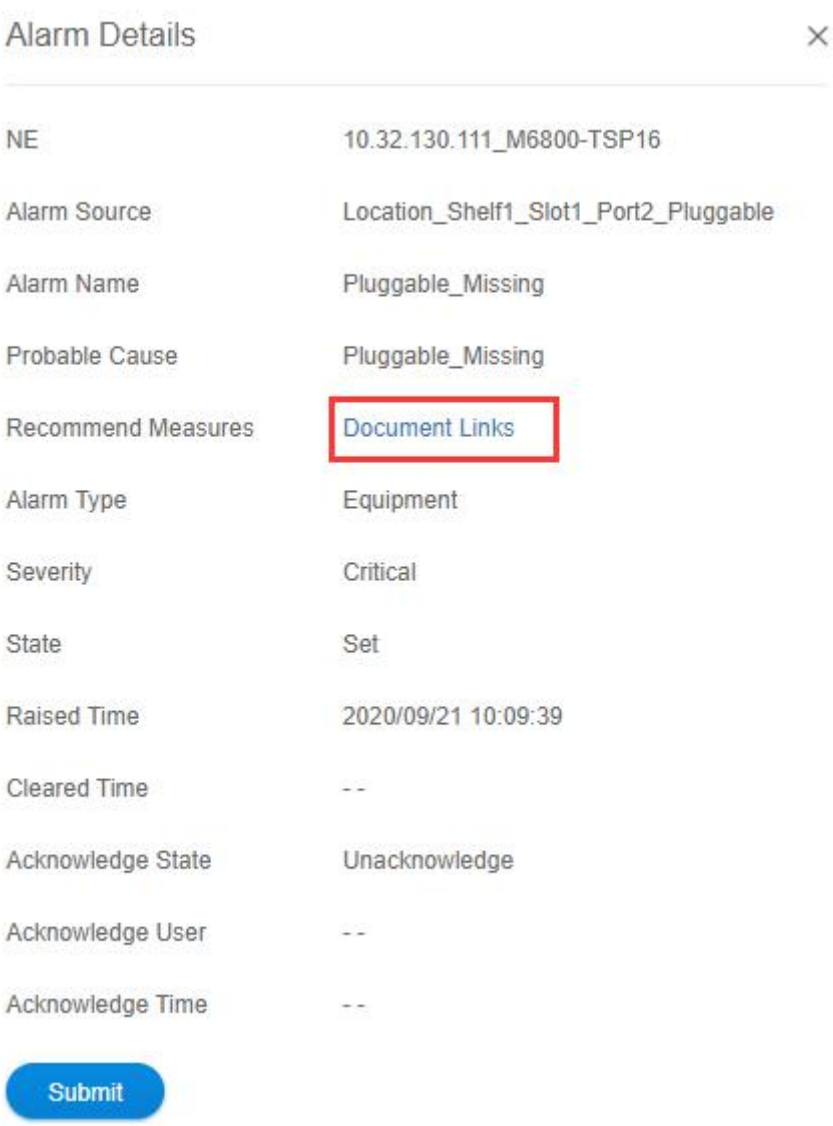


Figure 6-15 Alarm Details



http://localhost:9090/alarm/alarmdetail.html

Figure 6-16 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, confirmation status, confirmer , confirmation time and 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, confirmation status, confirmer and confirmation time are relatively simple, we will not go into much detail here.

6.2.2. History Alarm

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

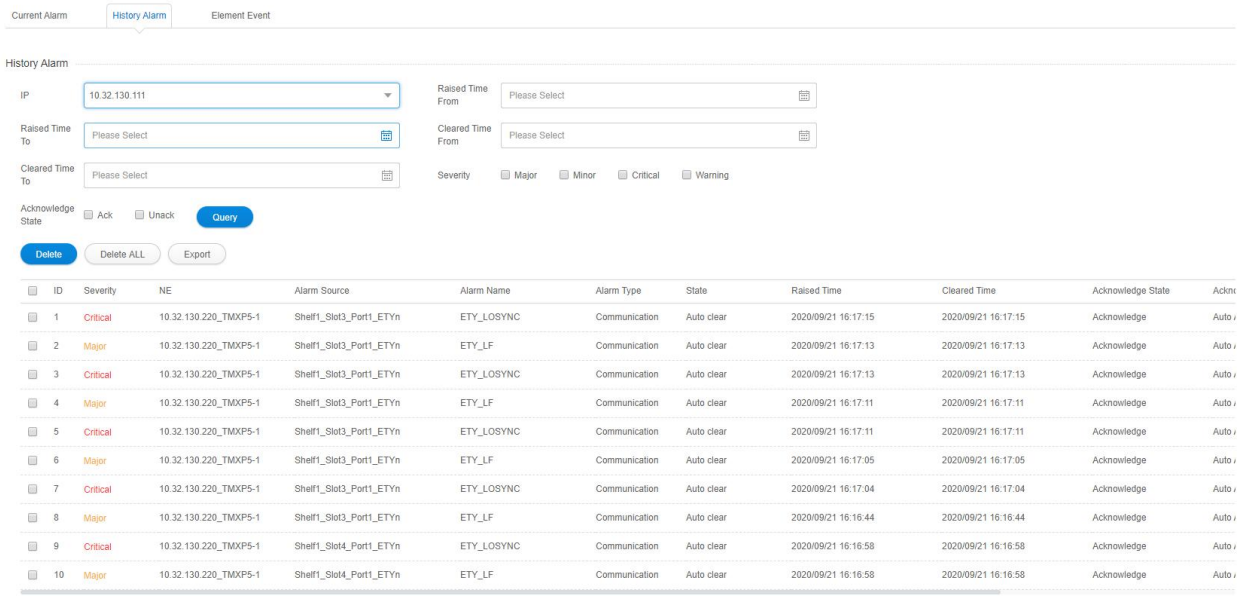


Figure 6-17 History Alarm

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.

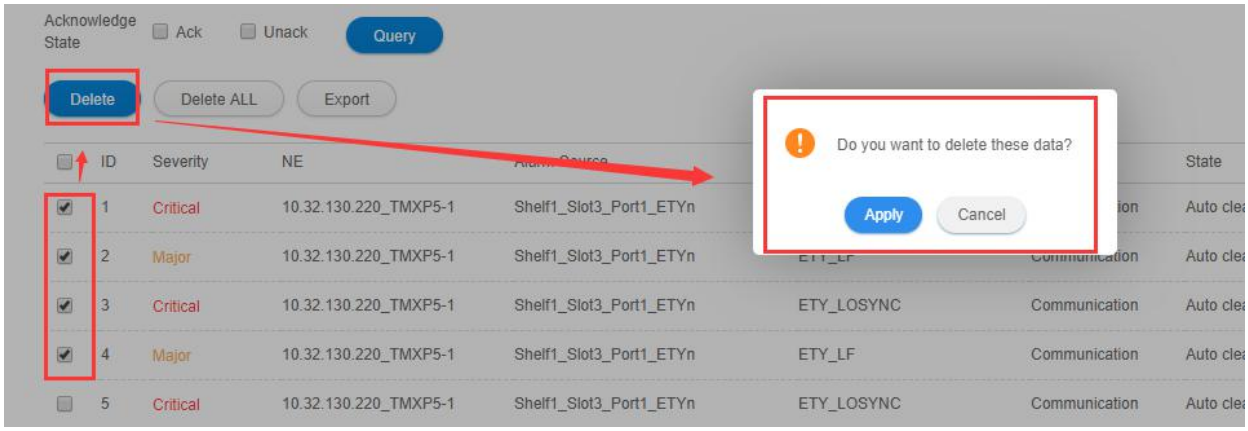


Figure 6-18 Delete History Alarm

- 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 the file, it will prompt to save the path. The exported data is saved in Excel format.

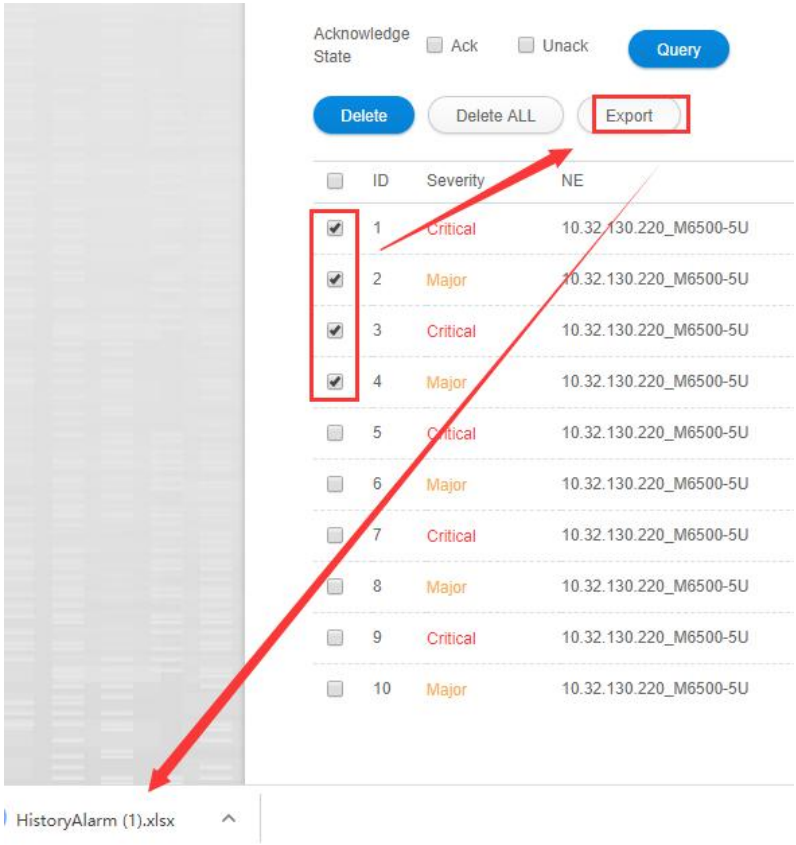


Figure 6-19 Export History Alarm

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.)

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.

6.3. Alarm Configuration

6.3.1. Alarm Configuration

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

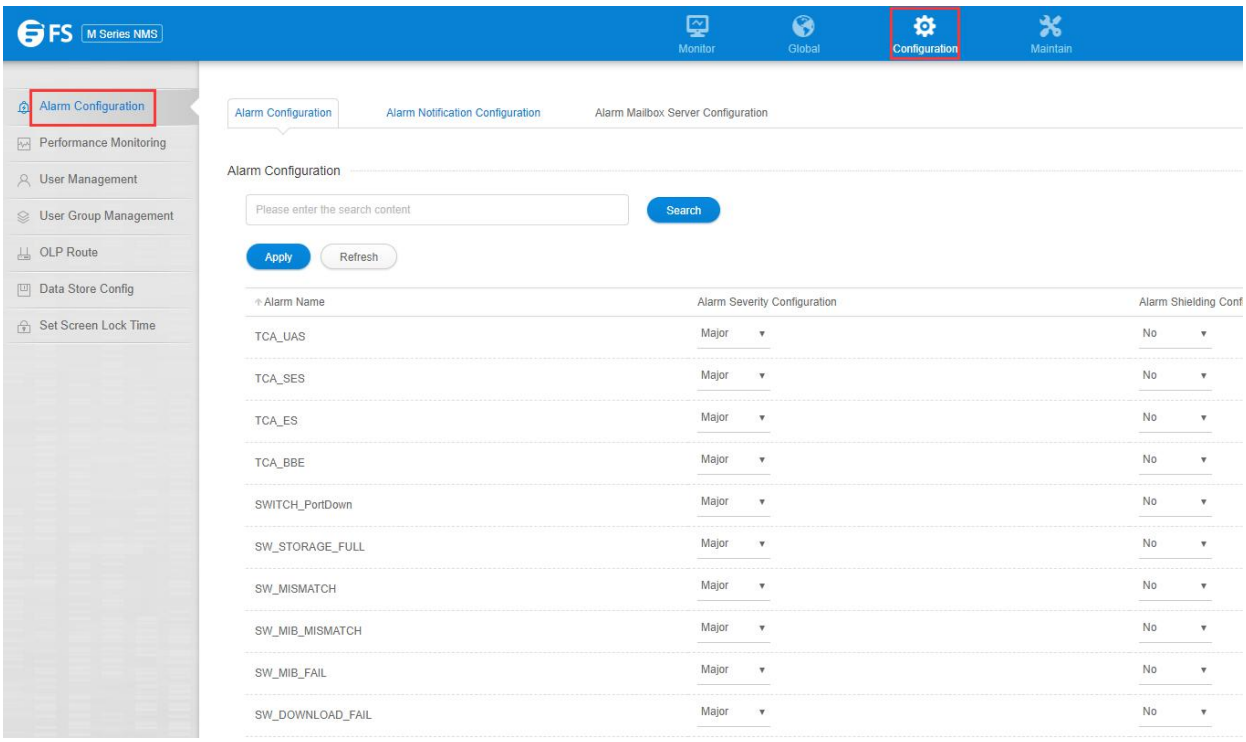


Figure 6-20 Alarm Configuration

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.

Figure 6-21 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.

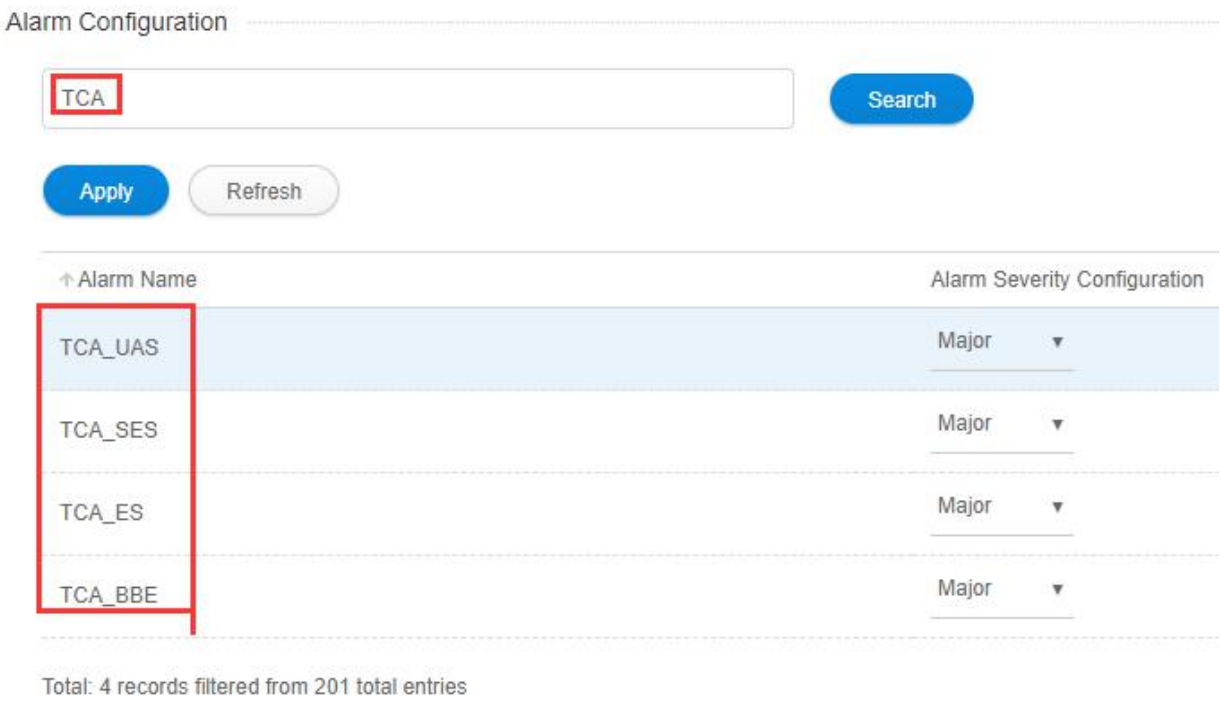


Figure 6-22 Searching Function in Alarm Configuration

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 and 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.)

6.3.2. Alarm Notification Configuration

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

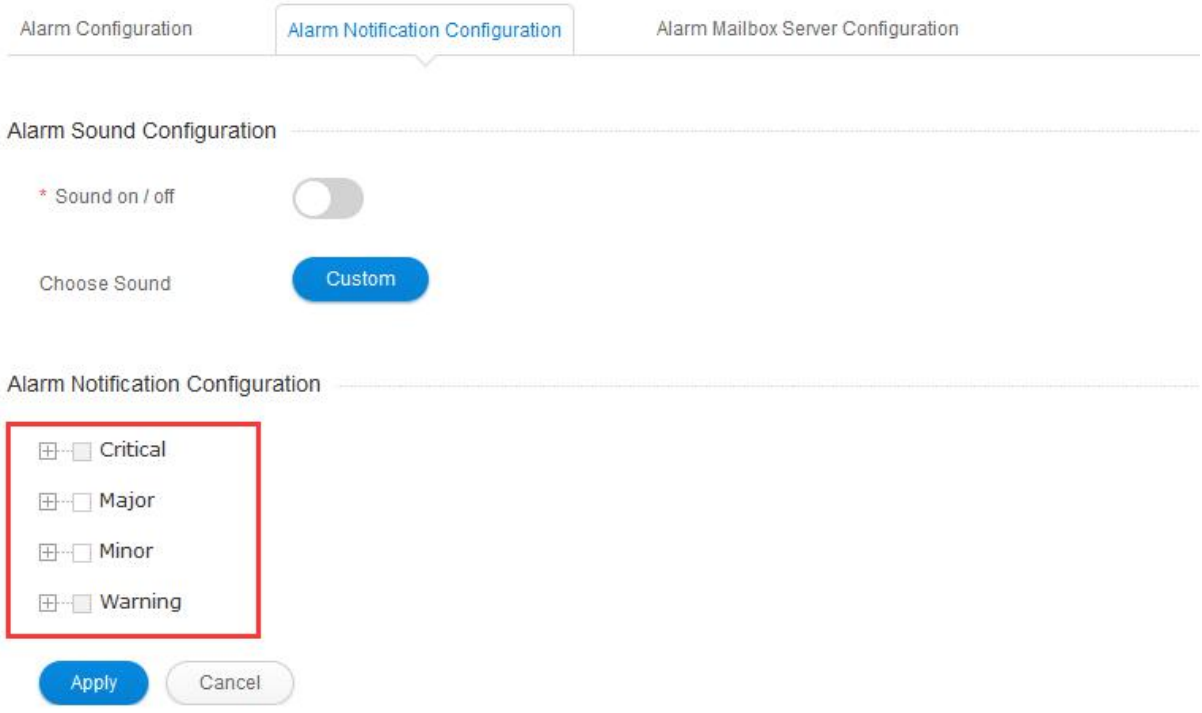


Figure 6-23 Alarm Notification Configuration

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 cancelled. In application, it will only receive the generation and elimination information of the selected alarm in the mail system.

