FMX Series Network Element Configuration Guide



Contents

Preface	1
1. Preparation Before Configuration	3
1.1. Configuration Process	3
1.2. Connect NMS System & NE	3
1.3. Start Network Management Service	4
1.3.1. Start Server Program	4
2. Create Network	6
2.1. Network Creation Process	6
2.2. Login NMS Interface	7
2.3. Create Group	8
2.4. Add NE	8
2.4.1. Add NE	8
2.4.2. Modify NE	9
2.4.3. Delete NE	9
2.4.4. Delete Single module	10
2.5. Manage NE IP	10
2.5.1. Node IP Configuration	10
2.5.2. NMS IP1 Configuration	11
2.5.3. Local NMS IP Configuration	12
2.5.4. Gateway Configuration	12
2.6. Configure FTP Server	13
2.7. SNMP Trap Configuration	14
2.8. Configure NE Time	15
2.8.1. Configure NTP Server	15
2.8.2. Configure NE Time	16
2.9. Configure NE Data	17
2.9.1. Save NE Configuration	17
2.9.2. Upload NE Configuration	18
2.9.3. Download NE Configuration	19
2.9.4. Restore NE Default Configuration	20
2.10. Create Fiber Optic	20
2.10.1. Adjust NE Layout	20
2.10.2. Create Link between NEs	20

2.10.3. Save Layout	
3. DCN Configuration	
3.1. DCN Introduction	
3.2. Configuration Steps	
3.2.1. Direct Connection between PC and Device	
3.2.2. Forwarding through Router	24
3.3. Configuration Example	
3.3.1. Direct Connection between PC and Device	
3.3.2. Forwarding Trough Routers	
4. NE & Module Configuration	
4.1. Shelf Information	
4.1.1. FMX-100G-CH2U	
4.2. LED Indicator Information	
4.2.1. NMU Module	
4.2.2. System Interface LED Indicator	
4.2.3. Business Module LED Indicator	
4.2.4. Fan Tray LED Indicator	
4.2.5. Port LED Indicator of Business Module	
4.2.6. Power Tray LED Indicator	
4.3. View Single Module Information	
4.4. Port Configuration	
4.4.1. Basic Information	
4.4.1.1. Interface Configuration	
4.4.1.2. ODU2/ODU2e Configuration	
4.4.1.3. OTU2/OTU2e Configuration	
4.4.1.4. ODU4 Configuration	
4.4.1.5. OTU4 Configuration	
4.4.2. Parameter Description	41
4.5. Configuration of Optical Module Information	42
4.5.1. SFP/SFP+ Optical Transceiver Information	
4.5.2. CFP Optical Transceiver Information	
4.5.3. WDM CFP Optical Transceiver Configuration	
5. Service Configuration	46
5.1. Electric Cross-Connect Introduction	46
5.1.1. Unidirectional Cross-Connection without Protection	

5.1.2. Bidirectional Cross-Connection without Protection	47
5.1.3. Unidirectional Cross-Connection with Protection	48
5.1.4. Bidirectional Cross-Connection with Protection	49
5.2. Service Type	49
5.2.1. Service Type	49
5.2.2. Service Mapping	
5.2.2.1. AMP	51
5.2.2.2. BMP	51
5.2.2.3. GMP	51
5.2.2.4. GFP-F	52
5.2.2.5. GFP-Fextp	52
Service Configuration Process	53
5.3. Configuration instructions	53
5.3.1. FMX-100G-MXP10	53
5.3.1.1. Service Type	54
5.3.1.2. Time Slot Configuration	55
5.3.1.3. Cross-Connection Configuration	57
5.3.1.4. FEC Configuration	
5.3.2. FMX-100G-TMXP2	
5.3.2.1. Service Type	59
5.3.2.2. Time Slot Configuration	62
5.3.2.3. Cross-Connection Configuration	64
5.3.2.4. FEC Configuration	64
5.4. Configuration Example	66
5.4.1. Service Transparent Transmission Configuration Example	66
5.4.2. Configuration Example of Service Protection	67
5.4.3. Configuration Example of Ring Network Service	68
6. Overhead Configuration	71
6.1. Configuration Rules	71
6.1.1. SM, PM & TCMi Overhead Introduction	71
6.1.2. Overhead Configuration Rules	71
6.1.3. TTI Configuration Rules	71
6.2. Configuration Steps	72
6.2.1. SM Configuration Steps	72
6.2.2. PM Configuration Steps	75

6.3. Configuration Examples	79
7. SNC Protection Configuration	
7.1. Introduction of SNC Protection	
7.2. Configuration Steps	
7.3. Configuration Example	
8. Alarm Management	90
8.1. Alarm Management Introduction	90
8.2. Main Interface of Alarm Management	90
8.2.1. Current Alarm	90
8.2.2. History Alarm	
8.3. Alarm Configuration	97
8.3.1. Alarm Configuration	97
8.3.2. Alarm Notification Configuration	
8.3.3. Alarm Mailbox Server configuration	
8.3.4. Enable the Alarm Sound	
9. Performance Management	
9.1. Performance Management Introduction	
9.1.1. Filter Box	
9.1.2. Performance Monitoring Point Introduction	
9.1.3. Enable Performance Monitoring Point	
9.1.4. Disable Performance Monitoring Point	
9.1.5. Attentions for Monitoring Performance	
9.2. Current Performance Statistics	
9.2.1. Monitoring of Optical Power	
9.2.1.1. Introduction of Optical Power Monitoring Parameters	
9.2.1.2. View Optical Power Monitoring Information	
9.2.1.3. Reset Optical Power Monitoring Data	
9.2.1.4. Optical Power Monitoring Data Shown as NA	
9.2.2. OCh Current Performance Statistics	
9.2.2.1. OCh Monitoring Parameters Introduction	
9.2.2.2. View OCh Monitoring Information	
9.2.2.3. Reset OCh Monitoring Data	
9.2.2.4. OCh Monitoring Data Shown as NA	
9.2.3. FEC Current Performance Statistics	
9.2.3.1. FEC Monitoring Parameters Introduction	

9.2.3.2. View FEC Monitoring Information	
9.2.3.3. Reset FEC Monitoring Data	110
9.2.3.4. FEC Monitoring Data Shown as NA	
9.2.4. OTUk/ODUk Current Performance Statistics	
9.2.4.1. OTUk/ODUk Monitoring Parameters Introduction	
9.2.4.2. View OTUk/ODUk Monitoring Information	112
9.2.4.3. Error Generation Conditions for Monitoring Parameters	112
9.2.4.4. OTUk/ODUk Monitoring Data Reset	113
9.2.4.5. OTUk/ODUk Monitoring Data Shown as NA	113
9.2.5. Current Performance Statistics of SDH Regeneration Segment	114
9.2.5.1. Monitoring Parameters Introduction of SDH Regeneration Segment	
9.2.5.2. View Monitoring Information of SDH Regeneration Segment	115
9.2.5.3. SDH Regeneration Segment Monitoring Data Reset	115
9.2.5.4. Monitoring Data of SDH Regeneration Segment Shown as NA	116
9.2.6. Current Performance Statistics of Ethernet	
9.2.6.1. Ethernet Monitoring Parameters Introduction	117
9.2.6.2. View Ethernet Monitoring Information	
9.2.6.3. Ethernet Monitoring Data Reset	118
9.2.6.4. Ethernet Monitoring Data Shown as NA	
9.3. History Performance Statistics	119
9.3.1. History Performance Statistics of Optical Power	119
9.3.1.1. History Monitoring Parameters Introduction of Optical Power	119
9.3.1.2. View History Monitoring Information of Optical Power	120
9.3.1.3. Export History Monitoring Information of Optical Power	121
9.3.2. OCh History Performance Statistics	122
9.3.2.1. OCh History Monitoring Parameters Introduction	
9.3.2.2. View OCh History Monitoring Information	
9.3.2.3. Export OCh History Monitoring Information	124
9.3.3. FEC History Performance Statistics	
9.3.3.1. FEC History Monitoring Parameters Introduction	
9.3.3.2. View FEC History Monitoring Information	
9.3.3.3. Export FEC History Monitoring Information	
9.3.4. OTUk/ODUk History Performance Statistics	
9.3.4.1. OTUk/ODUk History Monitoring Parametes Introduction	
9.3.4.2. View OTUk/ODUk History Monitoring Information	128

9.3.4.3. Export OTUk/ODUk History Monitoring Information129
9.3.5. History Performance Statistics of SDH Regeneration Segment
9.3.5.1. History Monitoring Parameters Introduction of SDH Regeneration Segment
9.3.5.2. View SDH Regeneration Segment History Monitoring Information
9.3.5.3. Export SDH Regeneration Segment History Monitoring Information
9.3.6. History Performance Statistics of Ethernet
9.3.6.1. Ethernet History Monitoring Parameters Introduction
9.3.6.2. View Ethernet History Monitoring Information
9.3.6.3. Export Ethernet History Monitoring Information134
10. Abbreviation

Preface

Overview

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

Content Introduction

This manual mainly introduces the general operation of the network management platform, including installation and startup of the FMX NMS system, login, exit, password change, security management, system management of network element, alarm management, log management, performance management, routine maintenance of the FMX 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
A Danger	Special attention should be paid to the content. If the operation is improper, it may cause serious injury to the person.
Attention	It reminds the matters for attention. Improper operation may cause loss of data or damage to the device.
Hint	It represents the operation or information that requires special attention to ensure the success of the operation or the normal work of the device.
Knack	A skill or a knack which helps to solve a problem and save time.
Explain	The necessary supplement and explanation for the description of the text.
Rote	Notes contain helpful suggestions or references to material not covered in the manual.