6.3.3. 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:

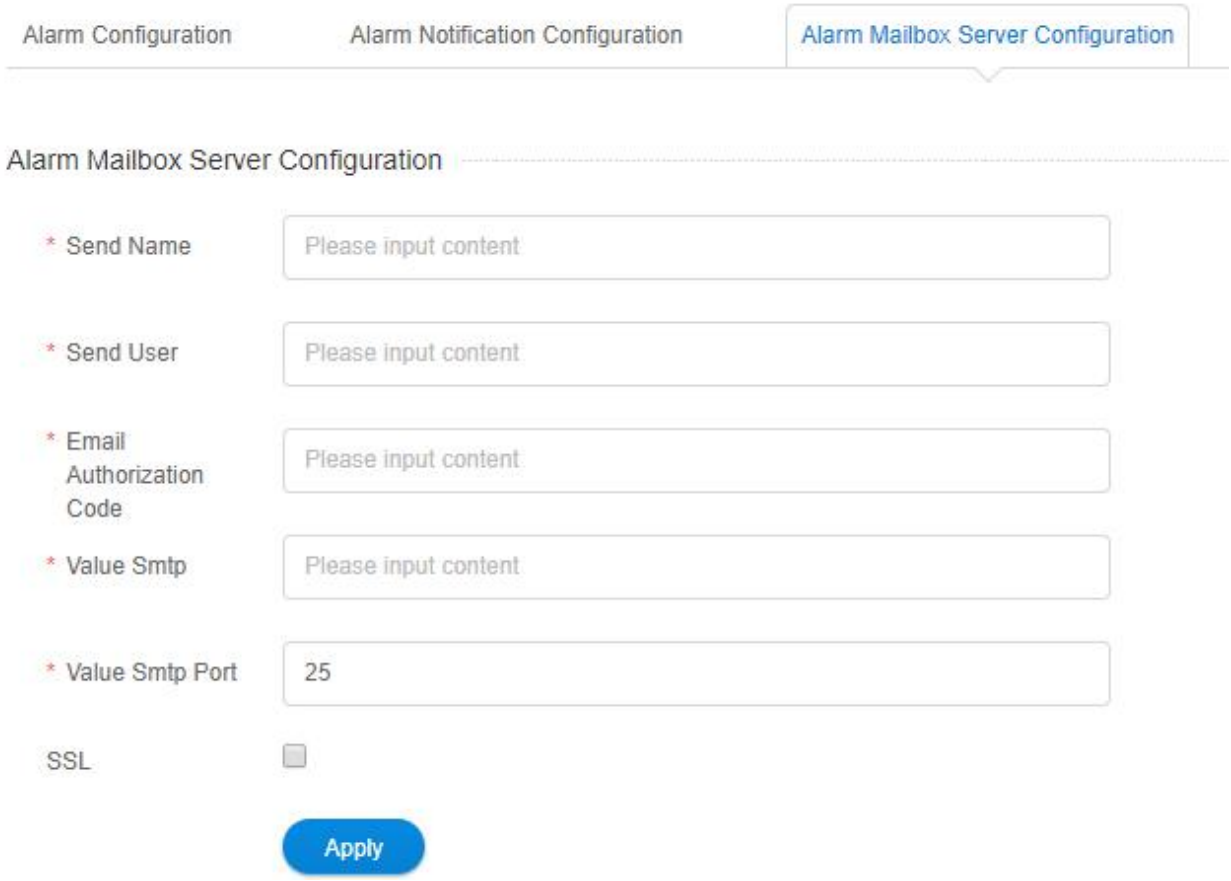


Figure 6-24 Alarm Mailbox Server Configuration

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

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.

6.3.4. 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.

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).

6.3.5. Custom Alarm Sound

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

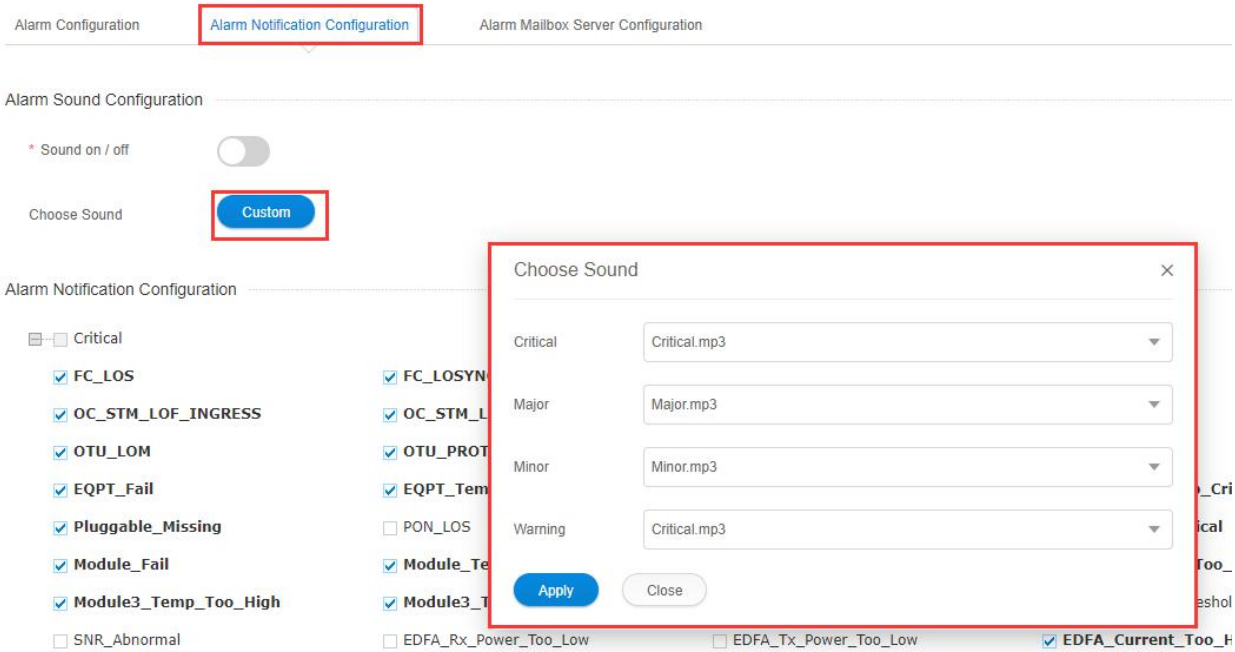


Figure 6-25 Custom Alarm Sound

7. 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.

7.1. Performance Management Introduction

7.1.1. Filter Box

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

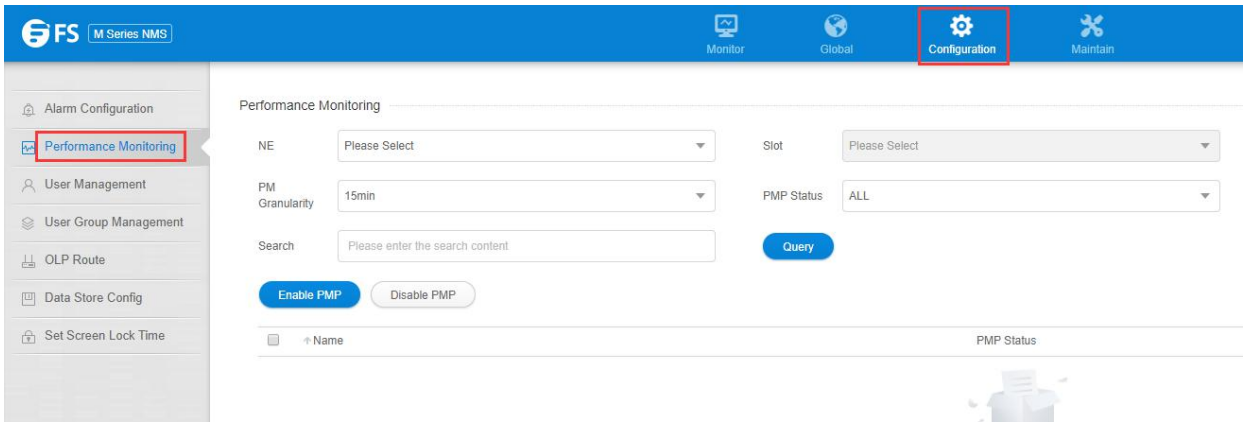


Figure 7-1 Performance Monitoring Point Management Interface

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.

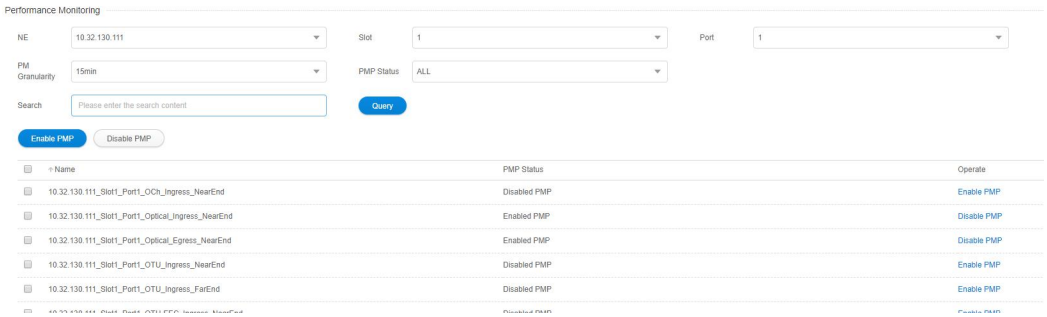


Figure 7-2 Show Monitoring Management Information

7.1.2. 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.

7.1.3. 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:

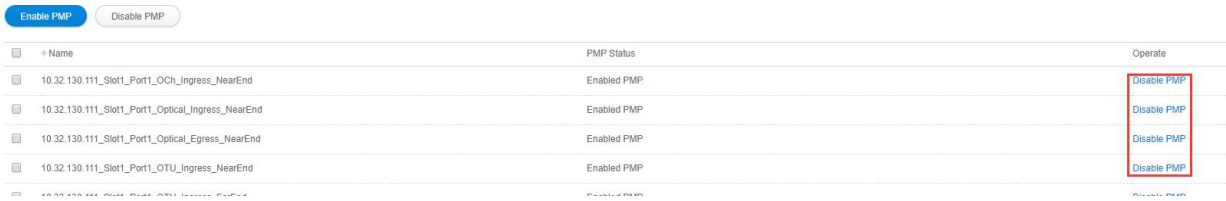


Figure 7-3 Enable Monitoring Points

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:

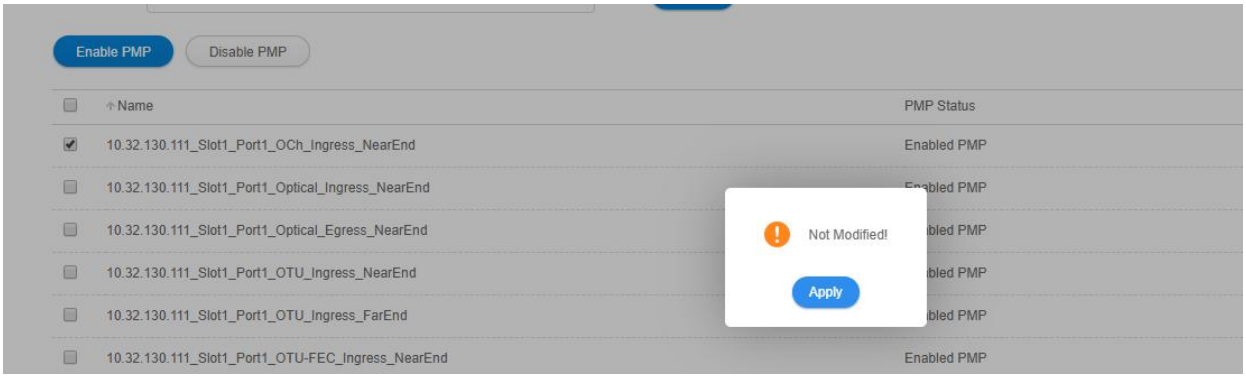


Figure 7-4 Operation Failure

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:

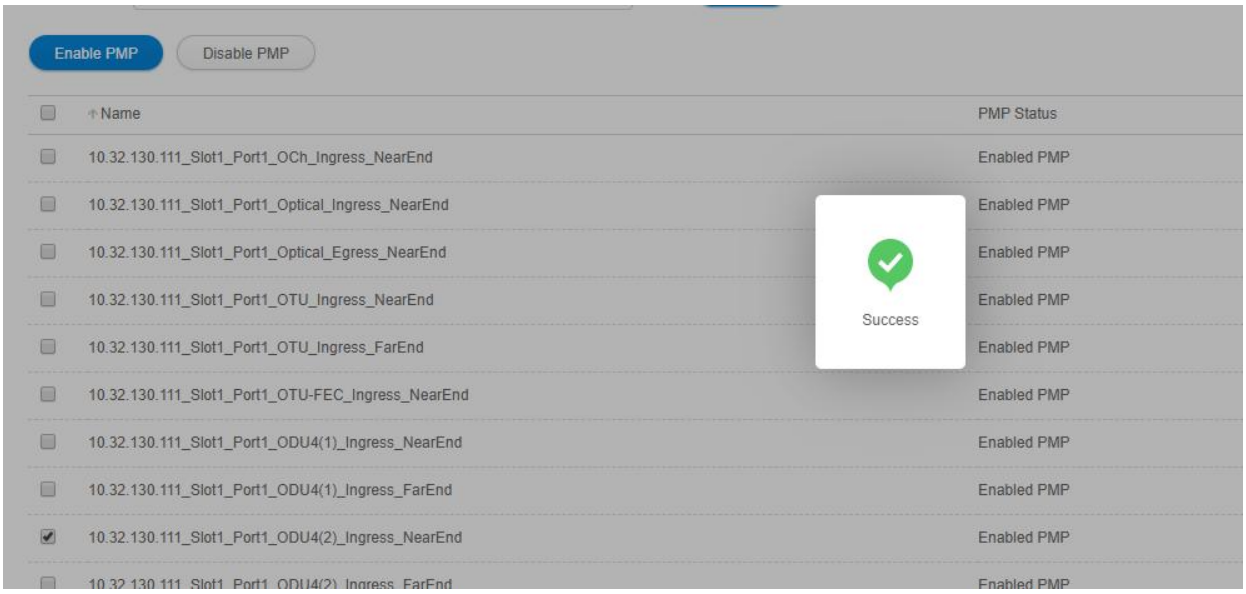


Figure 7-5 Enable A Single Monitoring Point

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:

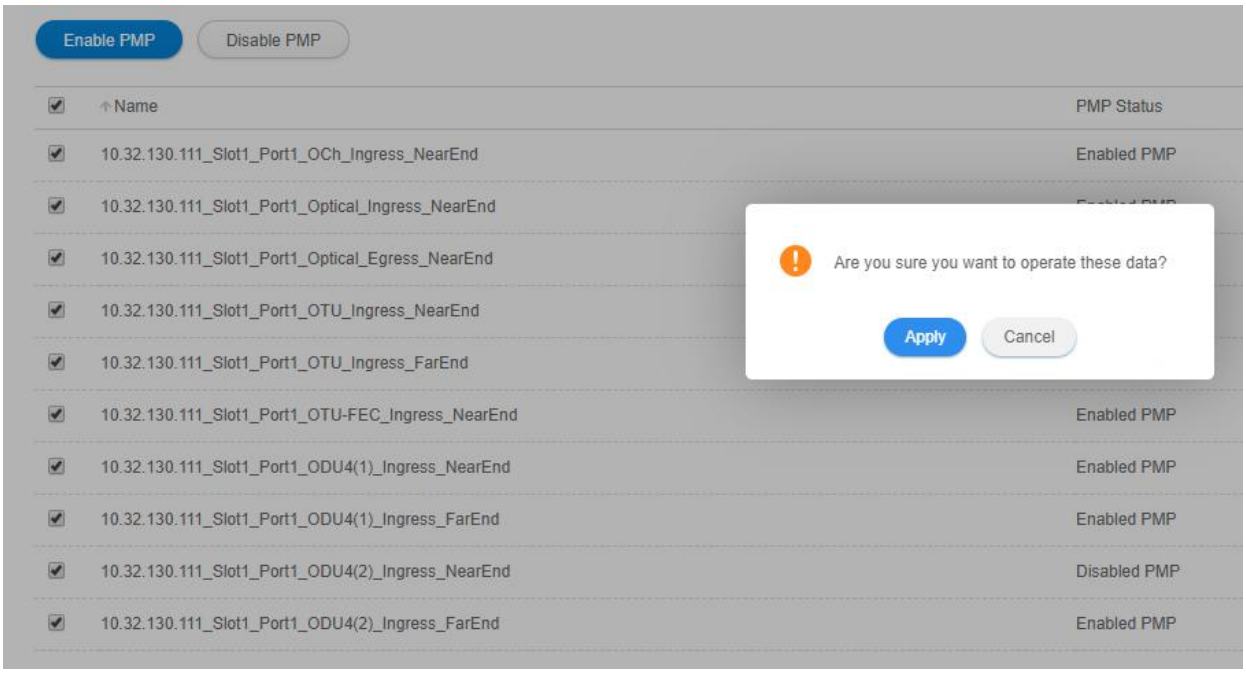


Figure 7-6 Batch Enabling Monitoring Points

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

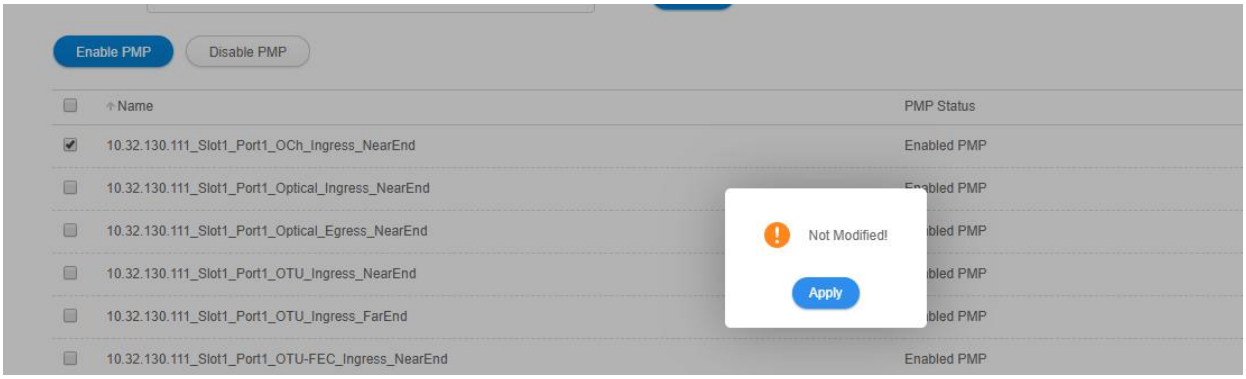


Figure 7-7 No Modification of Monitoring Point Status

7.1.4. 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 cannot be viewed, as shown in the figure below:

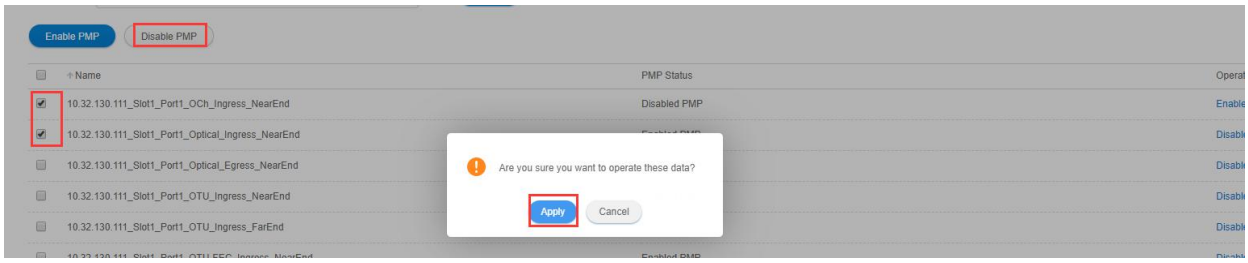


Figure 7-8 Disable Monitoring Point

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:

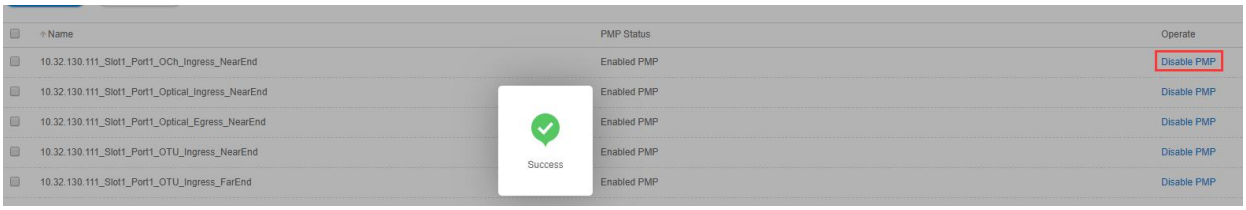


Figure 7-9 Disable A Single Monitoring Point

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:

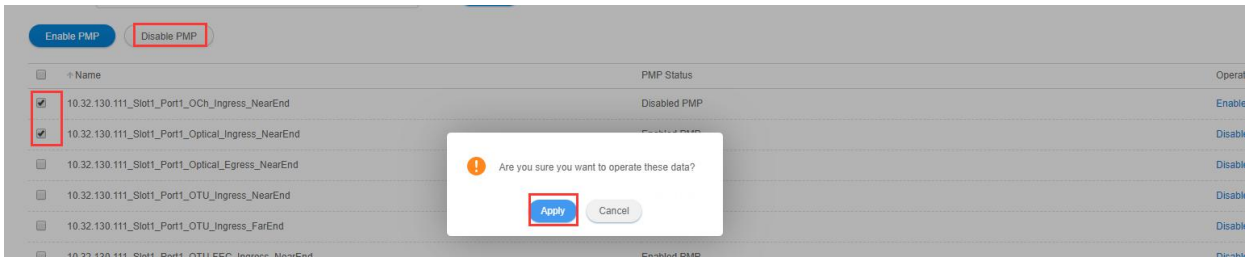


Figure 7-10 Disable Batch Monitoring Points

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

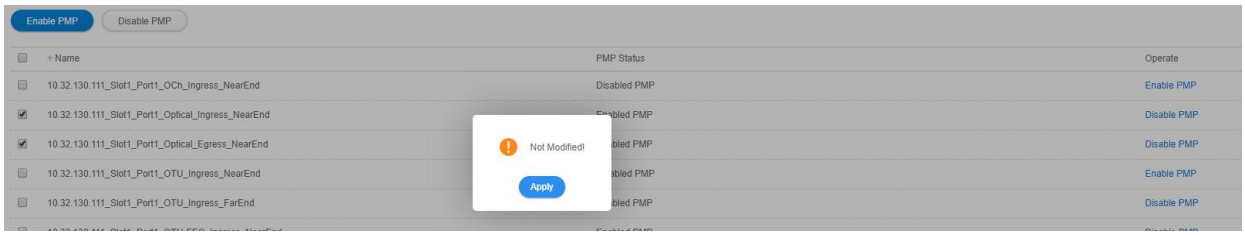


Figure 7-11 No Modification of Monitoring Point Status

7.1.5. 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, but 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 disables 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.)

7.2. Current Performance Info

Click "*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:

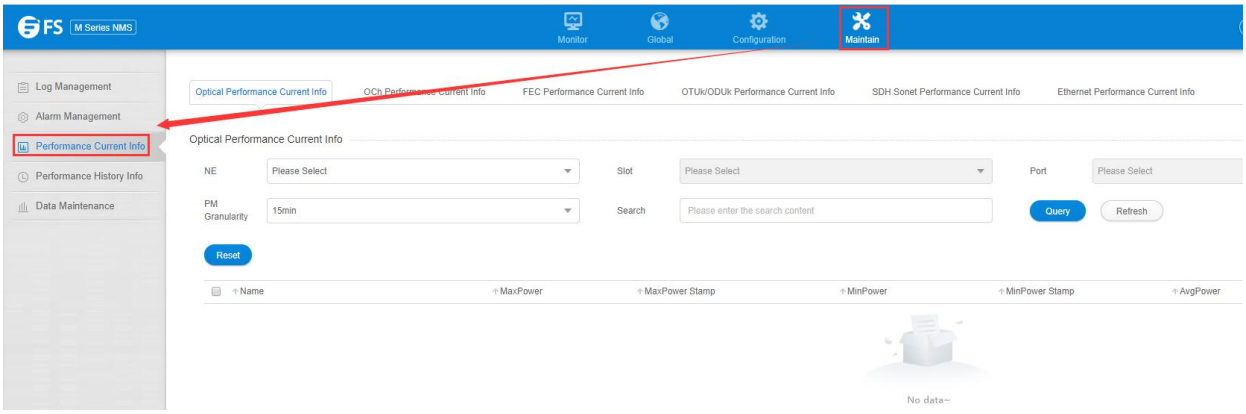


Figure 7-12 Current Performance Info Directory

7.2.1. Monitoring of Optical Power

7.2.1.1. Introduction of Optical Power Monitoring Parameters

The monitoring parameters of optical power monitoring point include maximum optical power, maximum optical power timestamp, minimum optical power, minimum optical power timestamp, 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.

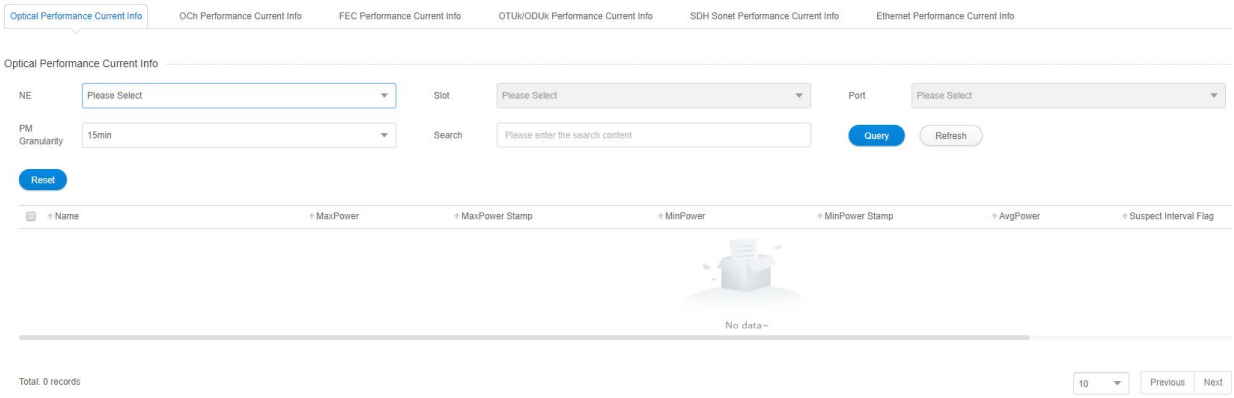


Figure 7-13 Display Monitoring Parameters

7.2.1.2. 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 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.

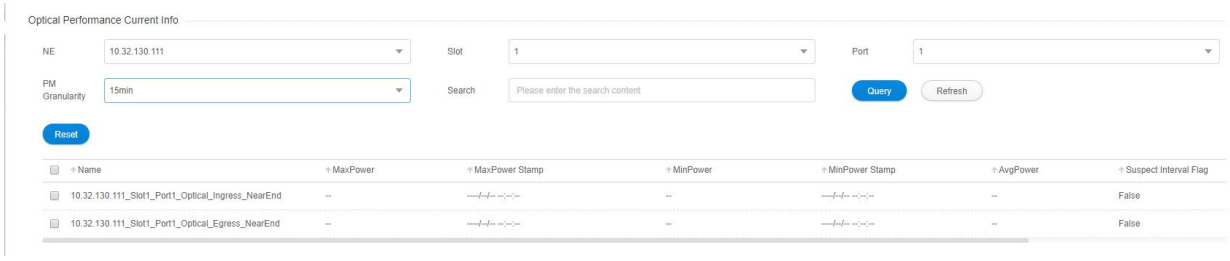


Figure 7-14 15-Minute Monitoring Point Data of Optical Power

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.

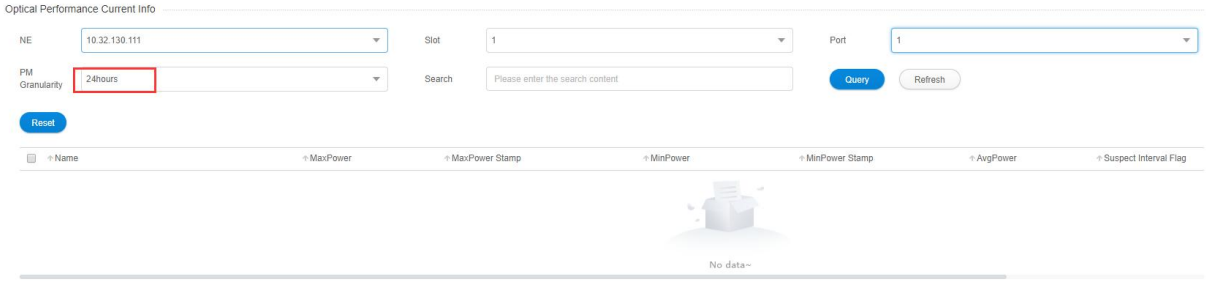


Figure 7-15 24-Hour Monitoring Point Data of Optical Power

7.2.1.3. 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.

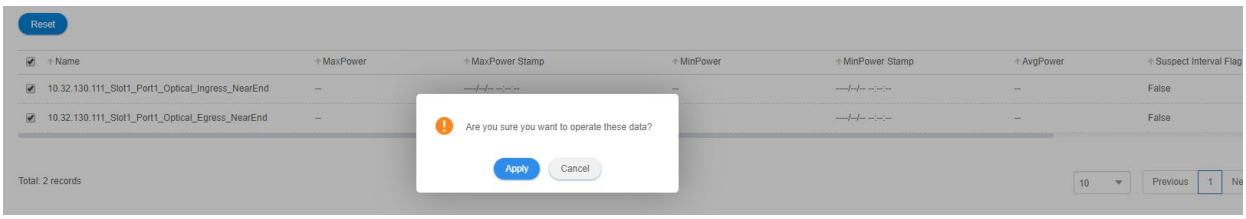


Figure 7-16 Batch Resetting of Optical Power

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.

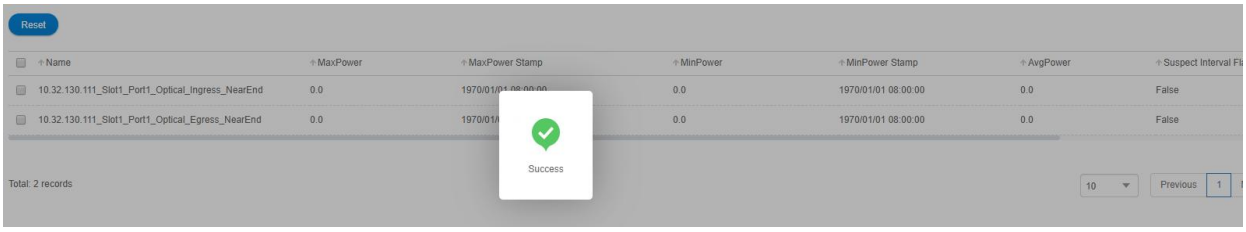


Figure 7-17 Successful Reset Operation

7.2.1.4. Optical Power Monitoring Data Show

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, that is to say, 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:

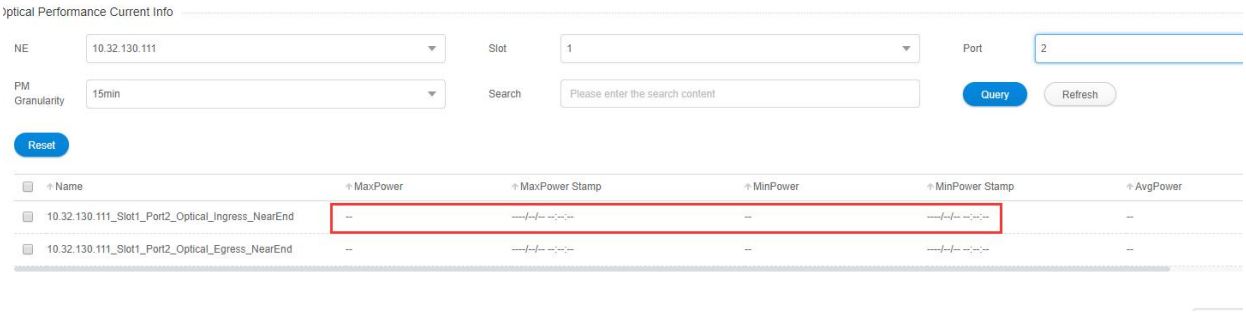


Figure 7-18 Optical Module of Optical Power Not in Position

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

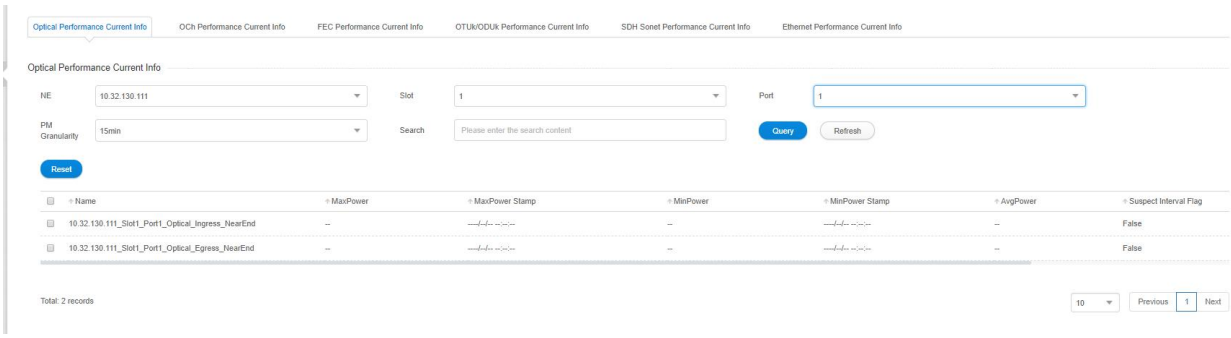


Figure 7-19 Optical Power Monitoring Data

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:

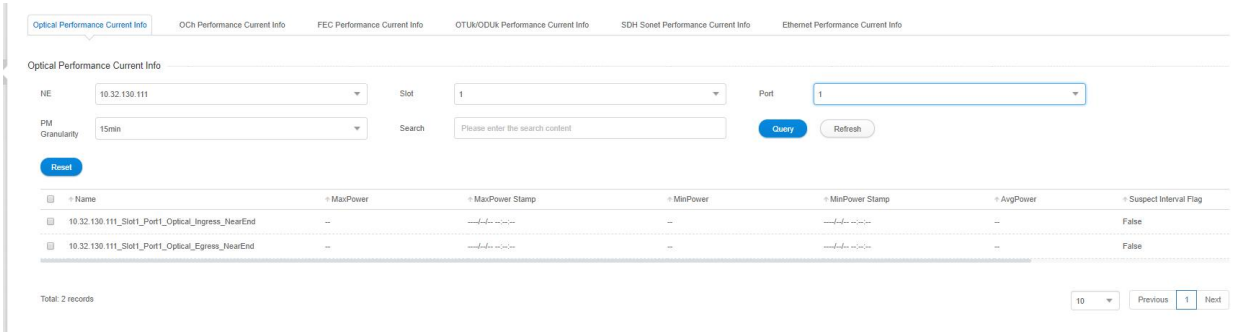


Figure 7-20 Optical Power Monitoring Data When Mismatched

7.2.2. OCh Current Performance Statistics

7.2.2.1. 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) time stamp, 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.