Rote

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

1. Preparation Before Configuration

1.1. Configuration Process

When configuring FMX 100G modules on FMX NMS system, some rules and orders must be followed.

If the whole project and its configuration are initially created, please refer to process in 2-1 to complete the operation. If the project has been created, only the configuration of one NE or single card needs to be changed, please perform the operation according to relevant content of chapters in Figure 2-1.



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

🕜 Hint

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

1.2. Connect NMS System & NE

For different network devices, there are multiple connection ways to connect FMX NMS network management computer and FMX 100G modules network elements. Normally the FMX NMS Server and FMX 100G modules Network Element are both connected to a HUB by direct connection network cable. But the FMX NMS Server can also be directly connected to FMX 100G modules Network Element's management port through twisted pair cable or direct connection 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 Ethemet port of HUB and connect the other end to MGMT1/MGM2 of SC module for FMX 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 FMX NMS system has been installed on the network management host.

1.3.1. Start Server Program



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



Figure 1-3 Start NMS Server

2. Create Network

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

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

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

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

It will introduce the creation steps of the network topology according to the configuration process in the following passage. Moreover, it will focus on the parameter configuration related to FMX 100G modules in each step, and only the sections of the reference book will be provided for the common configuration steps for each device. FMX NMS-related software was pre-installed when the network management host was manufactured. When the network management host was turned on, the network topology could be created according to the configuration process. This chapter includes the following content:

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

2.1. Network Creation Process

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

Steps

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

	× +				- 0	×
\leftrightarrow \rightarrow G (0)	localhost:9090			07 Q Å	0	:
						16
		root	2			
			0			
		Re	set			
		Lo	gin			

Figure 2-2 Login NMS System

2.3. Create Group

Right click on "*Global View*" on the top after clicking on "*Global View*", and then click on "*Add Group*". Input group name and description information. The description information can be blank. After that, click on "*Apply*".

G .	Home System Management	Configuration Management	Fault Management Performance M Add Group	agement OLP Rou	te	0	01		•		
B Global View		¢ @ Q ↔	Parent Node	Global View		\$10	0,		System Time	2019-12-	20 10:30:29
= m test			Describe Info	(69)							
				Apply Close							

Figure 2-3 Add Node

Right click on the group which has been created, or click on "Configuration Management" on the top after clicking on the group which has been created, you can continue to add the child group. Enter the name of the child group, click on "Apply".

(•••	Home	System Management	Configuration	Manageme	nt F	ault Management Add Group	Performance Ma	nagement	Security Man	agement Log	Manage ×	ment Ol	.P Route					
						0		in at					₩6	O 4	O ¹		@ 0	
B Global View			•	QQ		Parent Node		test								System Time	: 2019-12	-20 10:29:47
🖻 💼 test						Group Name		OTN										
						Describe Info												
										Apply Close	•							



2.4. Add NE

2.4.1. Add NE

Right click on the node which has been added, or click on "Configuration Management" on the top after clicking on the node which has been added. Then click on "Add NE", input the NE name, NE IP address, subnet mask, Trap host name, Trap host IP address, and click on "Apply".

.	Home System N	lanagement Cor	figuration Management	Fault Management	Performance Management Security N	Aanagement Log Management	OLP Route				
					100		₩6	⊘ 4	01	00	root
B Global View			000.	Parent Node	test						0 10 35 48
* entesti				Display Name	OTN						
				IP Address	10.32.130.116						
				Subnet Mask	255 255 255 0						
				Trap Name	trap						
				Trap Host	10.32.130.19						
						Apply Close					

Figure 2-5 Add NE

2.4.2. Modify NE

Right click on the NE which has been added, or click on "Configuration Management" on the top after clicking on the NE which has been added, and then click on "Modify NE". Here you can only modify the display name of the NE.

Home System Management Configuration	n Management Fault Mar	ify Equipment Performance Mana	oement Security Management Log Man	agement OLP Route	2	~		~	•	
	Pare	rent Node	test		% 0	04	0			
B ditest	Disp	play Name	OTN							
	IPA	Address	10.32.130.116							
	Subi	bnet Mask	255.255.255.0							
			Apply Close							

Figure 2-6 Modify NE

Rote

Trap IP is NMS server IP.

2.4.3. Delete NE

Right click on the NE which has been added, or click on "Configuration Management" on the top after clicking on the NE which has been added, and then click on "Delete NE".



Figure 2-7 Delete NE

2.4.4. Delete Single module

Prerequisite

There is no single module service or cross-module service running on this module.

Right click on the single module which has been added, or click on "*Configuration Management*" on the top after clicking on the single module which has been added, and then click on "*Delete Card*".



Figure 2-8 Delete Card

Attention

modules can be only added in available slots. Absent slots can be deleted.

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 "System Management" on the top, and then click on "MGMT IP Configuration".



Figure 2-9 Manage IP Configuration

Enter "MGMT IP Configuration" interface, input the IP address of the node, and then click on "Apply".



Figure 2-10 Manage IP Configuration

2.5.2. NMS IP1 Configuration

Click on the NE which has been added \rightarrow Click on "System Management" on the top \rightarrow Click on "MGMT IP Configuration" \rightarrow "Configure NMS IP1".



MGMT IP Configuration

Area	Global View>tes	st	NE	OTN(10.32.130.116)
Node IP		192.168.13	30.116	
NMS IP1				
IP Address		10.32.130	.116	
Subnet Mask		255.255.2	55.0	
OSPF		Enable		•
LCT IP				
IP Address		192.168.1	26.1	
Subnet Mask		255.255.2	55.252	
Gateway		10.32.130	.254	
Default route rodistribution	e-	Disable		v
				Apply Close

Figure 2-11 NMS IP1 Configuration

2.5.3. Local NMS IP Configuration

Ŀ.

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

LCT IP(MGMT_Port2)	
IP Address	192.168.126.1
Subnet Mask	255.255.255.252

Figure 2-12 Local NMS IP Configuration

2.5.4. Gateway Configuration

Click on the NE which has been added \rightarrow Click on "System Management" on the top \rightarrow Click on "Manage IP Configuration" \rightarrow "Gateway Configuration". Input gateway IP address, and click on "Apply".

GFS

Area	Global View>tes	t	NE	OTN(10.32.130.116)
Node IP	[192.168.13	30.116	
NMS IP1				
IP Address		10.32.130	.116	
Subnet Mask		255.255.2	55.0	
OSPF		Enable		v
LCT IP				
IP Address		192.168.1	26.1	
Subnet Mask		255.255.2	55.252	
Gateway		10.32.130	254	
Default route re distribution	-	Disable		v



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
- SC/LC Card BSP Upgrade
- Performance Management

Rote

Only one live FTP server for universal NMS server topology. For Multi-NMS server NMS topology, user can define multi-FTP servers.

Click on the NE which has been added \rightarrow Click on "System Management" on the top \rightarrow Click on "FTP Server Configuration" to make configuration, and input the IP address of the FTP server, then click on "Apply".

FTP Ser	ver Configuration	X
	Current Value	Set Value
IP	192.168.66.146	
		Apply Close

Figure 2-14 Configure FTP Server

2.7. SNMP Trap Configuration

Click on the NE which has been added \rightarrow Click on "System Management" on the top \rightarrow Click on "SNMP Trap Configuration" to make configuration. Enter SNMP Trap configuration interface, click on "Apply".

SNM	P Trap Co	onfiguration				
Area	Global View>test		NE	OTN(10.32.130.1	16)	
То	ol					> + × ∅
Show	10 🔻	entries			Search:	Search
	ID J1	Name 🕸	Trap Host ↓↑	Trap Port 1	Storage Type	Trap State ↓↑
	1	111	192.168.126.2	16222	NonVolatile	Active
	2	2	10.32.130.188	16222	NonVolatile	Active
	3	TRAP1	10.32.130.20	16222	NonVolatile	Active
	4	internal0	127.0.0.1	162	ReadOnly	Active
	5	internal1	127.0.0.1	162	ReadOnly	Active
Show	ing 1 to 5 of	5 entries				Previous 1 Next

Figure 2-15 SNMP Configuration

Click on"+"button in the toolbar to add trap address. The default port number of trap is 16222. It is not recommended to modify this port number.

\$ SNMP Trap Configu	Iration							
Area	Global View>test	NE	OTN(10.32.130.116)					
Tool				^	+	×	/ K	3
Name		moon						
Trap Host		10.32.132.28						
Trap Port		16222						
				App	ly	CI	ose	

Figure 2-16 Add Trap Address

Attention

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

2.8. Configure NE Time

Click on the NE which has been added \rightarrow Click on "System Management" on the top \rightarrow Click on "NTP Configuration" to make relevant configuration.