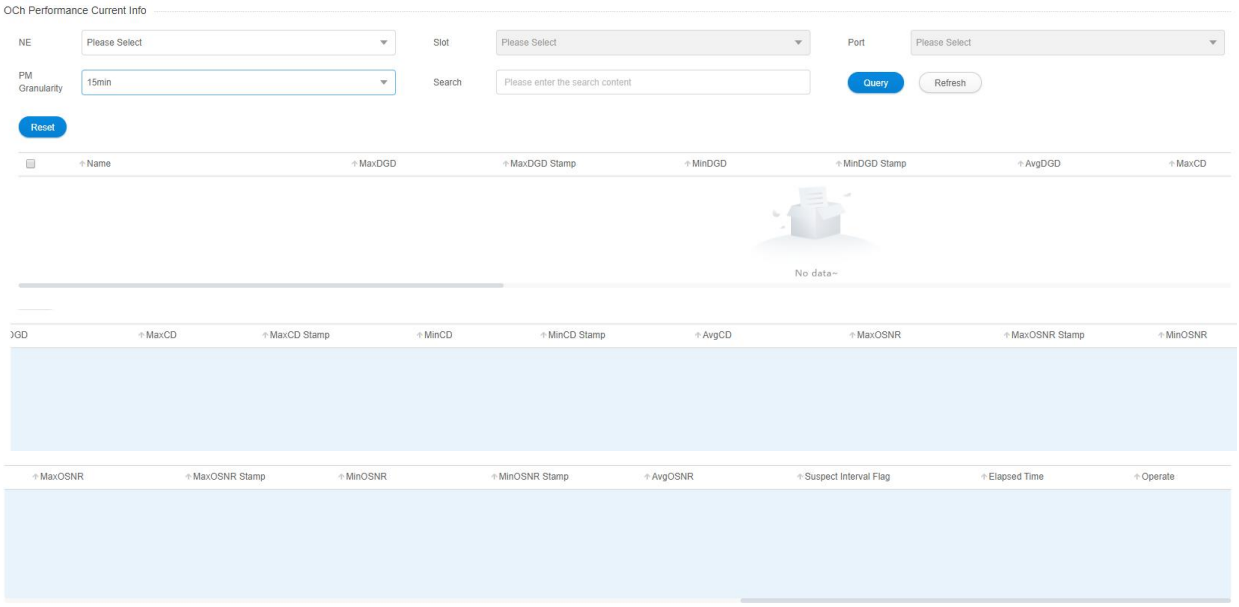


Figure 7-21 OCh Monitoring Parameters

7.2.2.2. 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.

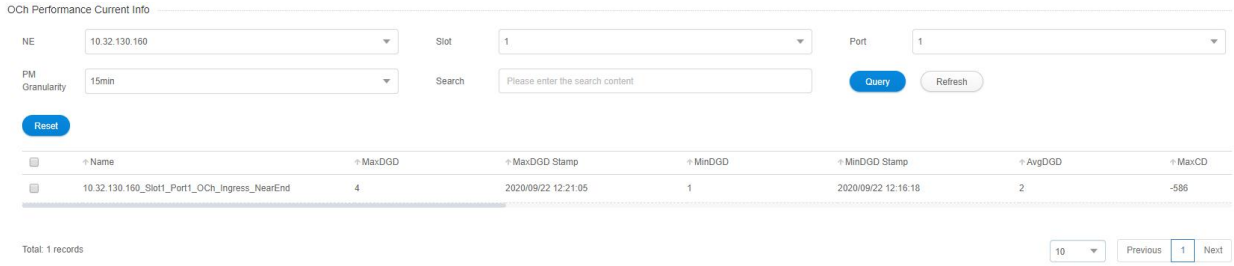


Figure 7-22 15-Minute OCh Monitoring Data

WDM module is inserted into the monitoring port. OCh data and corresponding generation timestamp 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:

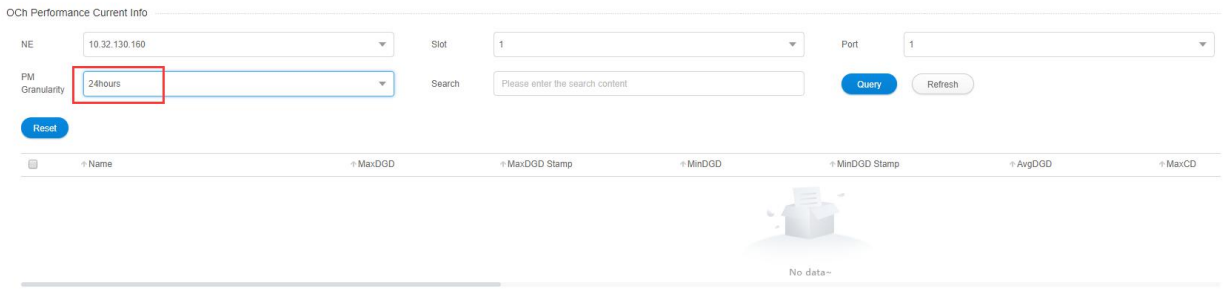


Figure 7-23 24-Hour OCh Monitoring Data

7.2.2.3. 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.

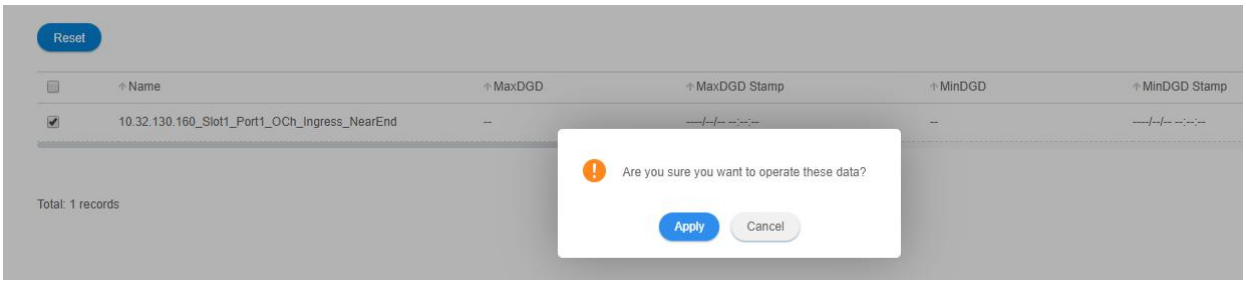


Figure 7-24 Reset OCh Data

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.

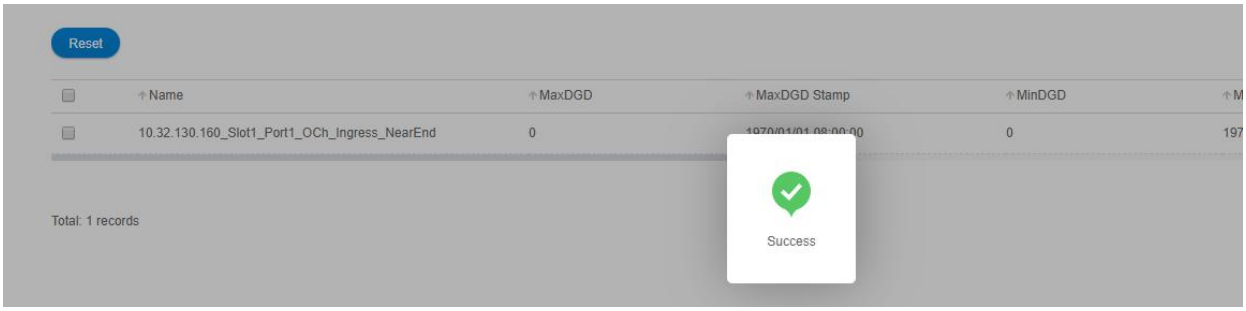


Figure 7-25 Successful Resetting of OCh

7.2.2.4. OCh Monitoring Data Show

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 time stamp 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:

Figure 7-26 Optical Module of OCh 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, 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 is always 0 without any change, as shown in the figure below.

Figure 7-27 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:

Figure 7-28 OCh Monitoring Data When Mismatched

7.2.3. FEC Current Performance Statistics

7.2.3.1. 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.

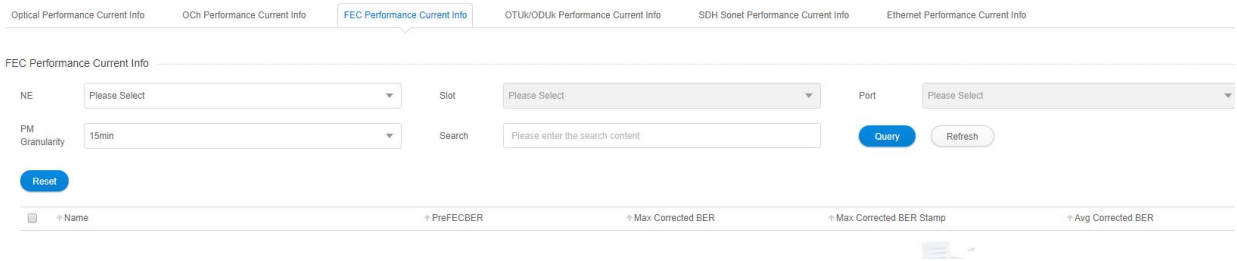


Figure 7-29 FEC Monitoring Parameters

7.2.3.2. 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.

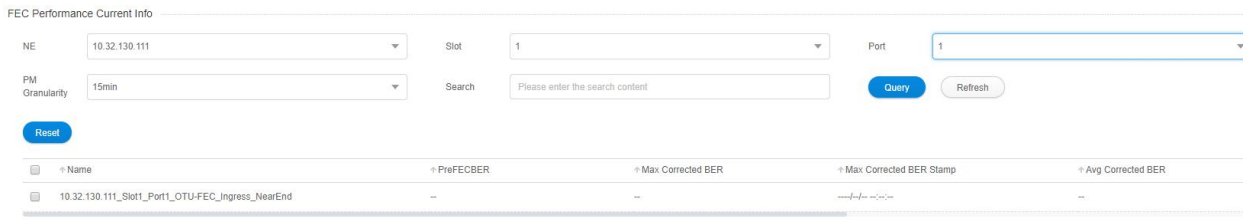


Figure 7-30 15-Minute Monitoring Data of FEC

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:

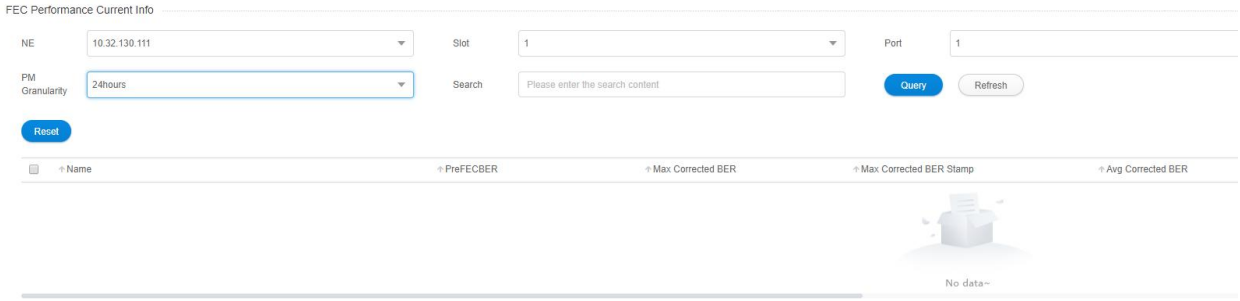


Figure 7-31 24-Hour Monitoring Data of FEC

7.2.3.3. 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.

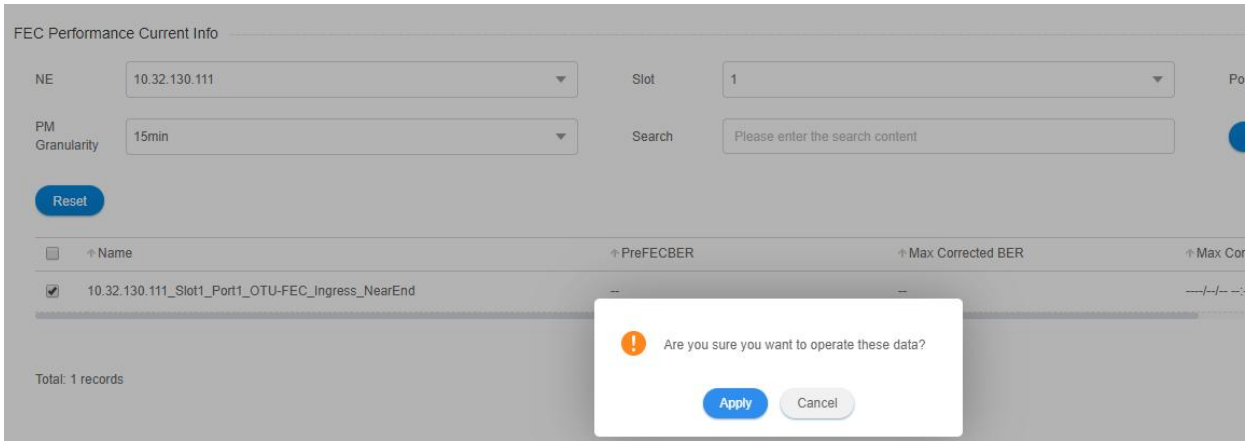


Figure 7-32 FEC Reset

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 trustworthy to untrustworthy 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.

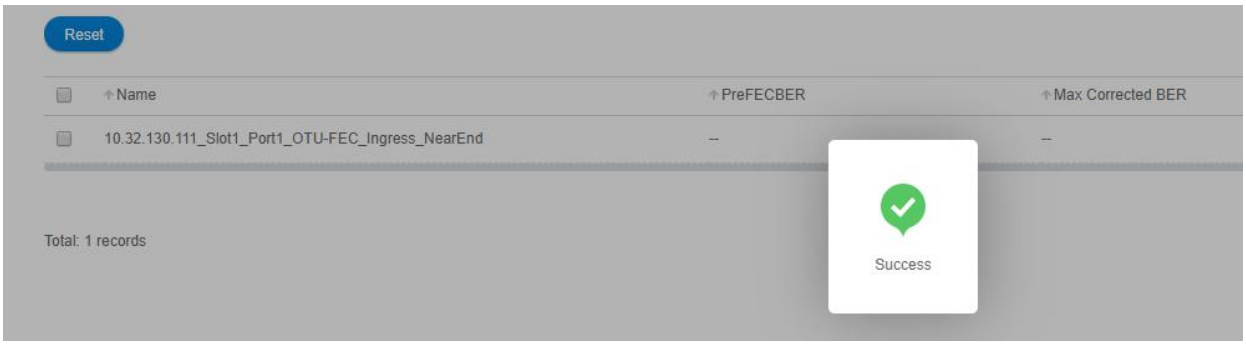


Figure 7-33 FEC Successfully Reset

7.2.3.4. FEC Monitoring Data Show

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:

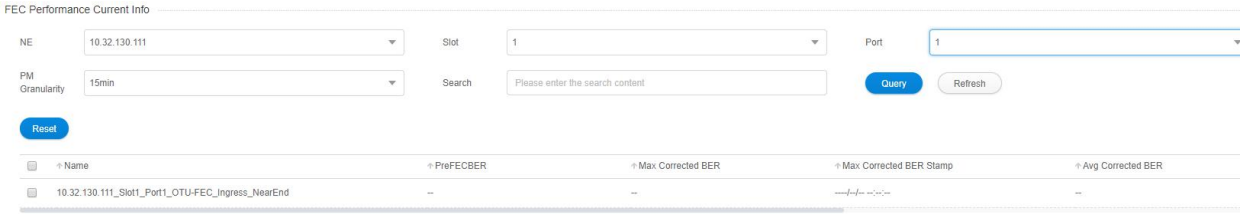


Figure 7-34 Optical Module of FEC Not In Position

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 times tamps 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.

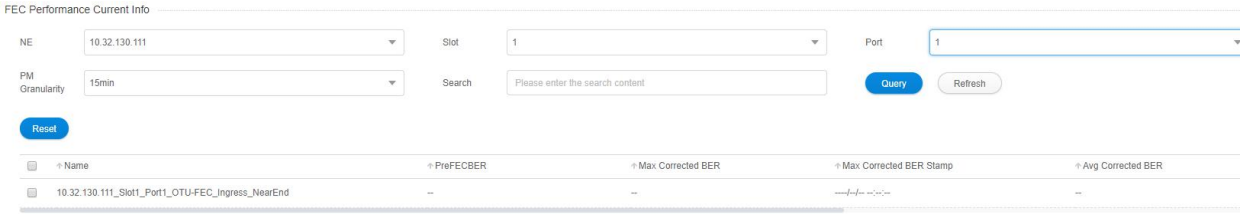


Figure 7-35 FEC Monitoring Data

(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:

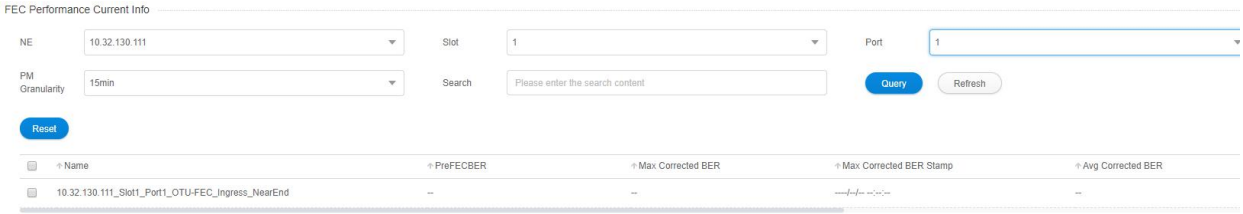


Figure 7-36 FEC Monitoring Data When Mismatched

7.2.4. OTUk/ODUk Current Performance Statistics

7.2.4.1. 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.

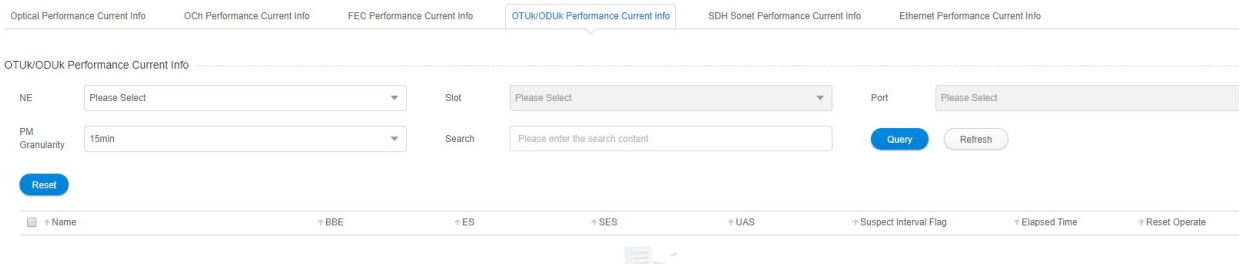


Figure 7-37 OTUk/ODUk Monitoring Parameters

7.2.4.2. 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.

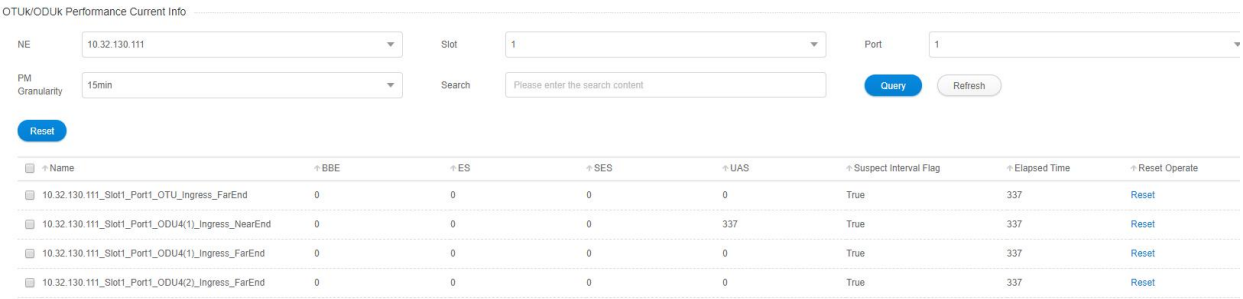


Figure 7-38 15-Minute OTUk/ODUk Monitoring Data

Optical module is inserted 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 below:

Optical module is inserted 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 below:

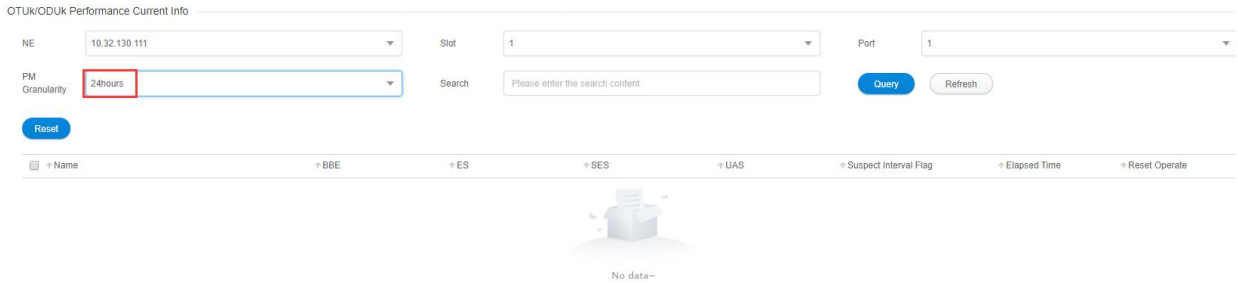


Figure 7-39 24-Hour OTUk/ODUk Monitoring Data

7.2.4.3. 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, 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.

Figure 7-40 UAS Always Counts

7.2.4.4. 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.

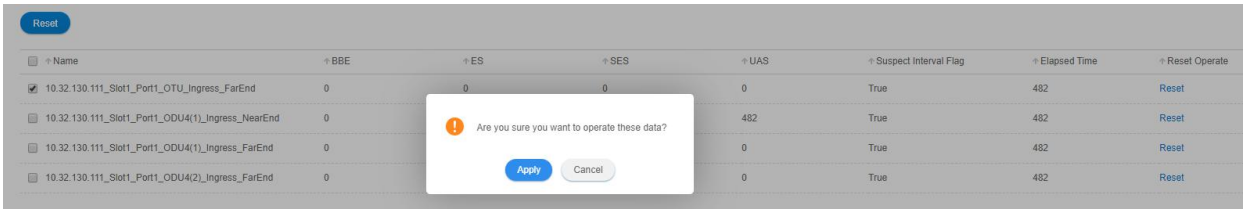


Figure 7-41 OTUk/ODUk Reset

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

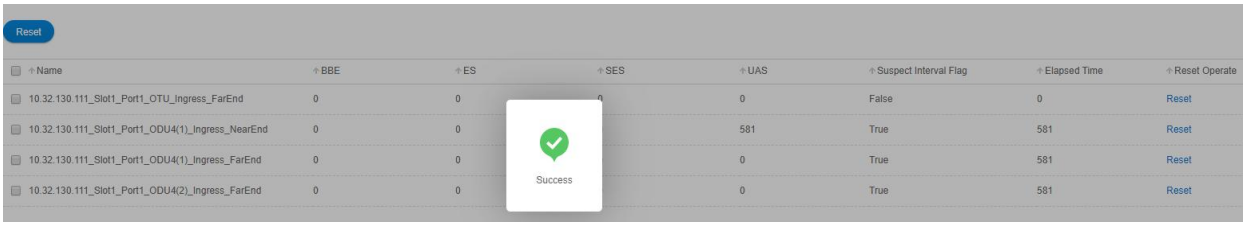


Figure 7-42 OTUk/ODUk Successfully Reset

7.2.4.5. OTUk/ODUk Monitoring Data Show

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 (after 900/86400 seconds) or untrustworthy. The running time is normal and counts from 0, as shown in the figure below:

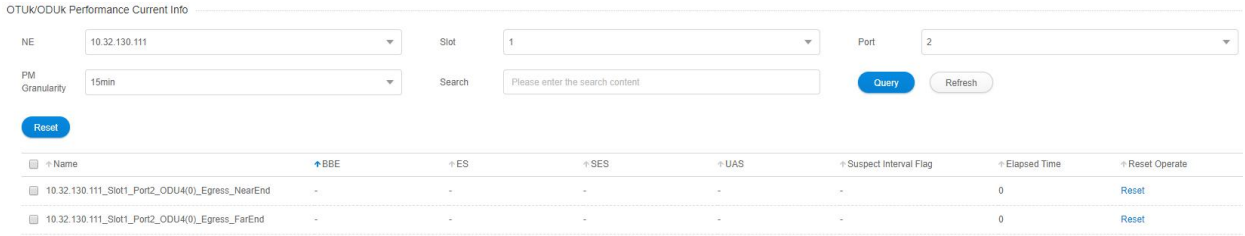


Figure 7-43 Optical Module of OTUk/ODUk Not In Position

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.

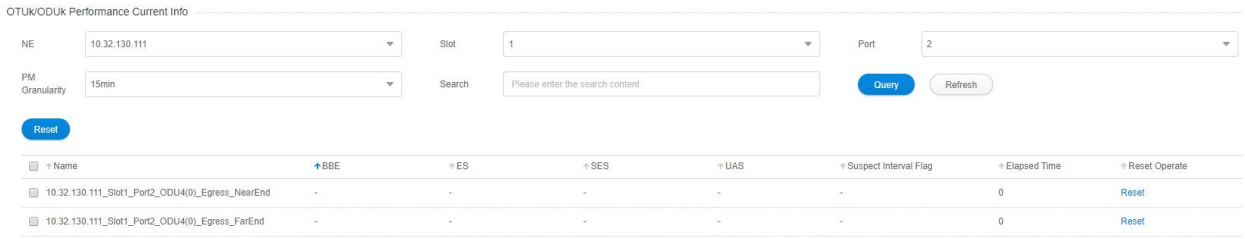


Figure 7-44 OTUk/ODUk Monitoring Data

(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:

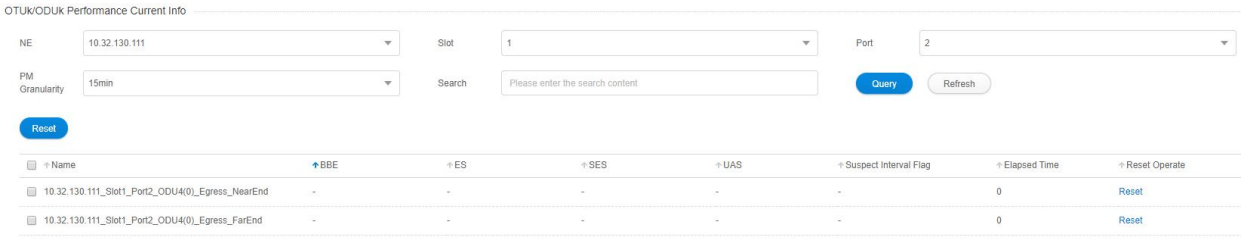


Figure 7-45 OTUk/ODUk Monitoring Data When Mismatched

7.2.5. Current Performance Statistics of Ethernet

7.2.5.1. 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.

Figure 7-46 Ethernet Monitoring Parameters

7.2.5.2. 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.

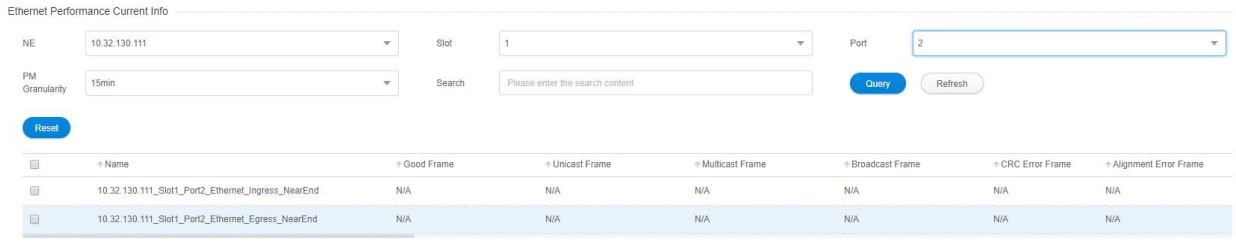


Figure 7-47 15-Minute Ethernet Monitoring Data

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:

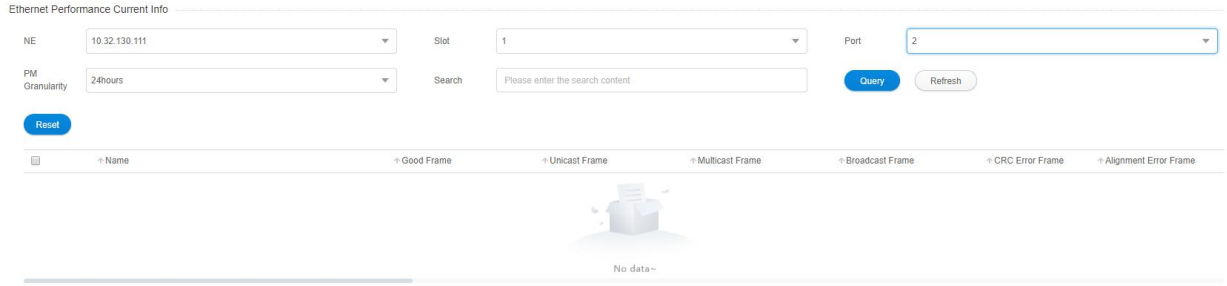


Figure 7-48 24-Hour Ethernet Monitoring Data

7.2.5.3. 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.

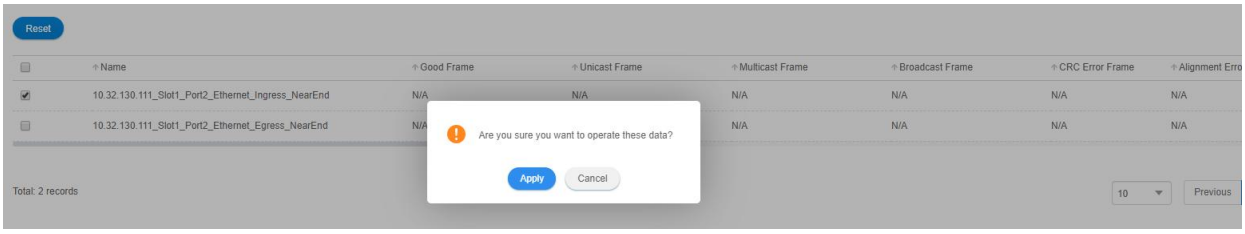


Figure 7-49 Ethernet Reset

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

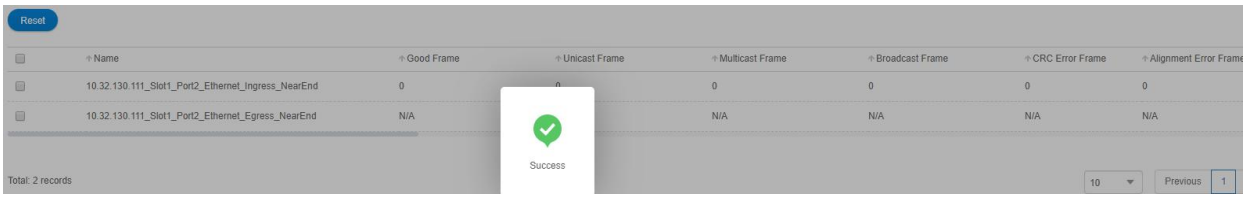


Figure 7-50 Ethernet Successfully Reset

7.2.5.4. Ethernet Monitoring Data Show

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:

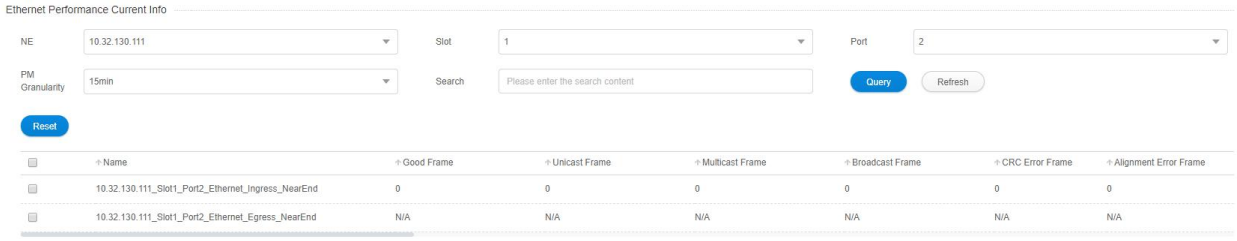


Figure 7-51 Optical Module of Ethernet Not In Position

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:

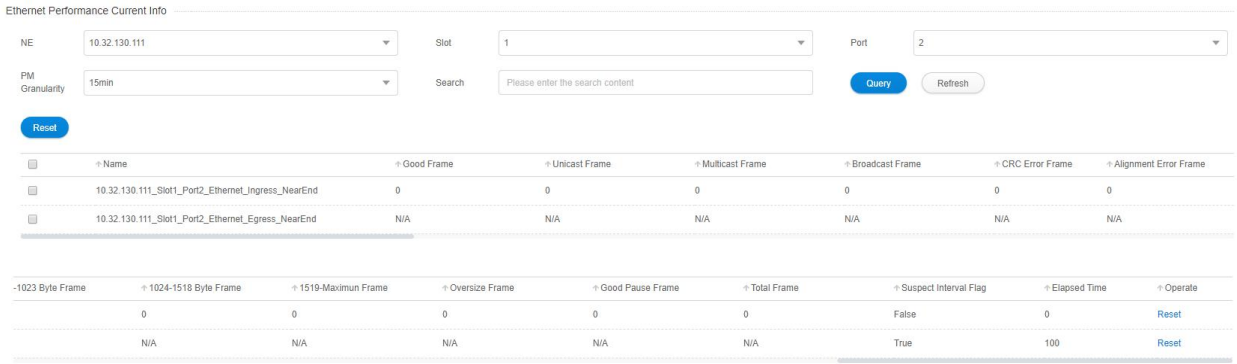


Figure 7-52 Ethernet Monitoring Data

(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:

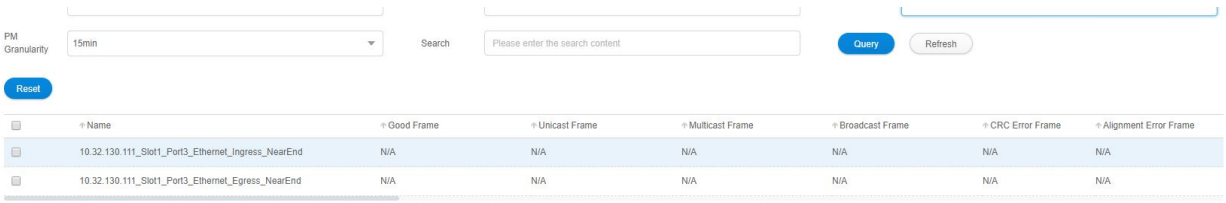


Figure 7-53 Ethernet Monitoring Data When Mismatched

7.3. History Performance Statistics

7.3.1. History Performance Statistics of Optical Power

7.3.1.1. 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.

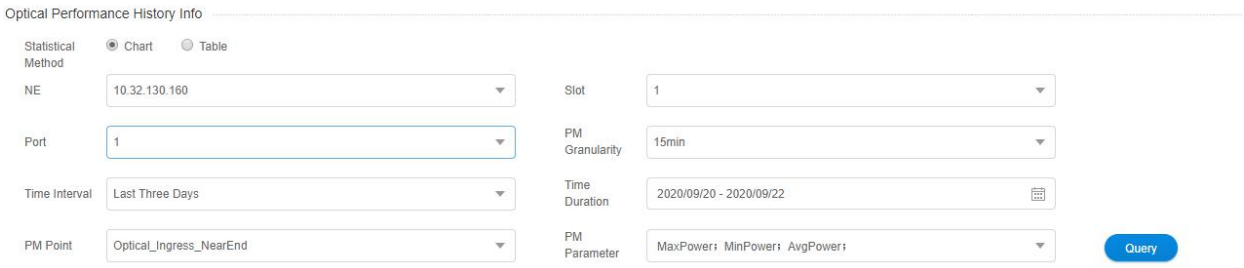


Figure 7-54 History Performance Parameters of Optical Power

7.3.1.2. View History Monitoring Information of Optical Power

15 minutes and 24 hours 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.

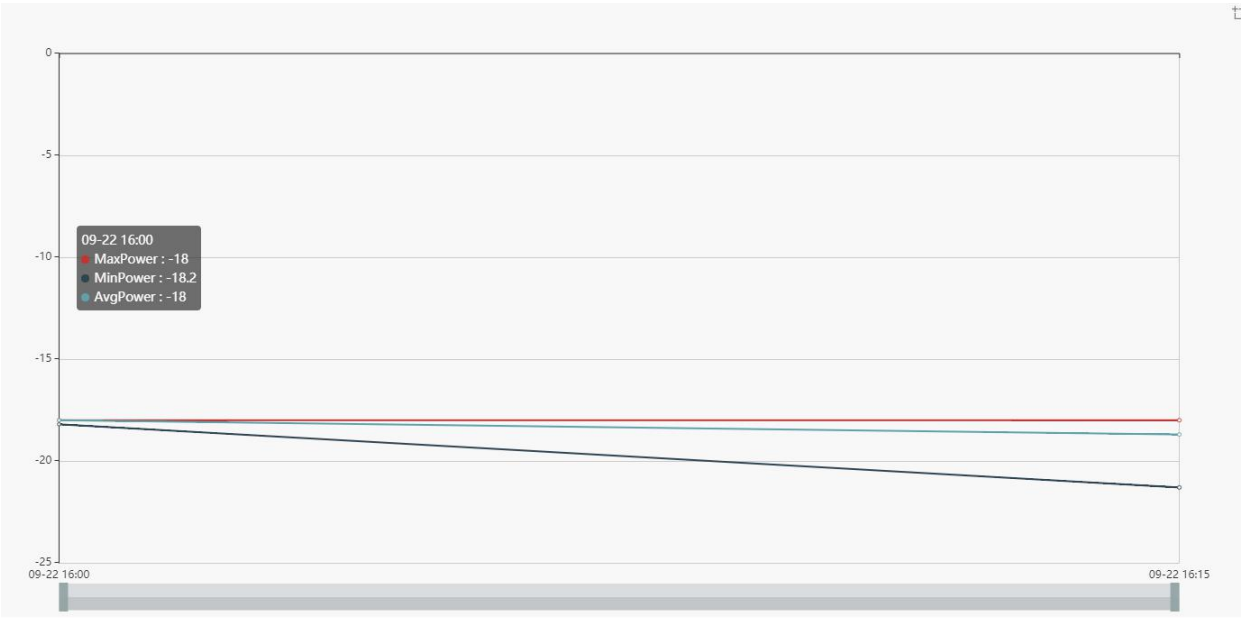


Figure 7-55 15-Minute Chart Data of Optical Power

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:

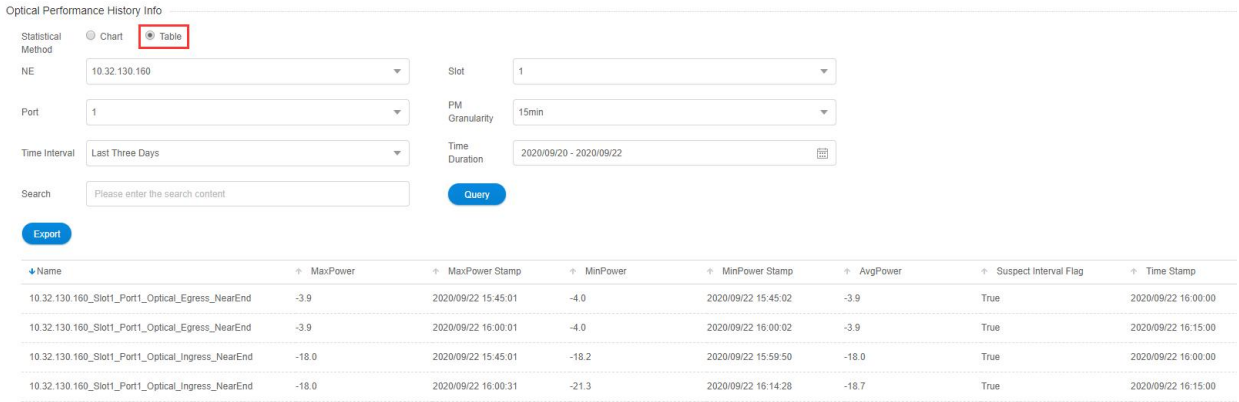


Figure 7-56 15-Minute Tabular Interface of Optical Power

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:

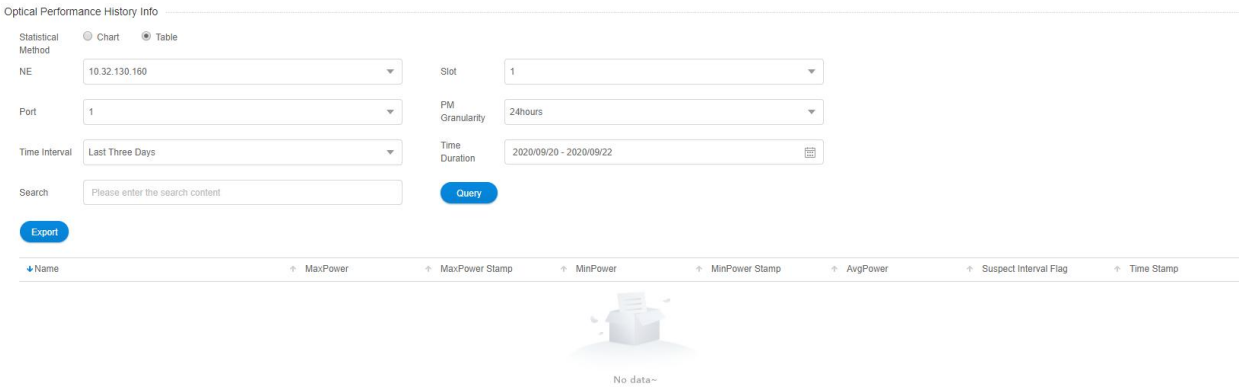


Figure 7-57 15-Minute Tabular History Data of Optical Power

7.3.1.3. 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:

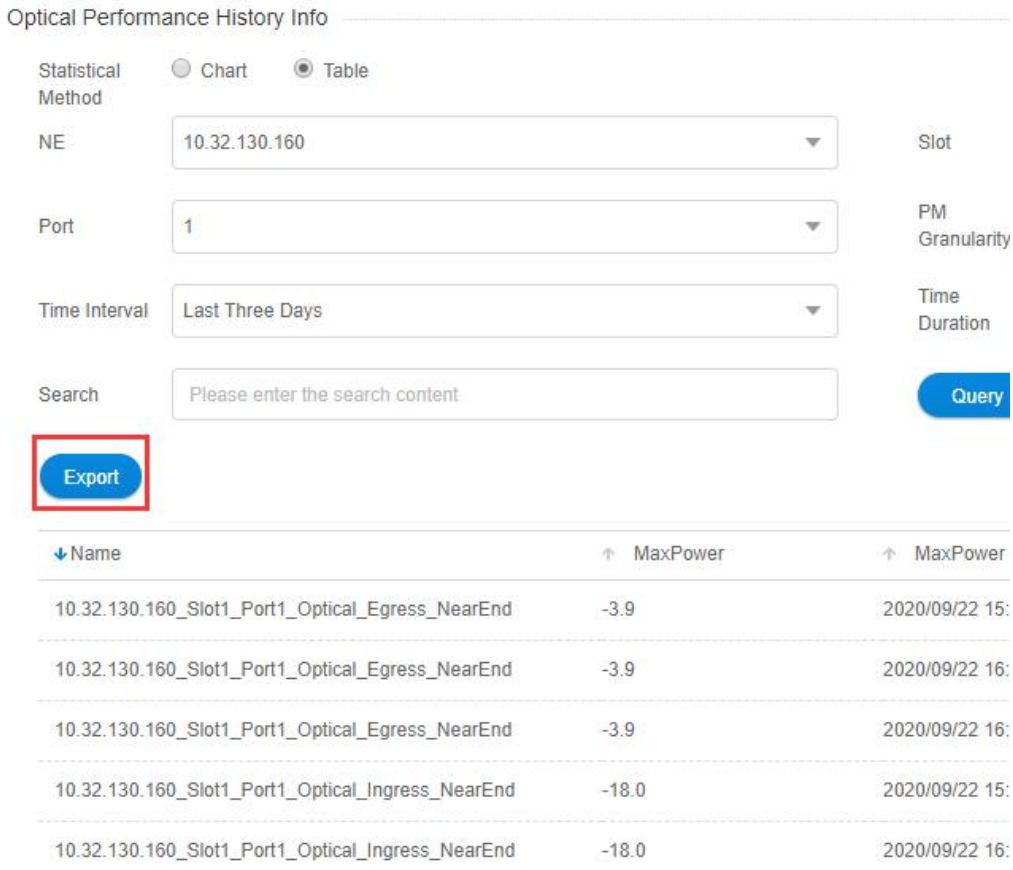


Figure 7-58 Export History Data of Optical Power

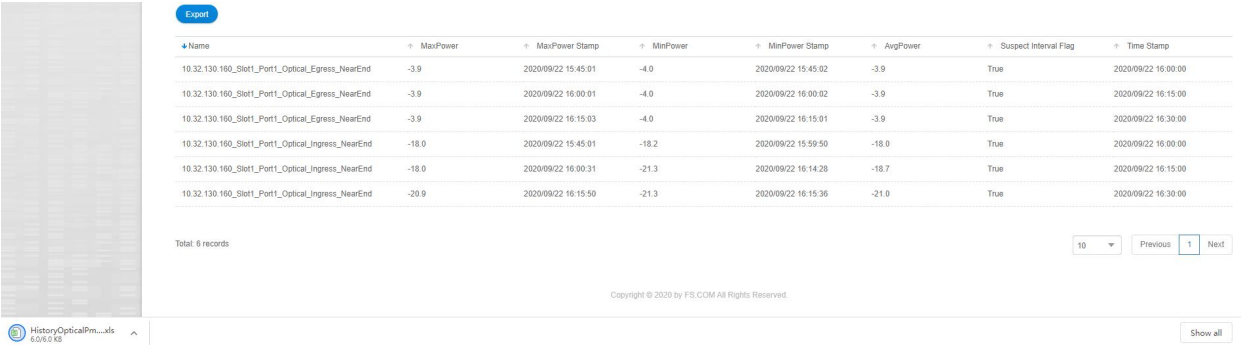


Figure 7-59 Successfully Export Data of Optical Power

7.3.2. OCh History Performance Statistics

7.3.2.1. 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.

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

(2) Performance Monitoring Point: entrance-near end.

(3) 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).

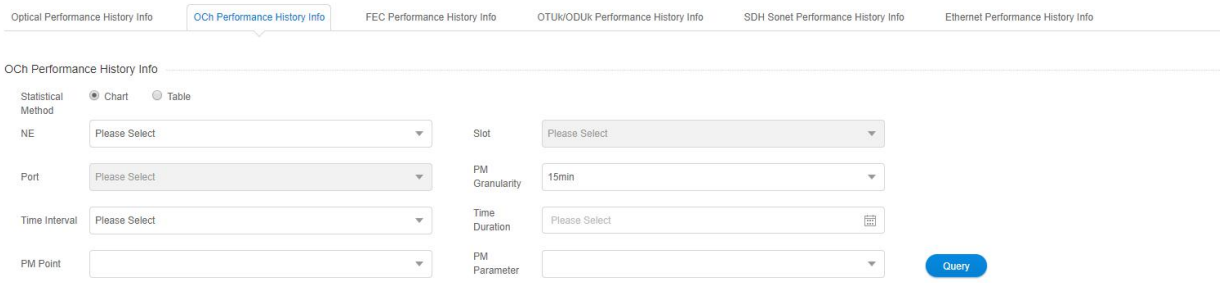


Figure 7-60 OCh History Performance Parameters

7.3.2.2. View OCh History Monitoring Information

15 minutes and 24 hours 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.