2.8.1. Configure NTP Server



Figure 2-17 NTP Configuration

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

rea	Global View>test		NE	OTN(10.32.130.116)	
Server Basi	c Info				
Tool				^	+ × 2
Server IP		192.1.1.5			
					Apply
Show 10 •	entries			Search: Search	
	Server IP			Server Status	
	192.1.1.1			Unsupport	
	192.1.1.2			Unsupport	
	192.1.1.3	 Success! 		Unsupport	
	192.1.1.4			Unsupport	
	192.1.1.5		Apply	Unknown	
Showing 1 to 5 c	f 5 entries			Draviaua	4 Next

Figure 2-18 Configure NTP Server

2.8.2. Configure NE Time

Click on the NE which has been added \rightarrow Click on "System Management" on the top \rightarrow Click on "NE Time Configuration" to make relevant configuration.



Figure 2-19 NE Time Configuration

Configure the current time of NE in the pop-up, and click on "Apply".

NE Time Configuration

Area Global Vie	ew>test	NE	OTN(10.32.130.116)
NE Current Time	2019-12-2	20 19:35:39	
Time Zone	(GMT+8:	:00)	•
			Refresh Apply Close

Figure 2-20 Set NE Time

2.9. Configure NE Data

Configure NE Data:

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

2.9.1. Save NE Configuration

Click on the NE which has been added \rightarrow Click on "System Management" on the top \rightarrow Click on "Configuration Data Save".



Figure 2-21 Configuration Data Save

2.9.2. Upload NE Configuration

Click on the NE which has been added \rightarrow Click on "System Management" on the top \rightarrow Click on "Configuration Data Upload".



Figure 2-22 Configuration Data Upload

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

Uploaded File Name	21-73	
		Apply Close

Figure 2-23 Input NE Configuration File Name

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

	ing (D:) →	WPS \rightarrow NMS \rightarrow TFTP \rightarrow config		✓ Ö Search co	onfig	Q
	* ^	Name	Date modified	Туре	Size	
S	*	10.32.130.116_config.tar.gz	12/19/2019 6:39 PM	WinRAR 压缩文件	0 KB	
ts	*					

Figure 2-24 Upload Path of NE Configuration

2.9.3. Download NE Configuration

Click on the NE which has been added \rightarrow Click on "System Management" on the top \rightarrow Click on "Configuration Data Download".



Figure 2-25 Configuration Data Download

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

onfiguration Data Do	wnload	
Configuration Data Download	10.32.130.116_config.tar.gz	,
		Apply Close

Figure 2-26 Select Configuration File To Be Downloaded

2.9.4. Restore NE Default Configuration

Click on the NE which has been added→Click on "System Management" on the top→Click on "Default Configuration Data Restore".



Figure 2-27 Default Configuration Data Restore

2.10. Create Fiber Optic

2.10.1. Adjust NE Layout

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



Figure 2-28 Adjust NE Layout

2.10.2. Create Link between NEs

Click on "Link" button in the global view.



Figure 2-29 Click "Link" Button

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

Name	config				
Source					
Network	192.168.21.73	Ŧ	Shelf	1	٣
Slot	15	•	Port	1	٣
Dest					
Network	192.168.21.63	•	Shelf	1	•
Slot	1		Port	11	•

Figure 2-30 Create Link between NEs

2.10.3. Save Layout

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



Figure 2-31 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

Here we take 100G muxponder FMX-100G-MXP10 as an example.

3.3.1. Direct Connection between PC and Device

Step 1:

Open the GCC channel of the occupied port: the NMS port of PC is connected with the MGMT2 port of the device. Add the IP of 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 OTU2/OTU2e/OTU4/OCh (OTU4).

Port Management		х
BasicInfo	BasicInfo	
Port Configuration	Tool	
	Administrative State	Enabled v
	Operational State	Down
	Availability	Notinstalled
	Port Mode	XGE_BMP *
	Port Description	XGE_GRPF XGE_GRPF XGE_GRPFextp STIME_AMP CC192_AMP
Port9 Port10 Port11		01U2 01U2e 31M64_BMP 0C192_BMP

Figure 3-3 Enable OTU2/2e Port

Port Management		
	BasicInfo Tool	
	Administrative State	Enabled
	Operational State	Up
	Availability	Normal
	Port Mode	OCh(OTU4)
		OTU4 OCh(OTU4)

Figure 3-4 Enable OTU4/OCh (OTU4) Port

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

Port Management				x
≡ BasicInfo	ODU2 * OTU2 BasicInfo *			
■ Port Configuration >	Tool			∧ <i>Q</i>
== 0102 == 0DU2	Administrative State	Enabled	Degrade Interval	2
	Operational State	Up	Degrade Threshold	12304
	Availability State	Normal	Near End ALS	No
	Loopback	NONE	FEC Туре	G709FEC V
	TIM Mode	NONE	Expected SAPI	
	TIM AIS Insertion	False •	Expected DAPI	
	Rx SAPI		Tx SAPI	
	Rx DAPI	'E:ý'ܜޥeóÓ1	Tx DAPI	
	Rx Operator	⊥\¢øV8òd¤Bmg}SŒþŒþ	Tx Operator	
				DCN Apply Close



Port Management				x
■ BasicInfo	OTU2e ODU2 * OTU2 * Ba	asicInfo *		
■ Port Configuration >	Tool			∧ <i>©</i>
OTU2e	Administrative State	Enabled	FEC Type	G709FEC V
	Operational State	Up	Loopback	NONE
	Availability State	Normal	Near End ALS	No
	Degrade Interval	2	Degrade Threshold	12748
	TIM Mode	NONE	Expected SAPI	
	TIM AIS Insertion	False v	Expected DAPI	
	Rx SAPI		Tx SAPI	
	Rx DAPI	' E:ý'ܜޥeóÓ1	Tx DAPI	
	Rx Operator	⊥\¢øV8òd¤Bmg}Sœþœþ	Tx Operator	
				DCN Apply Close



Port Management				
■BasicInfo	OTU4 BasicInfo *			
■ Port Configuration >	Tool			∧ 2
■ 0104 ■ 0DU4	Administrative State	Enabled •	FEC Type	G709FEC T
	Operational State	Up	Loopback	NONE
	Availability State	Normal	Near End ALS	No
	Degrade Interval	2	Degrade Threshold	128459
	TIM Mode	NONE	Expected SAPI	
	TIM AIS Insertion	False v	Expected DAPI	
	Rx SAPI		Tx SAPI	
	Rx DAPI		Tx DAPI	
	Rx Operator		Tx Operator	
				DCN Apply Close

Figure 3-7 Preparation before Enable GCC Channel of OTU4/ODU4

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

Port Management							×
BasicInfo Reat Configuration	DCN OTU2 * Bas	icInfo *					2
TU2	GCC Type	Disabled	•	lfindex	0		
CDU2	PPP Status	Disabled GCC0					
						Apply	Close

Figure 3-8 Open GCC Channel of OUT Layer

ODU4DCN	ODU4 * BasicInfo *		
GCC Type	Disabled	▼ Ifindex	0
PPP Status	Disabled GCC1		
	GCC2 GCC1+2		Apply Close
	ODU4DCN GCC Type PPP Status	ODU4DCN ODU4 * BasicInfo * GCC Type Disabled PPP Status Disabled GCC1 GCC2 GCC1+2	ODU4DCN ODU4 * BasicInfo * GCC Type Disabled Ifindex PPP Status GCC1 GCC2 GCC1+2 GCC1

Figure 3-9 Open GCC Channel of ODU Layer

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

Step 2:

Configure the node IP of the gateway NE and enable OSPF function: Select a NE as the gateway NE. After selecting the NE, click on *"System Management"* and select *"Manage IP Configuration"* to enter *"IP Configuration"* interface.



Figure 3-10 Select NE and Manage IP Configuration

MGMT IP Configuration

Area	Global View>tes	st	NE	OTN(10.32.130.116)			
Node IP		192.168.13	30.116				
NMS IP1							
IP Address		10.32.130	.116				
Subnet Mask		255.255.2	55.0				
OSPF		Enable					
LCT IP							
IP Address		192.168.1	26.1				
Subnet Mask		255.255.2	55.252				
Gateway		10.32.130	.254				
Default route r	e-	Disable		•			
				Apply Close			

Figure 3-11 Open Manage IP Configuration Interface

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



MGMT IP Cor	nfiguration						
Area	Global View>te	w>test NE			OTN(10.32	2.130.116)	
Node IP		192.168.13	30.116				
NMS IP1							
IP Address		10.32.130	.116				
Subnet Mask	Subnet Mask						
OSPF		Enable				•	
LCT IP				-			
IP Address		192.168.1	26.1				
Subnet Mask		255.255.2	55.252				
Gateway		10.32.130.254					
Default route r	e-	Disable					•
						Apply	Close

Figure 3-12 Configure Gateway NE IP

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



GMT IP Conf	iguration				
Area	Global View>te	st	NE	OTN(10.32.130.116)	
Node IP		192.168.13	30.116		
NMS IP1		Can not be in	the same network	segment with the gateway NE	
IP Address		10.32.130	.116		
Subnet Mask		255.255.2	55.0		
OSPF		Enable			•
LCT IP					
IP Address		192.168.1	26.1		
Subnet Mask		255.255.2	55.252		
Gateway		10.32.130	.254		
Default route re- distribution	-	Disable			·
				Apply Clo	se

Figure 3-13 Configure Remote NE IP

Step 3:

Configure the route on the computer to run CMD as an administrator and enter following two routes: route add 192.168.155.111 mask 255.255.255.255.255.192.168.21.111 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 3-14 Add Local Route