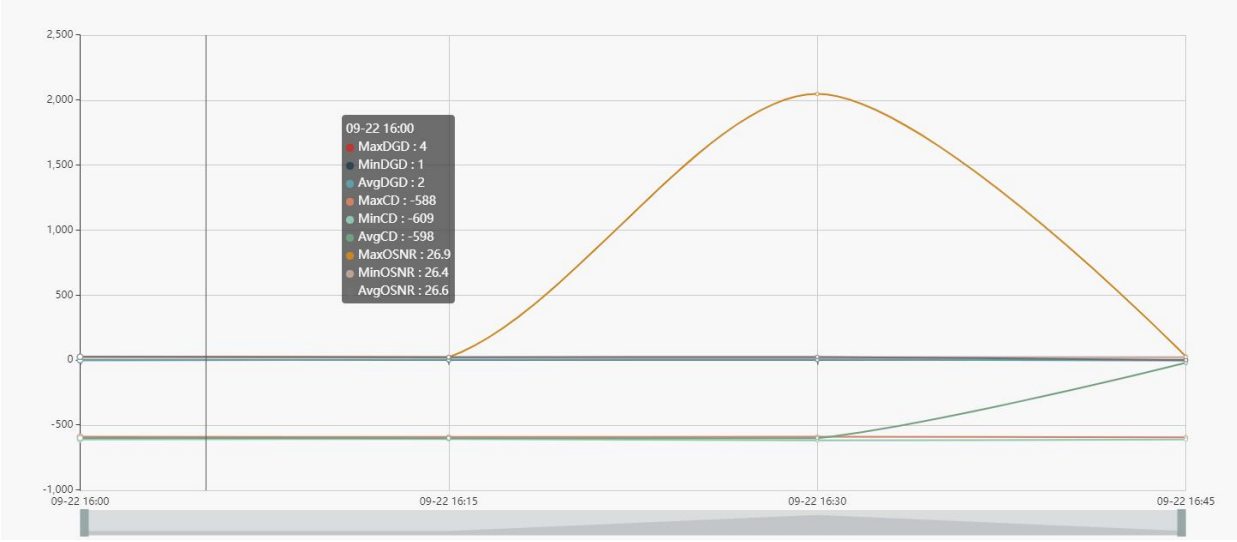


Figure 7-61 15-Minute Chart Data of OCh

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:

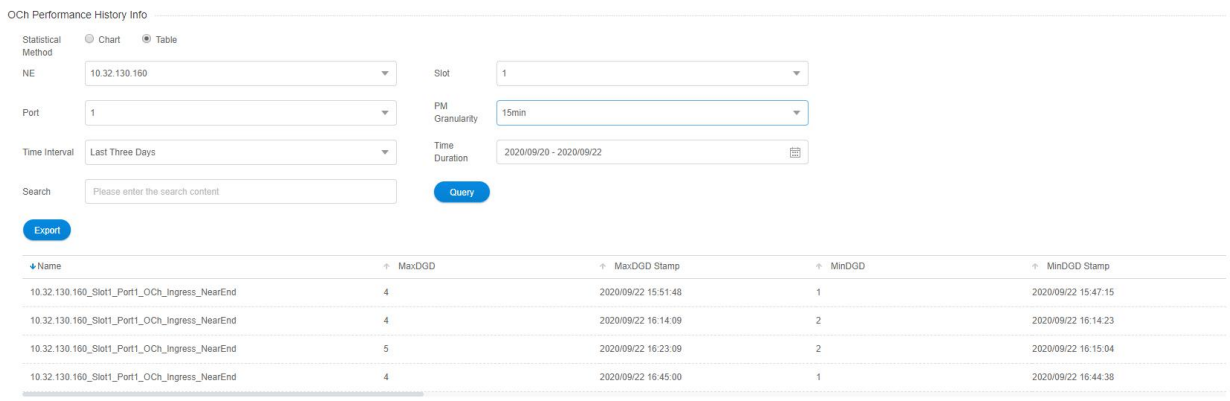


Figure 7-62 15-Minute Tabular Interface of OCh

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:

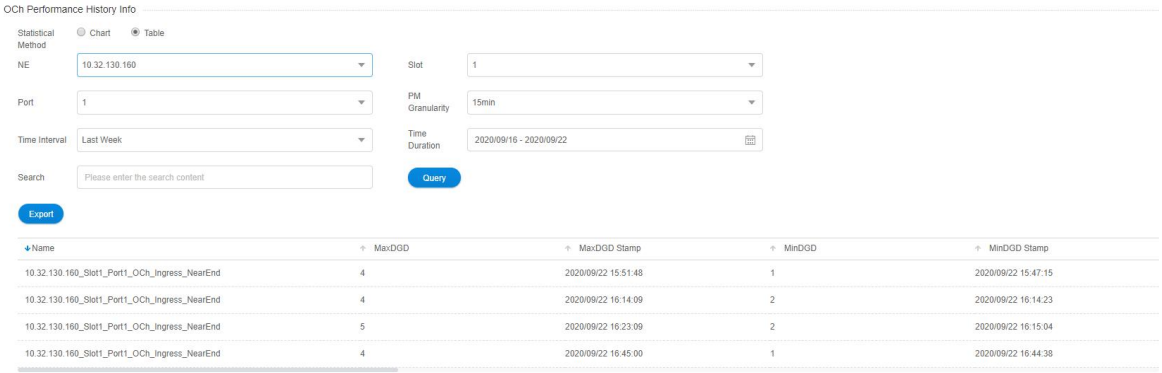


Figure 7-63 15-Minute Tabular History Data of OCh

7.3.2.3. Export OCh 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:

Figure 7-64 Export History Data of OCh

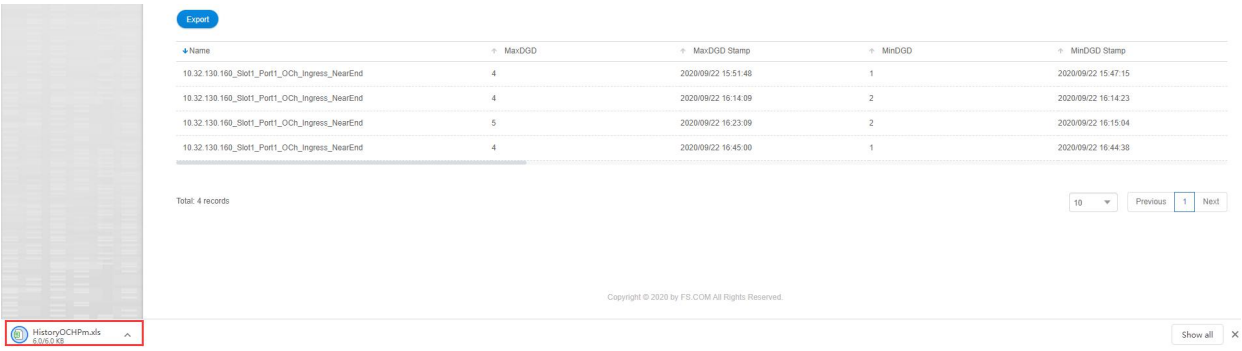


Figure 7-65 Successfully Export Data of OCh

7.3.3. FEC History Performance Statistics

7.3.3.1. 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.

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

(2) Performance Monitoring Point: entrance-near end.

(3) Performance Monitoring Parameters: maximum error correction rate and average error correction rate.

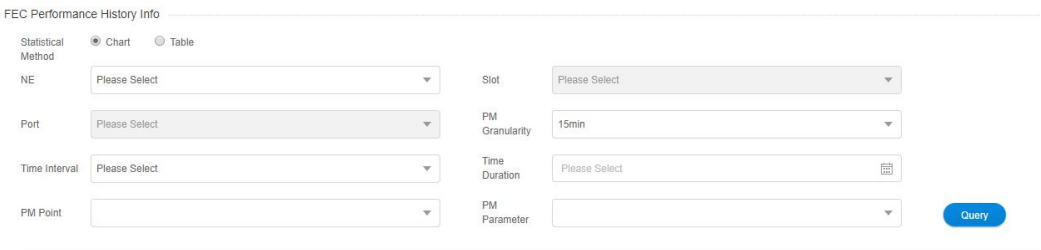


Figure 7-66 FEC History Performance Parameters

7.3.3.2. View FEC History Monitoring Information

15 minutes and 24 hours 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.

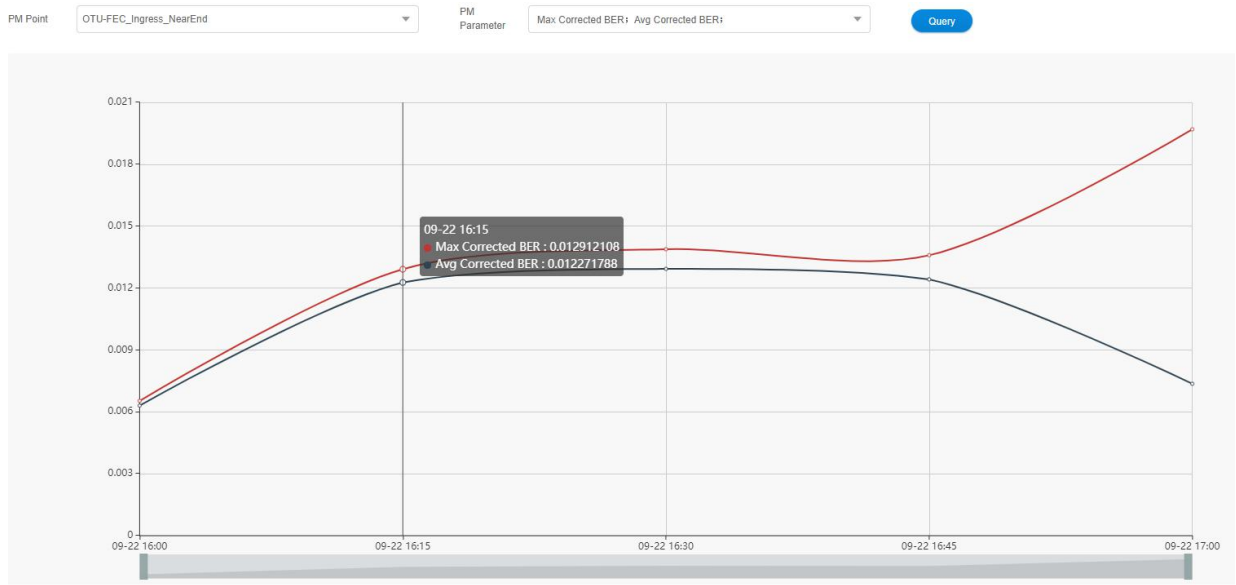


Figure 7-67 15-Minute Chart Data of FEC

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:

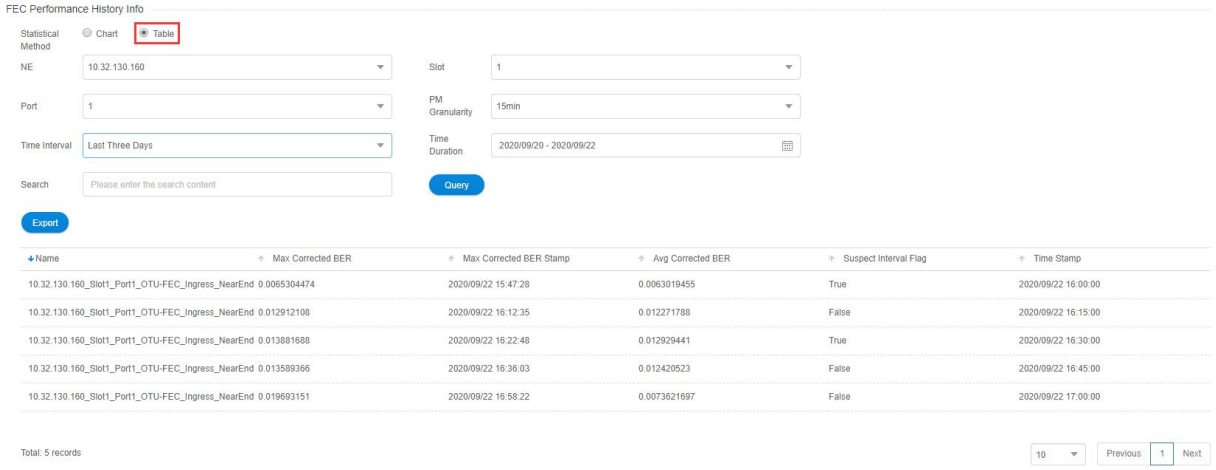


Figure 7-68 15-Minute Tabular Interface of FEC

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:

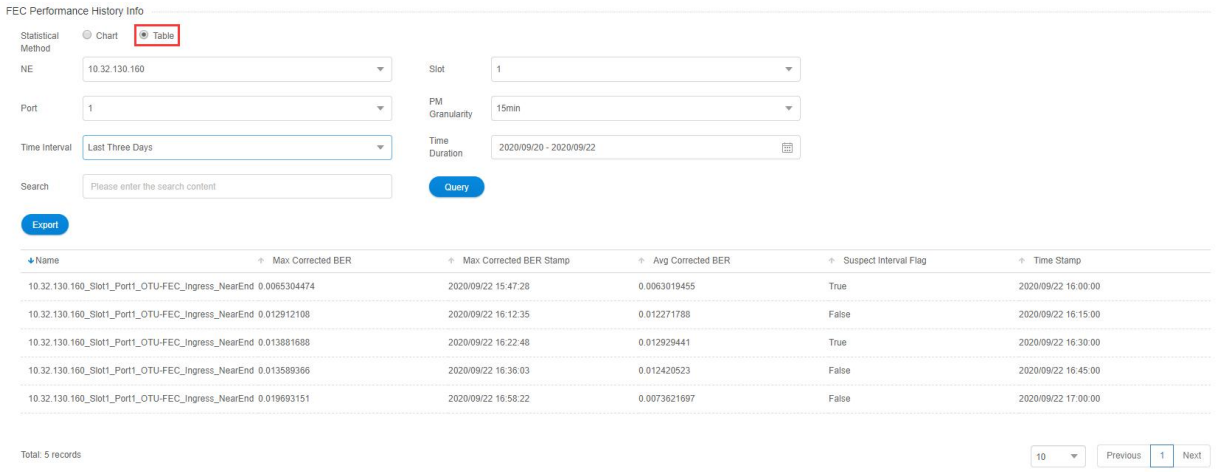


Figure 7-69 15-Minute Tabular History Data of FEC

7.3.3.3. 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:

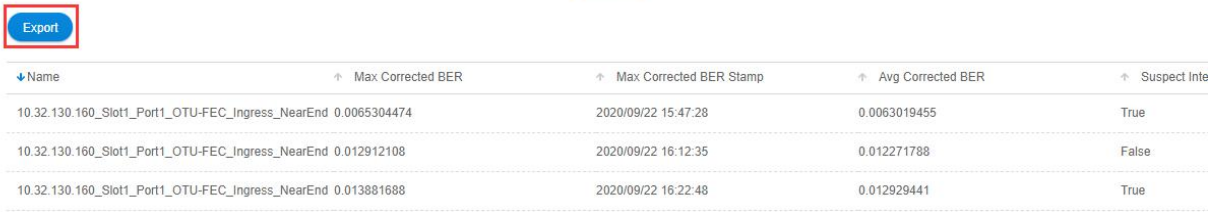


Figure 7-70 Export History Data of FEC

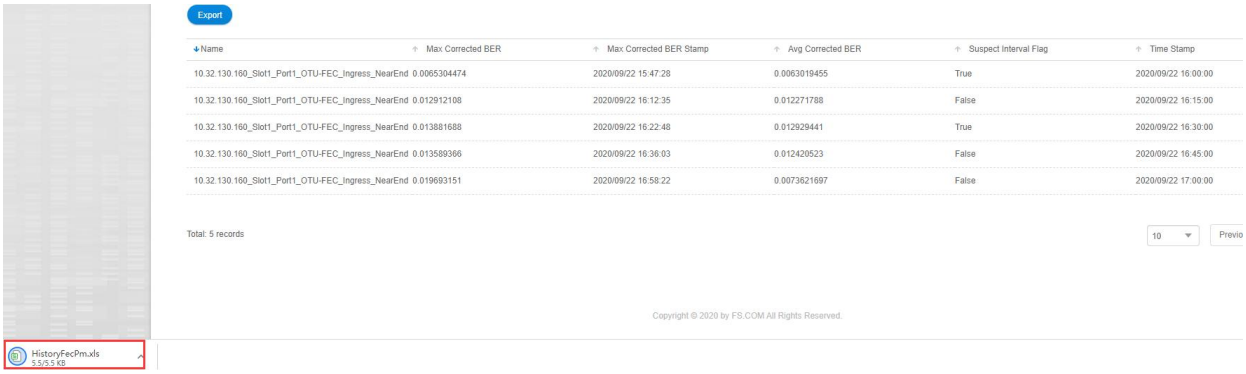


Figure 7-71 Successfully Export Data of FEC

7.3.4. OTUk/ODUk History Performance Statistics

7.3.4.1. 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.

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

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

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

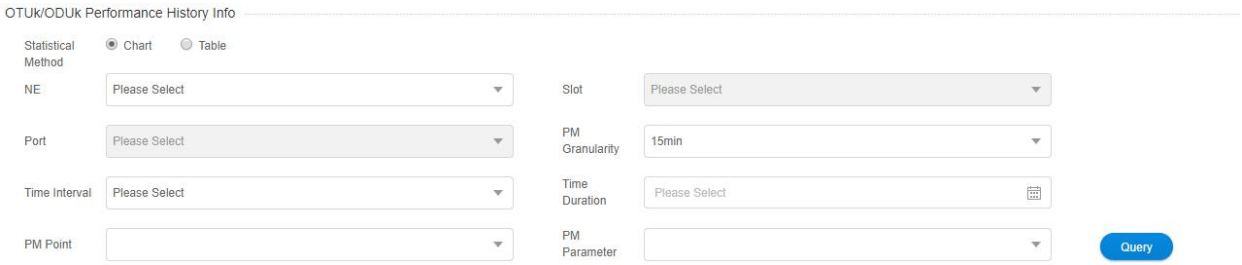


Figure 7-72 OTUk/ODUk History Performance Parameters

7.3.4.2. View OTUk/ODUk History Monitoring Information

15 minutes and 24 hours 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.

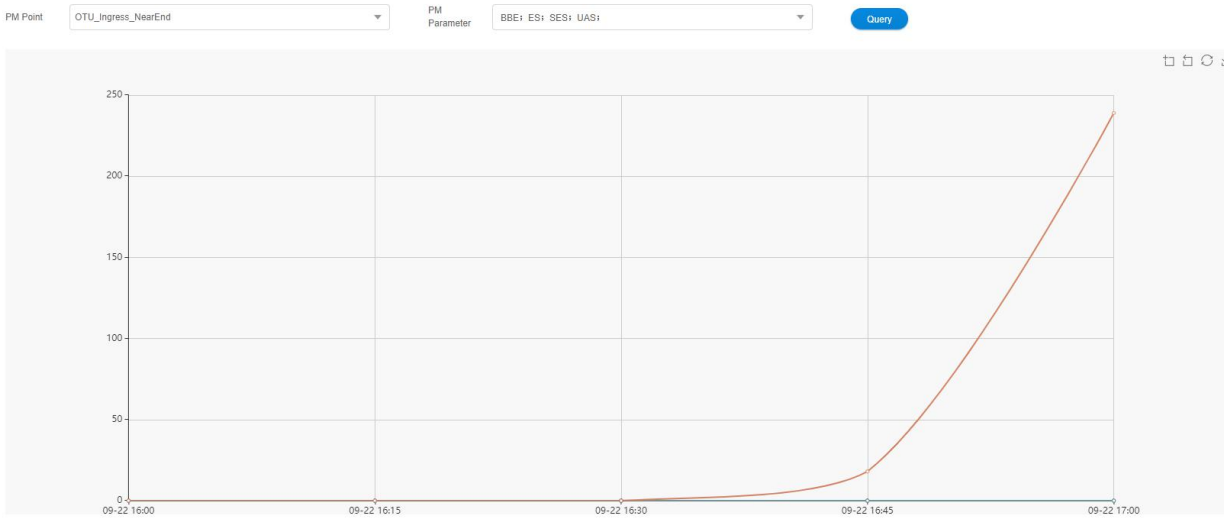


Figure 7-73 15-Minute Chart Data of OTUk/ODUk

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:

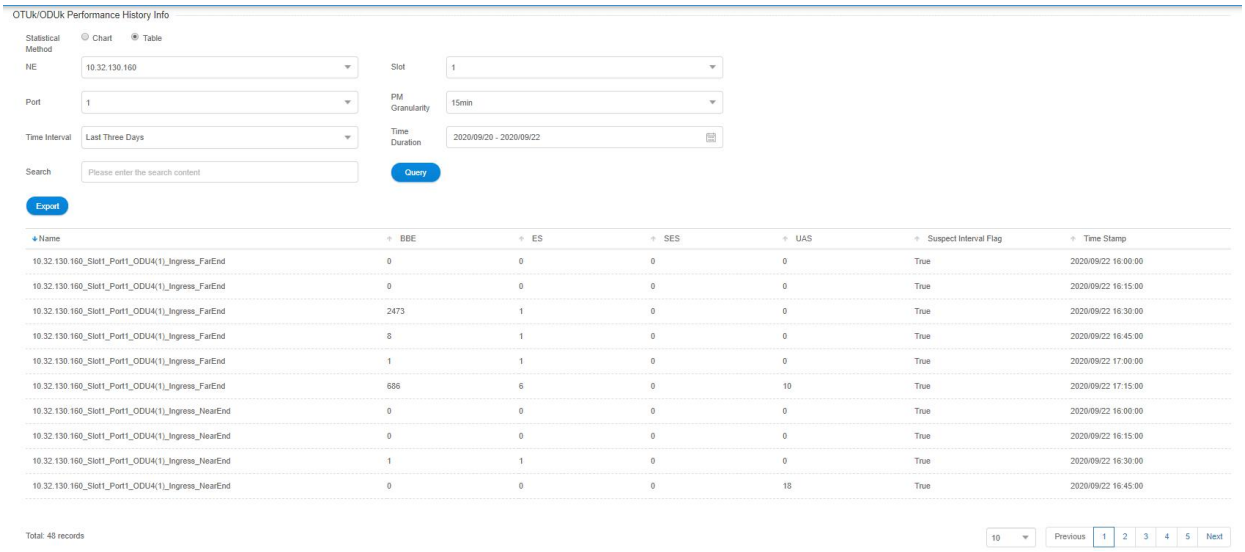


Figure 7-74 15-Minute Tabular Interface of OTUk/ODUk

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:

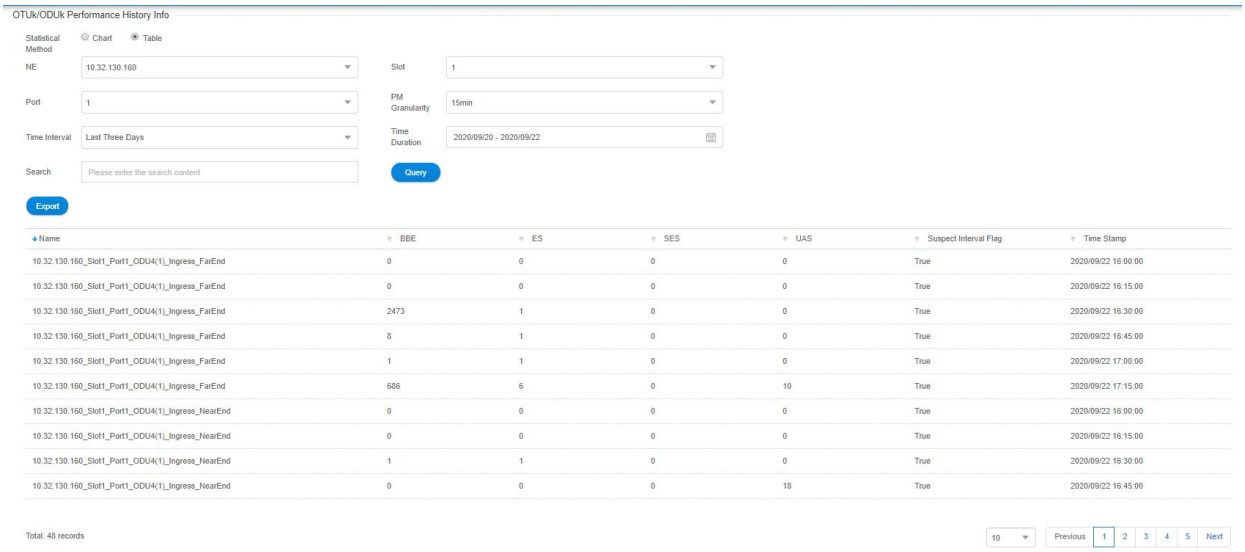


Figure 7-75 15-Minute Tabular History Data of OTUk/ODUk

7.3.4.3. 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:

Figure 7-76 Export History Data of OTUk/ODUk

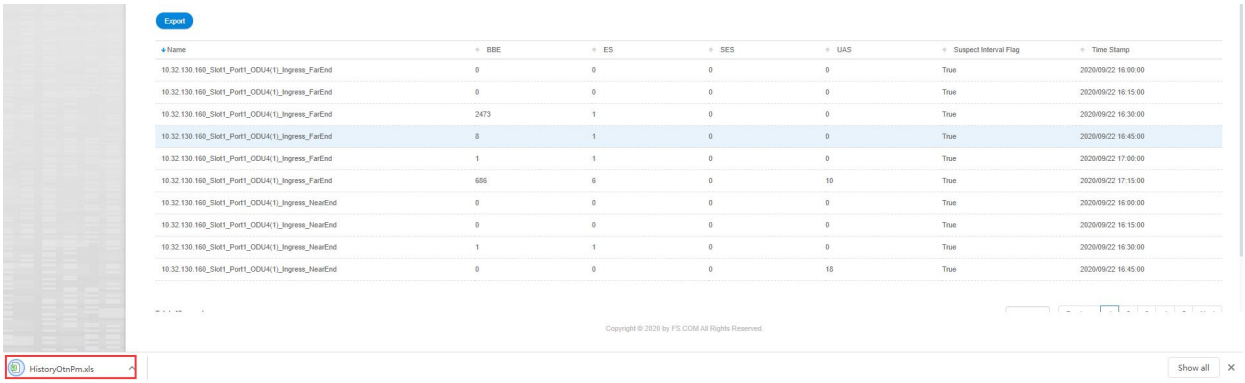


Figure 7-77 Successfully Export Data of OTUk/ODUk

7.3.5. History Performance Statistics of Ethernet

7.3.5.1. 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.

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

(2) Performance Monitoring Point: entrance-near end, exit-near end.

(3) 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.

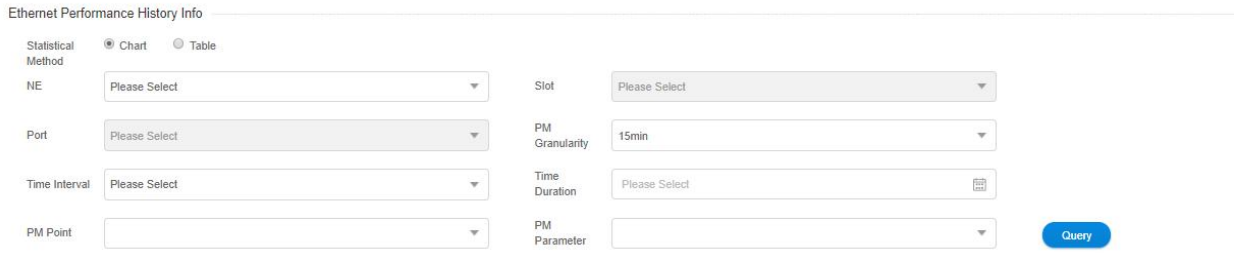


Figure 7-78 Ethernet History Performance Parameters

7.3.5.2. View Ethernet History Monitoring Information

15 minutes and 24 hours 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.

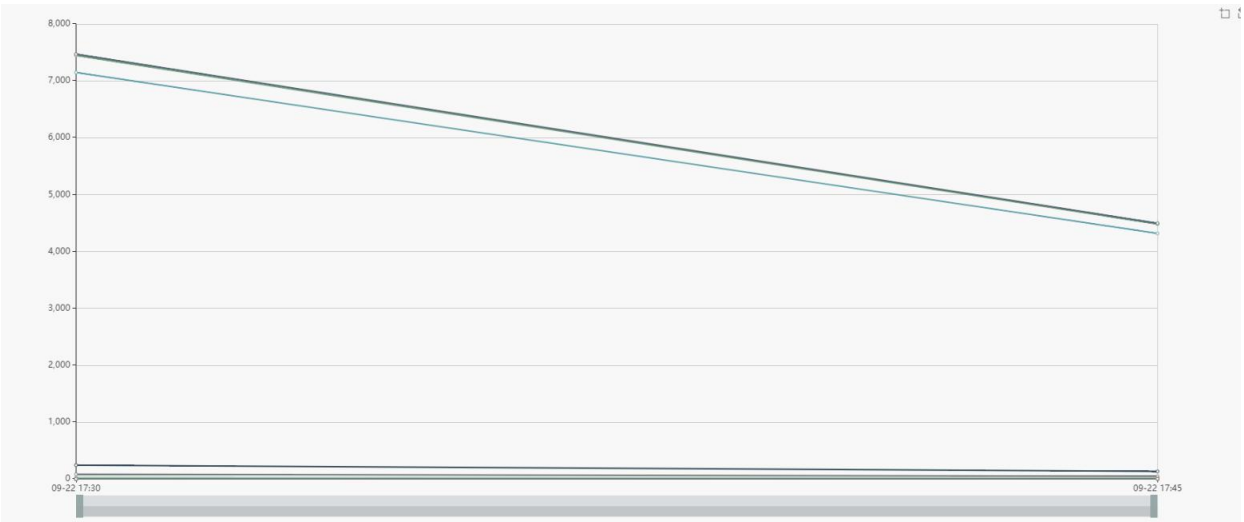


Figure 7-79 15-Minute Chart Data of Ethernet

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:

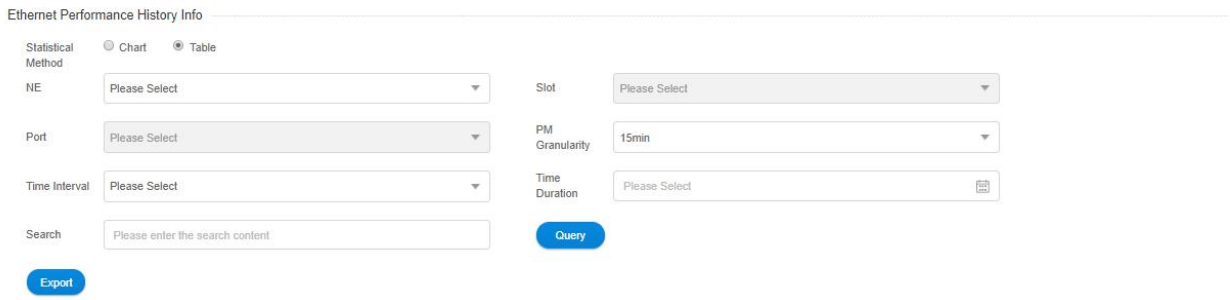


Figure 7-80 15-Minute Tabular Interface of Ethernet

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:

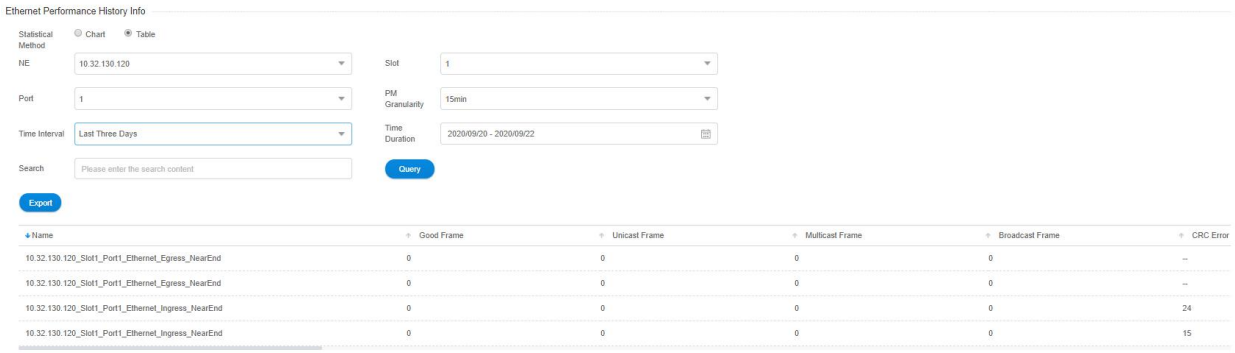


Figure 7-81 15-Minute Tabular History Data of Ethernet

7.3.5.3. 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:

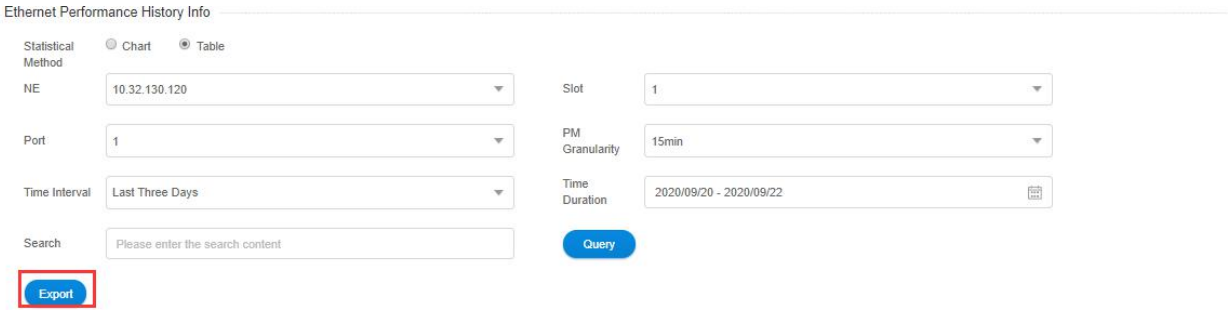


Figure 7-82 Export History Data of Ethernet

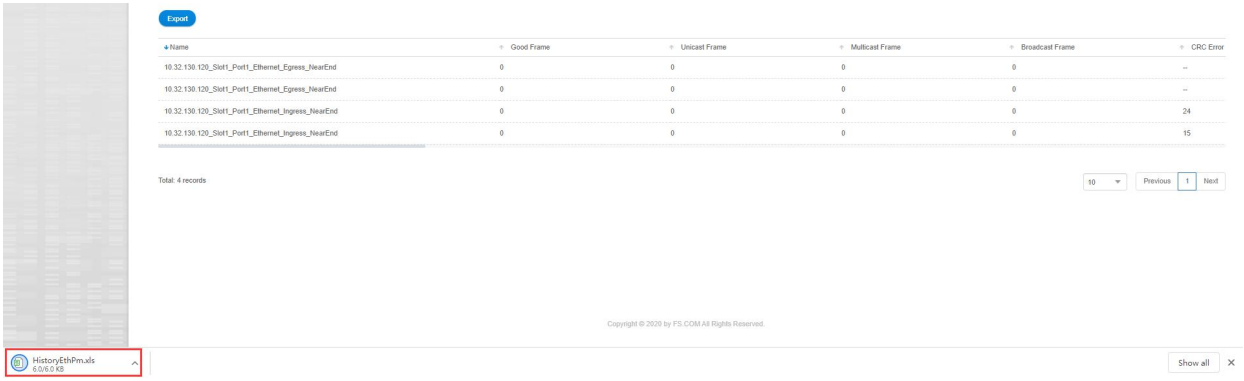


Figure 7-83 Successfully Export Data of Ethernet

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
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