Check the input route through route print command.
IPv4				
0 0 0 0	0 0 0 0	102 162 20 1		
0. 0. 0. 0	0. 0. 0. 0	192. 10/1. 105. 1	192. 168. 66. 65	121
127.0.0.0	255.0.0.0		127. 0. 0. 1	331
127.0.0.1	255.255.255.255		127.0.0.1	331
127. 255. 255. 255	255. 255. 255. 255		127.0.0.1	331
192.168.0.0	255.255.0.0	192.168.66.1	192.168.66.65 121	
192. 168. 30. 0	255.255.254.0		192. 168. 30. 243	311
192. 168. 30. 243	255.255.255.255		192. 168. 30. 243	311
192. 168. 31. 255	255.255.255.255		192.168.30.243	311
192.168.66.0	255.255.255.0		192.168.66.65	376
192.168.66.65	255.255.255.255		192. 168. 66. 65	376
192 168 66 255	255 255 255 255	· · · · · · · · · · · · · · · · · · ·	192 168 66 65	376
192.168.155.111	255. 255. 255. 255	192. 168. 21. 111	192.168.66.65 121	
192.168.155.112	255.255.255.255	192. 168. 21. 111	192.168.66.65 121	
224.0.0.0	240.0.0.0		127. 0. 0. 1	331
224.0.0.0	240.0.0.0		192. 168. 66. 65	376
224.0.0.0	240.0.0.0		192. 168. 30. 243	311
255. 255. 255. 255	255.255.255.255		127. 0. 0. 1	331
255. 255. 255. 255	255. 255. 255. 255		192. 168. 66. 65	376
255. 255. 255. 255	255. 255. 255. 255		192. 168. 30. 243	311

Figure 3-15 View Local Route

Use optical fiber to connect occupied ports: Use optical fiber to connect the occupied ports of the two network elements, and to form fiberoptic 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:



MGMT IP Configuration

Area Global V	liew NE	Down(10.32.130.116)
Node IP	192.168.130.116	
NMS IP1		
IP Address	10.32.130.116	
Subnet Mask	255.255.255.0	
OSPF	Enable	¥
LCT IP		
IP Address	192.168.126.1	
Subnet Mask	255.255.255.252	
Gateway	10.32.130.254	
Default route re- distribution	Enable	*

Figure 3-16 Enable Default Route Redistribution Function of the Gateway NE

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



MGMT IP Configuration

Area Global V	iew	Down(10.32.130.116)				
Node IP	192.168.130.116					
NMS IP1						
IP Address	10.32.130.116					
Subnet Mask	255.255.255.0	255.255.255.0				
OSPF	Enable	Enable				
LCT IP						
IP Address	192.168.126.1					
Subnet Mask	255.255.255.252	255.255.255.252				
Gateway	0.0.0.0					
Default route re- distribution	Enable					
		Apply Close				



Add Configuration 3:

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

Attention

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

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

4. NE & Module 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 FMX NMS interface is displayed after successful login.

4.1. Shelf Information

Select NE and right click on "Shelf 01", then select "Shelf Inventory" to open the chassis information interface. Information such as chassis type and temperature is displayed in this interface, as shown in Figure 4-1:

•	Home System Management	Configuration Management	Fault Management	Performance Management	Security Management	Log Management	OLP Route					
							≽16	011	02	3	<u>@</u> 0	root
🖻 🚯 Global View		¢ Q Q	⇔ # 0 ₿	E Find						System Time	: 2019-12-2	0 15:36:08
CTN(10.3	32.130.116)											
Shel	If Inventory operational											
Carc	d Inventory erational											
Slot Traff	t Info Mic Configuration pperational											
Slot	6 Empty : available 7 FMX-100G-2UPSM : operational											
 Slots 	8 Empty : available			and the second	and the second s		and an an an					

Figure 4-1 Operation Steps to View Shelf Inventory

4.1.1. FMX-100G-CH2U

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

Shelf Inventory				
01.157				
Shelt Type	OTN_2U_AC	PN	20.010.5175	
HW Version	2.0	SN	2022B00SN1807016	
MacAddress	60:E6:BC:02:19:B8	Assigned ShelfId	1	
Location		Temperature(°C)	31	
Fan Speed PWM	80%	Auto Regulate Speed	True	v
Fan Top Speed	False			
			Lam	Apply Close



4.2. LED Indicator Information

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

4.2.1. NMU Module

Indicator	FMX-100G-CH2U



NMU Module Control System LED Indicator (NMU Module, Business Module Integration)	RUN	Green Light Slow Flash: The software is successfully started, and it is Active module. Green Light On: The software is successfully started, but it is Standby module. Green Light Off: The software is not started.
	FAULT/ALM	Red Light Quick Blink: The module is mismatched. Red Light Slow Flash: There is latch open alarm. Red Light On: There is alarm. Red Light Off: There is no alarm.

Table 4-1 LED Indicator Status of Integrated NMU Module

	Indicator	FMX-100G-CH2U
System Module Optical Management Port (MGMT) LED Indicator	Monochromatic Green Light	Off: The port is disabled/There is los alarm. Green Light On: There is no los alarm and the port is enabled.

Table 4-2 LED Indicator Status of System Module Optical Management Port

4.2.2. System Interface LED Indicator

	Indicator	FMX-100G-CH2U
System Interface LED Indicator	SYS	On SIE Module: Green Light On: The system is successfully started. Green Light Off: The system is not started.
	CR/MJ/MN	On SIE Module: CR: Red Light On: There is Critical alarm. MJ: Orange Light On: There is Major alarm. MN: Yellow Light On: There is Minor alarm.

Table 4-3 System Interface LED Indicator Status

4.2.3. Business Module LED Indicator

	Indicator	FMX-100G-CH2U
Business Module LED Indicator	RUN	Green Light Slow Flash: The software is successfully started and it is active module. Green Light On: The software is successfully started but it is standby module. Green Light Off: The software is not started.
	FAULT/ALM	Red Light Quick Blink: The module is mismatched. Red Light Slow Flash: There is latch open alarm. Red Light On: There is alarm. Red Light Off: There is no alarm.

Table 4-4 Business Module LED Indicator Status

4.2.4. Fan Tray LED Indicator

Indicator FMX-100G-CH20

Fan Tray LED Indicator	RUN (Monochrome)	NA
	FAULT/ALM (Monochrome)	NA
	FAN (Two Colors)	Red Light On: There is alarm of the fan. Green Light On: There is no alarm of the fan.

Table 4-5 Fan Tray LED Indicator Status

4.2.5. Port LED Indicator of Business Module

	Indicator	FMX-100G-CH2U
Business Module Port LED Indicator	Bi-Color LED Indicator	Off: The port is disabled. Red Light Quick Blink: There is mismatch alarm of the port. Red Light On: There is los alarm of the port. Green Light On: There is no los or mismatch alarm.

Table 4-6 Port LED Indicator Status of Business Module

4.2.6. Power Tray LED Indicator

	Indicator	FMX-100G-CH2U
Power Tray LED Indicator	PWR (Monochrome)	Off: The power tray is not powered. Green Light On: Normal power supply.
	FAULT (Monochrome)	Off: There is not any alarm of the power tray. Red Light On: There is alarm that the power supply is not powered on or there is power failure.
	PWR1 (Monochrome)	NA
	PWR2 (Monochrome)	NA

Table 4-7 Power Tray LED Indicator Status

4.3. View Single Module Information

Select NE and right click on "Shelf 01", and then select "Card Inventory".

Home System Management	Configuration Managemen	nt Fault Management Performance Management	Security Management Log Management	OLP Route			
				≽ 16 €	11 📀2	03	@0 root
Global View Global Vi	\$ Q Q	↔ 4 O 13 4 Find				System Time	2018-12-20 15-44-48

Figure 4-3 View Single Module Information

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

Card Inventory										
Show 10	Show 10 • entries Search. Search.									
Slot ID	Туре ↓↑	SN ↓†	PN ↓↑	HW Version $\downarrow\uparrow$	SW Version 1	Sw Version in Load $\downarrow\uparrow$	FPGA ID 🗍	FPGA Version $\downarrow\uparrow$	FPGA Version status $\downarrow\uparrow$	Fpga Load Version \downarrow
1	FMX-100G-MXP10	272AHB0RS19010009	20.010.5121	2.7	R6.3.23_v6704_release		9	18121000	0	18121000
2	FMX-100G-MXP10	272AHB0RS19010010	20.010.5121	2.7	R6.3.23_v6704_release		9	18121000	0	18121000
3	FMX-100G-NMU	2022100RS19030007	20.010.5177	2.0	N/A	N/A	N/A		0	N/A
4	Empty									
5	FMX-100G-2UPSM	1022P01YD19020069	20.010.5174	1.0	N/A	N/A	N/A		0	N/A
6	Empty									
7	FMX-100G-2UPSM	1022P01YD19020050	20.010.5174	1.0	N/A	N/A	N/A		0	N/A
8	Empty									
9	Empty									
10	FMX-FAN	1222F00YD19020051	20.010.5172	1.2	N/A	N/A	N/A		0	N/A
Showing 1 to 10 of 10 entries 1 Next										
										Close

Figure 4-4 Module Information Interface

4.4. Port Configuration

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



Figure 4-5 View Port Configuration Information

4.4.1. Basic Information

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

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

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

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



Port Management		X
■BasicInfo ■Port Configuration	BasicInfo Tool	
	Administrative State	Enabled
	Operational State	Up
	Availability	Normal
	Port Mode	XGE_BMP T
		Apply Close

Figure 4-6 Port Management Interface

4.4.1.1. Interface Configuration

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

Port Management							×
■BasicInfo	Interface	BasicInfo 3	¢				
■ Port Configuration >	Tool						∧ <i>©</i>
Interface							
DDU2e	Administrati	ve State	Enabled	Ŧ	Operational State	Up	
	Availability S	tate	Normal	v	LoopBack	NONE	¥
	Near End Al	S	No	Ŧ	Client Shutdown	No	Ŧ
					(CSD) by Alarm		
							Apply Close



4.4.1.2. ODU2/ODU2e Configuration

ODU2 Configuration

Select NE-Slot 2, right click on "Port 1" and select "Port Management", the port management interface pops up (here we take ODU2 corresponding to XGE_GFPF port mode as an example). Click on ODU2 option from "Port Configuration" in this interface, as shown in the figure below. It shows ODU2 toolbar interface.

Port Management						x
■ BasicInfo ■ Port Configuration Interface ■ ODU2	ODU2 BasicInfo Tool	×				~
	Show 10 v entries			Search:	Search	
	ODU2 It	Administrative State	Operational State		Operation	
	0	Enabled	Up		Management	
	Showing 1 to 1 of 1 entrie	25		P	Previous 1	Next

Figure 4-8 ODU2 Toolbar Interface

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

Port Management				X
■ BasicInfo Port Configuration >	ODU2 BasicInfo *			^
Interface	Administrative State	Enabled	OPU State	Client
	Availability State	NotConnected	Tx PT	0x5
	PLM AIS Insertion Degrade Interval	True v	Expected PT Degrade Threshold	0x5 12304
	TIM Mode	NONE	Expected SAPI	
	Rx SAPI	YYYYYYYYYYY	Tx SAPI	
	Rx DAPI Rx Operator	<i>ууууууууууууу</i> az âèX <i>f</i> -¶p¦«[c[/)®/⊢nM″E"< r	Tx DAPI Tx Operator	
	Show 10 ventries			Apply Close
	ODU2 It	Administrative State	Operational State	↓↑ Operation ↓↑
	0 Showing 1 to 1 of 1 entries	Enabled	Up	Management Previous 1 Next

Figure 4-9 ODU2 Toolbar Management Interface

• ODU2e Configuration

Select NE-Slot 2, right click on "Port 1" and select "Port Management", the port management interface pops up (here we take ODU2e corresponding to XGE_BMP port mode as an example). Click on ODU2e option from "Port Configuration" in this interface, as shown in the figure below. It shows ODU2e toolbar interface.

Port Management						x
BasicInfo Port Configuration	ODU2e BasicInfo *					~
Interface ODU2e	Show 10 • entries			Search:	Search	
	ODU2e 🎝	Administrative State	Operational State		Operation	
	0	Enabled	Up		Management	
	Showing 1 to 1 of 1 entries			Pre	evious 1	Next

Figure 4-10 ODU2e Toolbar Interface

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

Port Management				×				
■BasicInfo	ODU2e BasicInfo *							
■ Port Configuration >	Tool			^				
Interface	Administrative State	Enabled	OPU State	Client				
	Operational State	Up	Rx PT	0xf6				
	Availability State	NotConnected	Tx PT	0x3				
	PLM AIS Insertion	True	Expected PT	0x3				
	Degrade Interval	2	Degrade Threshold	12748				
	TIM Mode	NONE	Expected SAPI					
	Trace Identifier Mismatch(TIM) AIS Insertion	False	Expected DAPI					
	Rx SAPI	<u> </u>	Tx SAPI					
	Rx DAPI	<u> </u>	Tx DAPI					
	Rx Operator	<u> </u>	Tx Operator					
	Apply Close							
	Show 10 ventries			Search: Search				
	ODU2e ↓↑	Administrative State	Operational State	It Operation It				
	0	Enabled	Up	Management				
	Showing 1 to 1 of 1 entries			Previous 1 Next				

Figure 4-11 ODU2e Toolbar Management Interface

4.4.1.3. OTU2/OTU2e Configuration

OTU2 Configuration

Select NE-Slot 2, right click on "Port 1" and select "Port Management" (here we take OTU2 corresponding to OTU2 port mode as an example), the port management interface pops up. Click on OTU2 option from "Port Configuration" in this interface, as shown in the figure below. It shows OTU2 toolbar interface.

Port Management					×
■ BasicInfo Port Configuration	ODU2 * OTU2 BasicInfo *			^	. 2
 OTU2 ODU2 	Administrative State	Enabled	Degrade Interval	2	
	Operational State Availability State	Up Normal v	Degrade Threshold Near End ALS	12304 No	•
	Loopback	NONE	FEC Type	G709FEC	•
	TIM Mode TIM AIS Insertion	NONE T	Expected SAPI Expected DAPI		
	Rx SAPI		Tx SAPI		
	Rx DAPI Rx Operator	'E:ý'ۜޥe6Ó1 ⊥\¢øV8òd¤Bmq}Sœþœþ	Tx DAPI Tx Operator		
			·	DCN Apply	Close

Figure 4-12 OTU2 Toolbar Interface

• OTU2e Configuration

Select NE-Slot 2, right click on "Port 1" and select "Port Management", the port management interface pops up (here we take OTU2e corresponding to OTU2e port mode as an example). Click on OTU2e option from "Port Configuration" in this interface, as shown in the figure below. It shows OTU2e toolbar interface.

Port Management				×
■ BasicInfo ■ Port Configuration >	OTU2e BasicInfo * Tool			^ <i>C</i>
DU2e	Administrative State	Enabled •	FEC Type	G709FEC V
	Availability State	Normal V	Near End ALS	No V
	Degrade Interval	2 NONE	Degrade Threshold Expected SAPI	12748
	TIM AIS Insertion	False 🔻	Expected DAPI	
	Rx DAPI	' E:ý'ܜޥeóÓ1	Tx SAPI Tx DAPI	
	Rx Operator	⊥\¢øV8òd¤Bmg}SŒþŒþ	Tx Operator	
				DCN Apply Close

Figure 4-13 OTU2e Toolbar Interface

4.4.1.4. ODU4 Configuration

Select NE-Slot 4, right click on "Port 1" and select "Port Management", the port management interface pops up (here we take ODU4 corresponding to HGE_GMP port mode as an example). Click on ODU4 option from "Port Configuration" in this interface, as shown in the figure below. It shows ODU4 toolbar interface.

Port Management				x
■BasicInfo ■Port Configuration >	ODU4 BasicInfo * Tool			^ <i>C</i>
 Interface ODU4 	Administrative State	Enabled	Opu State	Client
	Operational State	Up	Degrade Interval	2
	Availability State	Normal	Degrade Threshold	128459
	PLM AIS Insertion	True	Expected PT	0x7
	Rx PT	0×ff	Tx PT	0x7
	TIM Mode	NONE	Expected SAPI	
	TIM AIS Insertion	False •	Expected DAPI	
	Rx SAPI		Tx SAPI	
	Rx DAPI		Tx DAPI	
	Rx Operator		Tx Operator	
				Apply Close

Figure 4-14 ODU4 Toolbar Interface

4.4.1.5. OTU4 Configuration

Select NE-Slot 4, right click on "*Port 3*" 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.

Port Management					x
■ BasicInfo ■ Port Configuration >	OTU4 BasicInfo * Tool			^	C
TU4	Administrative State	Enabled •	FEC Туре	SDFEC3	•
DDU4	Operational State	Up	Loopback	NONE	۳
	Availability State	Normal			
	Degrade Interval	2	Degrade Threshold	128459	
	TIM Mode	NONE	Expected SAPI		
	TIM AIS Insertion	False •	Expected DAPI		
	Rx SAPI		Tx SAPI		
	Rx DAPI		Tx DAPI		
	Rx Operator		Tx Operator		
				DCN Apply CI	lose

Figure 4-15 OTU4 Toolbar Interface

4.4.2. Parameter Description

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





module	Interface	Description
FMX-100G- MXP10	1*100G line side interface (CFP) 10 * 10G client side interface (SFP+)	 The client side signal (10GE, STM-64/OC-192) is mapped to ODU2/2e. The line side signal is demultiplexed from ODU4 to ODU2/2e and connected to the client side signal. 100G line side supports G.709 general FEC or Soft-Decision FEC. 10G OTU2/2e supports I.4 and I.7 EFEC, or G.709 general FEC Support GCC0, GCC1 and GCC2 in-band management Support SNC/I and SNC/N transmission protection
FMX-100G- TMXP2	1*100G line side interface (CFP) 1*100G (QSFP28) or 2*40G client side interface (QSFP+)	The client side 100G signal (100GE or OTU4) is mapped to ODU4. The client side 40G signal (40GE or OTU3) is mapped to ODU3. The line side signal is terminated to ODU4 or ODU3, and is connected to the client side signal. 100G line side supports G.709 general FEC or Soft-Decision FEC Support GCC0, GCC1 and GCC2 in-band management Support SNC/I and SNC/N transmission protection

Table 4-8 Parameter Description of OTN Module

4.5. Configuration of Optical Module Information

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

Select NE-Slot, right click on "Port" and select "Optical Module Configuration", as shown in the figure below:



Figure 4-18 View Optical Module Information

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

4.5.1. SFP/SFP+ Optical Transceiver Information

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

Pluggable			×
Pluggable BasicInfo	Optics Paramete		
Туре	SFP/SFP+	Present or Absent	Work
Vendor SN	B19030415	Vendor PN	10.600.6070
Vendor Name	OEM	Vendor OUI	00-0B-40
Application Code	Ethernet 10GBASE_LR	CLEI	
LaneNum	1	Firmware	
Tunable	False	Wavelength(nm)	1310
			Apply Close

Figure 4-19 Basic Information of SFP/SFP+ Optical Transceiver

Optics Paramete				
}			Search:	Search
ane TxPower(dBm)	Lane RxPower(dBm)	Laser Temperature(°C)	Laser Bias(mA)	Laser Vcc(mV)
)	-2.20	36.0	27	3.23
es			1	Previous 1 Next
	Optics Paramete	Optics Paramete ane TxPower(dBm) t Lane RxPower(dBm) t -2.20	Optics Paramete ane TxPower(dBm) 1 Lane RxPower(dBm) 1 -2.20 36.0	Image: Depict s Paramete Search: Search:

Figure 4-20 Parameter Information of SFP/SFP+ Optical Transceiver

4.5.2. CFP Optical Transceiver Information

Pluggable			×
Pluggable BasicInfo	Optics Paramete		
Туре	CFP	Present or Absent	Alarm
Vendor SN	CPC003C	Vendor PN	FTLC1182SDNL
Vendor Name	FINISAR CORP.	Vendor OUI	00-90-65
Application Code	A4I1_9D1F	CLEI	20 20 20 20 20 20 20 20 20 20 20 0e 0e 02 01 03 03
LaneNum	4	Firmware	
			Apply Close

Figure 4-21 Parameter Information of CFP Optical Transceiver

Pluggable Pluggable Basic	Info Optics Paramete				
Show 10	ontries			Search	Soarch
Lane ID	Lane TxPower(dBm)	Lane RxPower(dBm)	Laser Temperature(°C)	Laser Bias(mA)	Laser Vcc(mV)
1	0.20	-22.90	37.0	43	3.22
2	0.50	-22.60	37.0	61	3.22
3	0.80	-22.20	37.0	59	3.22
4	0.70	-23.90	37.0	55	3.22
Showing 1 to 4 o	f 4 entries			l	Previous 1 Next
					Close

Figure 4-22 Parameter Information of CFP Optical Transceiver

4.5.3. WDM CFP Optical Transceiver Configuration

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

Port Management				
BasicInfo Port Configuration	Interface BasicInfo Tool	ĸ		^ C
TU4	Administrative State	Enabled •	Operational State	Up
COU2e	Near End ALS TxPower(set value) DGD(ps) CD(ps/nm)	195.057142-1537.003nm-H50 195.057142-1537.003nm-H50 195.107Hz-1536.609nm-C51 195.207Hz-1536.216nm-H51 195.207Hz-1536.22nm-C52 195.257Hz-1535.429nm-H52 195.307Hz-1535.036nm-C53 195.307Hz-1534.4280nm-H53 195.407Hz-1534.4280nm-K53 195.407Hz-1534.4280 195.407Hz-1544.4280 195.407Hz-1544.4280 195	Availability State TxPower(current value) OSNR(db/0.1nm)	Normal V -4.9dBm 25.5
 Slot3 OTH_STE : operational Slot4 Empty : available Slot5 PWR_AC : operational Slot6 Empty : available Slot7 PWR_AC : operational Slot8 Empty : available Slot8 Empty : available Slot0 OTN_FAN_2U : operational 		135.50THz-1533.465mm-C55 195.50THz-1533.465mm-C55 195.60THz-1533.073mm-H55 195.60THz-1532.681mm-C56 195.70THz-1531.898nm-C57 195.70THz-1531.1697mm-H57 195.80THz-1531.161mm-C58 195.85THz-1530.725nm-H58 195.90THz-1529.944mm-H59 195.90THz-1529.944mm-H59 195.90THz-1529.944mm-H59 195.00THz-1529.953mm-C60		Apply Close

Figure 4-23 Configure Operating Wavelength of WDM CFP

Port Management					
■ BasicInfo	Interface BasicInfo 3	د			
■ Port Configuration >	Tool				× 0
Interface OTU4	Administrative State	Enabled	Ŧ	Operational State	Up
CDU4	Frequency(set value)	196.00THz-1529.553nm-C60	٣	Frequency(current value)	196.00THz-1529.553nm-C60
	Near End ALS	No	٣	Availability State	Normal
	TxPower(set value)	-5.0dBm	•	TxPower(current value)	-4.9dBm
	DGD(ps)	-14.00Bm -13.5dBm -13.0dBm	Î	OSNR(db/0.1nm)	25.5
	CD(psmin)	-12.5dBm -12.0dBm -11.6dBm			Apply Close
 Slot5 OfM_SIE : operational Slot5 Empty : available Slot5 Empty : available Slot6 Empty : available Slot8 Empty : available Slot8 Empty : available Slot0 OTM_FAN_2U : operational 114(192.168.21.114) Shelf01 * Slot1 M2X16_1U 		- 11.30B/ll -10.5dBm -10.5dBm -9.5dBm -9.5dBm -8.5dBm -8.5dBm -7.5dBm -7.5dBm -6.5dBm -5.5dBm -5.5dBm -5.5dBm	Ţ	8.	

Figure 4-24 Configure Transmitting Optical Power of WDM CFP

Port Management						Х
■ BasicInfo	Interface BasicInfo *	t				
■ Port Configuration >	Tool					∧ <i>C</i>
Interface						
TU4	Administrative State	Enabled	Operation	al State	Up	
BB ODU4	Frequency(set value)	196.00THz-1529.553nm-C60	 Frequency 	(current	196.00THz-1529.553nm-C60	
DU2e			value)			
	Near End ALS	No	 Availability 	/ State	Normal	*
	TxPower(set value)	-5.0dBm	 TxPower(events) value) 	current	-4.9dBm	
	DGD(ps)	6	OSNR(db/	/0.1nm)	25.5	
	CD(ps/nm)	748				
						Apply Close

Figure 4-25 Parameter Reading of WDM CFP Optical Transceiver

Pluggable			×
Pluggable BasicInfo	Optics Paramete		
Туре	CFP	Present or Absent	Alarm
Vendor SN	161931552	Vendor PN	AC100-M01-210
Vendor Name	Acacia Comm Inc.	Vendor OUI	00-00-00
Application Code	Application_Unknown	CLEI	
LaneNum	1	Firmware	01.06.10
			Apply Close

Figure 4-26 Basic Information of WDM CFP Optical Transceiver

Pluggable					
Pluggable BasicInt	fo Optics Paramete				
Show 10 v e	ntries			Search:	Search
Lane ID	Lane TxPower(dBm)	Lane RxPower(dBm)	Laser Temperature(°C)	Laser Bias(mA)	Laser Vcc(mV)
1	-5.00	-40.00	48.0	20	3.17
Showing 1 to 1 of 1	entries			1	Previous 1 Next
					Close

Figure 4-27 Parameter of WDM CFP Optical Transceiver

5. Service Configuration

Prerequisite

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

5.1. Electric Cross-Connect Introduction

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

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

Configuration Steps

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

• 🥩	Home System Management	Configuration Management	Fault Management	Performance Management	Security Management	Log Management	OLP Route						
								> 16	011	() 2	<mark>()</mark> 3	0	root
Global View		\$ Q Q	⇔ & O ≞	Find Find							System Time :	2019-12-3	20 15:51:11
B CTN(10	.32.130.116)												
🖯 🛥 SI	Shelf Inventory SC1+1 Management												
	Card Inventory												
	Traffic Configuration												
	Port6												
•	Port7				and the second		a dipe	1. 19					

Figure 5-1 Operation Steps of Traffic Configuration

The "Service Configuration-SNC Configuration" interface pops up, as shown in the figure below:

Traffic Configuration										x
■ SNC Configuration ■ OCH1+1 Configuration		SNC Configuration Show 10 • entries Search: Search								
		ID ↓↑	Snc Type 1	Circuit ID 1	Src TpID	Des TpID 🛛 🗍	SrcProt TpID 1	DesProt TpID 1	Opera	tion ↓↑
		1	2WAY		Slot1-port1-ODU2e(0)	Slot1-port11-ODU2e(1)			Delete	Protect
		2	2WAY		Slot2-port1-ODU2e(0)	Slot2-port11-ODU2e(1)			Delete	Protect
	g 1 to 2 d	of 2 entries					Previo	us 1	Next	
								Del	ete Add	Close

Figure 5-2 Traffic Configuration Interface

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



Figure 5-3 Protection Schematic Diagram

5.1.1. Unidirectional Cross-Connection without Protection

Select NE, right click on "Chassis" and select "Add" button in "SNC Configuration" of "Traffic Configuration" interface; you can create unidirectional cross-connection without protection (here we take FMX-100G-MXP10 port 1-port 11 cross-connection as an example to select the corresponding slot, cross-connection type and capacity information).

Traffic Configuration					
SNC Configuration	Add SNC Configurat	tion ×			
■ OCH1+1 Configuration	Tool				^
	Label		Туре	1WAY	•
	Capacity	ODU2e			
	А				
	Shelf	1	Slot	1	•
	Port	1	ТР	ODU2e(0)	٣
	Z				
	Shelf	1	Slot	1	٣
	Port	11	TP	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	•
				Add	Close

Figure 5-4 Configuration of Unidirectional Cross-Connection without Protection

Traffic Configuration		÷							×
■ SNC Configuration ■ OCH1+1 Configuration	SNC Show	Configu	ration					Search: Se	arch
	0 11	ID J†	Snc Type 1	Circuit ID ↓↑	Src TpID	Des TpID	SrcProt TpID	DesProt TpID ↓↑	Operation 1
	Showing 1 to 1 of 1 entries Previous Nex Nex Nex Nex Nex Nex Nex Ne								bus 1 Next
								De	lete Add Close

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

5.1.2. Bidirectional Cross-Connection without Protection

Select NE, right click on "Chassis" and select "Add" button in "SNC Configuration" of "Service Configuration" interface; you can create bidirectional cross-connection without protection (here we take FMX-100G-MXP10 port 1-port 11 cross-connection as an example to select the corresponding slot, cross-connection type and capacity information).

r						
Traffic Configuration						
SNC Configuration	Add SNC Configurat	ion *				
■ OCH1+1 Configuration	Tool				^	
	Label		Туре	2WAY	•	•]
	Capacity	ODU2e 🔻				
	A					
	Shelf	1	Slot	1		•
	Port	1	ТР	ODU2e(0)	*	•
	Z					
	Shelf	1	Slot	1	*	•]
	Port	11 •	ТР	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	•	-
				A	dd Clos	e

Figure 5-6 Configuration of Bidirectional Cross-Connection without Protection

Traffic Configuration										×
SNC Configuration	Add * SNC Configuration									
	Show	10 •	entries					Search: Sea	arch	
	0 II	ID 11	Snc Type ↓↑	Circuit ID ↓↑	Src TpID 1	Des TpID ↓↑	SrcProt TpID	DesProt TpID ↓↑	Opera	tion ↓↑
		1	2WAY		Slot1-port1-ODU2e(0)	Slot1-port11-ODU2e(1)			Delete	Protect
	Showing	g 1 to 1 o	of 1 entries					Previo	us 1	Next
								Del	Add	Close

Figure 5-7 Configuration Result of Bidirectional Cross-Connection without Protection

5.1.3. Unidirectional Cross-Connection with Protection

Select NE, right click on "*Chassis*" and select "*Add*" button in "*SNC Configuration*" of "*Service Configuration*" interface; you can create unidirectional cross-connection with protection (here we take FMX-100G-MXP10 as an example, the 11 ports from Port 1-Port 11 of one module create unidirectional cross-connection with protection, and the 11 ports of the other module act as the protection to select the corresponding slot, cross-connection type and capacity information).

Traffic Configuration					×
SNC Configuration	Add SNC Configura	tion *			
CCH1+1 Configuration	Tool				^
	Label		Туре	1WAYPR	Ŧ
	Capacity	ODU2e	•		
	A				
	Shelf	1	Slot	1	•
	Port	1	TP	ODU2e(0)	•
	Z				
	Shelf	1	Slot	1	•
	Port	11	r TP	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	•
	A Protection				
	Shelf	1	/ Slot	1	٣
	Port	1	TP TP		Ŧ
	Z Protection				
	Shelf	1	Slot	2	•
	Port	11	TP	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	•
		L		Add	Close
	L				

Figure 5-8 Configuration of Unidirectional Cross-Connection with Protection



Traffic Configuration		÷						· ·	×
■ SNC Configuration ■ OCH1+1 Configuration	Add ¹ Show	* SNC	C Configuration					Search: Search	
	0.11	ID ↓†	Snc Type ↓↑	Circuit ID ↓↑	Src TpID ↓↑	Des TpID 🛛 🕹 🕇	SrcProt TpID 1	DesProt TpID	Oţ
	Showing	1 g 1 to 1 c	1WAYPR of 1 entries		Slot1-port1-ODU2e(0)	Slot1-port11-ODU2e(1)		Slot2-port11-ODU2e(1) Previous	Delete Unp
								Delete	Add Close

Figure 5-9 Configuration Result of Unidirectional Cross-Connection with Protection

5.1.4. Bidirectional Cross-Connection with Protection

Select NE, right click on "Chassis" and select "Add" button in "SNC Configuration" of "Service Configuration" interface; you can create bidirectional cross-connection with protection (here we take FMX-100G-MXP10 as an example, the 11 ports from Port 1-Port 11 of one module create bidirectional cross-connection with protection, and the 11 ports of the other module act as the protection to select the corresponding slot, cross-connection type and capacity information).

Traffic Configuration					
SNC Configuration	Add SNC Configurat	tion *			
■ OCH1+1 Configuration	Tool				^
	Label		Туре	2WAYPR	T
	Capacity	ODU2e v			
	A				
	Shelf	1	Slot	1	•
	Port	1	ТР	ODU2e(0)	•
	Z				
	Shelf	1	Slot	1	•
	Port	11	TP	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	•
	A Protection				
	Shelf	1	Slot	1	Ŧ
	Port	1	TP		
	Z Protection				
	Shelf	1	Slot	2	•
	Port	11	ТР	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	•
		L	5		Add Close
	U.				

Figure 5-10 Configuration of Bidirectional Cross-Connection with Protection

Traffic Configuration										
SNC Configuration		Add × SNC Configuration								
	Show		Snc Type	Circuit ID	Src ToID	Des TolD	SrcProt ToID	DesProt ToID		Or
		1	2WAYPR	Gircuit ID 4	Slot1-port1-ODU2e(0)	Slot1-port11-ODU2e(1)	Sici lot tpib +	Slot2-port11-ODU2e(1)	Delete	Unp
	Showing	g 1 to 1 c	of 1 entries					Previous	1	Next
								Delete	Add	Close

Figure 5-11 Configuration Result of Bidirectional Cross-Connection with Protection

5.2. Service Type

5.2.1. Service Type

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

ë <u>■</u> OTN(10.3) [©] 🖆 Shelf01 © 😂 Slot1	2.130.116) FMX-100G-MXP10 : opera	itional
📥 F	Port Configuration	
F F	Pluggable Configuration	
- Po	rt4	I
- 📥 Po	rt5	
- 📥 Po	rt6	
- 📥 Po	rt7	
- 📥 Po	rt8	
- 📥 Po	rt9	
- 📥 Po	rt10	
- Po	rt11	

Figure 5-12 Operation Steps of How to View Service Type

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

Port Management		ж
BasicInfo Port Configuration →	BasicInfo Tool	
	Administrative State	Enabled
	Operational State	Down
	Availability	Notinstalled
	Port Mode	XGE_BMP v
	Port Description	XGE_GRPF XGE_GFPF XGE_GFPFextp STIME_AMP OC192_AMP
Port9 Port10 Slot2 FMX-100G-MXP10 : operational		OTU2 OTU2e STM64_BMP OC192_BMP



5.2.2. Service Mapping

In FMX NMS, you can select the service mapping mode in the port management-port mode interface. Here we take the FMX-100G-MXP10 module as an example. As shown in the figure below, the left of the underline is port mode and the right is the mapping mode (OTU signal is not included).

STM64_AMP	•
XGE_BMP	
XGE_GFPF	
XGE_GFPFextp	
STM64_AMP	
OC192_AMP	
OTU2	
OTU2e	
STM64_BMP	
OC192_BMP	

Figure 5-14 Mapping Mode Interface

5.2.2.1. AMP

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

Here we take FMX-100G-MXP10 module as an example. Select NE-Slot, right click on "*Port 1*" and select "*Port Management*", and then select M64_AMP mode.

Port Management			×
 ■ BasicInfo ■ Port Configuration 	BasicInfo Tool		
	Administrative State	Enabled	•
	Operational State	Up	
	Availability	Normal	
	Port Mode	STM64_AMP	٣
		Apply	Close



5.2.2.2. BMP

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

Here we take FMX-100G-MXP10 module as an example. Select NE-Slot, right click on "*Port 1*" and select "*Port Management*", and then select XGE_BMP mode.

Port Management				×
■ BasicInfo ■ Port Configuration >	BasicInfo Tool			
	Administrative State	Enabled		•
	Operational State	Up		
	Availability	Normal		
	Port Mode	XGE_BMP		•
		A	Apply	Close

Figure 5-16 XGE_BMP Mapping Mode

5.2.2.3. GMP

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

Here we take FMX 100G modules MXP10 module as an example. Select NE-Slot, right click on "Port 3" and select "Port Management", and then select XGE_BMP mode.

Port Management			x
 BasicInfo Port Configuration 	>	BasicInfo	
		Administrative State	Enabled •
		Operational State	Up
		Availability	Normal
		Port Mode	XGE_BMP v
 Port4 Port5 		Part of the	XGE_BMP XGE_GFPF XGE_GFPFextp STM64_AMP OC192_AMP
Port6 Port7 Port8			OTU2e STM64_BMP OC192_BMP



5.2.2.4. GFP-F

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

Here we take FMX-100G-MXP10 module as an example. Select NE-Slot, right click on "*Port 1*" and select "*Port Management*" and then select XGE_GFPF mode.

Port Management			
	BasicInfo Tool		
	Administrative State	Enabled	
	Operational State	Up	
	Availability	Normal	
	Port Mode	XGE_GFPF	•
		App	ply Close



5.2.2.5. GFP-Fextp

Here we take FMX-100G-MXP10 module as an example. Select NE (192.168.21.72)-Slot 2, right click on "Port 1" and select "Port Management", and then select XGE_GFPFextp mode.

Port Management			
■ BasicInfo ■ Port Configuration >	BasicInfo Tool		
	Administrative State	Enabled]
	Operational State	Up	
	Availability	Normal	
	Port Mode	XGE_GFPFextp •]
		Apply Close	e





Figure 5-20 Service Configuration Process

5.3. Configuration instructions

5.3.1. FMX-100G-MXP10

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

5.3.1.1. Service Type

Line Side Port

Select NE-Slot 2, right click on "Port 11" and select "Port Management", the operation interface is as shown in the figure below:





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

Port Management			
BasicInfo Port Configuration >	BasicInfo Tool		
	Administrative State	Enabled •	·]
	Operational State	Up	
	Availability	Normal	
	Port Mode	OCh(OTU4)	·]
		OTU4 OCh(OTU4)	

Figure 5-22 FMX-100G-MXP10 Line Side Port Interface

Client Side Port

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





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

Port Management		x
BasicInfo	BasicInfo	
Port Configuration	> Tool	
	Administrative State	Enabled
	Operational State	Up
	Availability	Normal
	Port Mode	XGE_BMP v
Port4	Market in the second	XGE_BMP XGE_GFPF XGE_GFPFextp STM64_AMP
 Port5 Port6 Port7 Port8 		OC192_AMP OTU2 OTU2e STM64_BMP OC192_BMP

Figure 5-24 FMX-100G-MXP10 Client Side Port Interface

5.3.1.2. Time Slot Configuration

Select NE and right click on "Slot 2", and then select "TP Multiplexing Structure", as shown in the figure below:



Figure 5-25 Operation Steps of FMX-100G-MXP10-TP Multiplexing Configuration

The interface is as shown in the figure below. Select ODU4 to demultiplex to ODU2/ODU2e.

TP	Multiplexing Structure							x
F	Port	11	•					
Œ	<u>ODU4(0)</u>							
					ODU2	ODU2e	Clear All	Close

Figure 5-26 FMX-100G-MXP10 Demultiplexing Configuration Interface

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

Port ParentName ODU4 TP ID 2 Image: Solution of the second	TP Multiplexing Stru	ODU4 To ODU2e						× ×
* ODU4(0) TS(#1) TS(#2) TS(#3) TS(#4) TS(#5) TS(#6) TS(#7) TS(#8) TS(#9) TS(#10) TS(#11) TS(#12) tear All TS(#13) TS(#14) TS(#15) TS(#16) TS(#17) TS(#18) TS(#13) TS(#14) TS(#15) TS(#16) TS(#17) TS(#18) TS(#19) TS(#20) TS(#21) TS(#22) TS(#23) TS(#24) TS(#25) TS(#26) TS(#27) TS(#28) TS(#29) TS(#30) TS(#31) TS(#32) TS(#33) TS(#34) TS(#35) TS(#36) TS(#31) TS(#38) TS(#39) TS(#40) TS(#41) TS(#42) ort1 TS(#43) TS(#44) TS(#45) TS(#46) TS(#41) TS(#42) ort2 TS(#49) TS(#50) TS(#51) TS(#52) TS(#48) TS(#54) ort3 TS(#61) TS(#62) TS(#63) TS(#64) TS(#59) TS(#60) ort4 TS(#61) TS(#68) TS(#68) TS(#71) TS(#71) TS(#71) TS(#71) TS(#71)	Port	ParentName	ODU4		TP ID	2	v	
art8 ITS(#79) ITS(#80)	DOU4(0) MIALON MIH10 : operatio MIH10 : operatio ort1 ort2 ort3 ort4 ort5 ort6 ort7 ort8	□TS(#1) □TS(#7) □TS(#13) □TS(#19) □TS(#25) □TS(#31) □TS(#37) □TS(#43) □TS(#43) □TS(#49) □TS(#49) □TS(#55) □TS(#61) □TS(#67) □TS(#73) □TS(#79)	TS(#2) TS(#8) TS(#14) TS(#20) TS(#26) TS(#32) TS(#32) TS(#38) TS(#44) TS(#50) TS(#56) TS(#56) TS(#62) TS(#68) TS(#68) TS(#74)	□TS(#3) ☑TS(#9) ☑TS(#15) □TS(#27) □TS(#33) □TS(#39) □TS(#45) □TS(#51) □TS(#57) □TS(#63) □TS(#69) □TS(#75)	□TS(#4) ☑TS(#10) ☑TS(#16) □TS(#22) □TS(#28) □TS(#34) □TS(#40) □TS(#46) □TS(#52) □TS(#58) □TS(#58) □TS(#64) □TS(#70) □TS(#76)	TS(#5) TS(#11) TS(#17) TS(#23) TS(#29) TS(#35) TS(#41) TS(#41) TS(#47) TS(#53) TS(#53) TS(#59) TS(#65) TS(#71) TS(#77)	□TS(#6) ☑TS(#12) □TS(#18) □TS(#24) □TS(#30) □TS(#36) □TS(#42) □TS(#42) □TS(#48) □TS(#48) □TS(#54) □TS(#60) □TS(#66) □TS(#72) □TS(#78)	lear All Close

Figure 5-27 FMX-100G-MXP10 Demultiplex ODU2e Configuration

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

TP Multiplexing Str	ucture						
Port	11	T					
	1)(TS:1,2,3,4,5,6,7,8) 2)(TS:9,10,11,12,13,14,15, 3)(TS:17,18,19,20,21,22,2) 4)(TS:25,26,27,28,29,30,3) 5)(TS:33,34,35,36,37,38,39) 6)(TS:41,42,43,44,45,46,4' 7)(TS:49,50,51,52,53,54,51) 8)(TS:57,58,59,60,61,62,6) 9)(TS:65,66,67,68,69,70,7' 10)(TS:73,74,75,76,77,78,5)	,16) 3,24) 1,32) 9,40) 7,48) 5,56) 3,64) 1,72) 79,80)					
				ODU2	ODU2e	Clear All	Close

Figure 5-28 Configuration Result of FMX-100G-MXP10 Demultiplexing 10*ODU2e

5.3.1.3. Cross-Connection Configuration

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

Traffic Configuration					
■SNC Configuration	Add SNC Configurat	ion *			
CCH1+1 Configuration	ΤοοΙ				^
	Label		Туре	2WAYPR	Ŧ
	Capacity	ODU2e	T		
	А				
	Shelf	1	r Slot	2	•
	Port	1	TP TP	ODU2e(0)	Ŧ
	Z				
	Shelf	1	Slot	2	Ŧ
	Port	11	TP	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	•
	A Protection O				
	Shelf	1	Slot	1	Ŧ
	Port	1	TP		٣
	Z Protection				
	Shelf	1	Slot	1	Ŧ
	Port	11	TP	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	T
				Add	Close

Figure 5-29 FMX-100G-MXP10 Bidirectional Cross-Connection with Protection

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

Traffic Configuration										
SNC Configuration	Add ¹	* SNC	C Configuration					Coursely a		
	Snow	10	entries					Search: Search.		
	0 11	ID J1	Snc Type 🕼	Circuit ID 1	Src TpID	Des TpID	SrcProt TpID 1	DesProt TpID ↓↑		Ор
		1	2WAYPR		Slot2-port1-ODU2e(0)	Slot2-port11-ODU2e(1)		Slot1-port11-ODU2e(1)	Delete	Unpri
	Showing	g 1 to 1 o	of 1 entries					Previous	1	Next
								Delete	Add	Close

Figure 5-30 Successful Establishment of FMX-100G-MXP10 Bidirectional Cross-Connection with Protection

5.3.1.4. FEC Configuration

FEC is only configurable on OUT layer.

Line Side Port

Select NE-Slot 2, right click on "Port 11" and select "Port Management", and then select OCh (OTU4) as the port mode. In "OTU4" interface under "Port Configuration", select "FEC type" to view the configuration. There are in all 4 FEC modes for FMX-100G-MXP10 line side, which are respectively G.709FEC/SDFEC1/SDFEC2/SDFEC3. SDFEC2 is the default mode, as shown in the figure below:

Port Management				
BasicInfo Port Configuration	OTU4 BasicInfo *			A 2
Interface	Administrative State	Enabled •	FEC Type	SDFEC2 V
ODU4	Operational State	Down	Loopback	NONE
	Availability State	Normal		
	Degrade Interval	2	Degrade Threshold	128459
	TIM Mode	NONE	Expected SAPI	
	TIM AIS Insertion	True	Expected DAPI	
	Rx SAPI		TX SAPI	
	Rx DAPI		Tx DAPI	
	Rx Operator		Tx Operator	
				DCN Apply Close

Figure 5-31 FEC Configuration of FMX-100G-MXP10 Line Side Port

Client Side Port

Select NE-Slot 2, right click on "Port 11" and select "Port Management", and then select OTU2/OTU2e as the port mode. In "OTU2/OTU2e" interface under "Port Configuration", select "FEC type" to view the configuration. There are in all 4 FEC modes for FMX-100G-MXP10 client side, which are respectively FEC/G.709FEC/I.4EFEC/I.7EFEC. G.709FEC is the default mode, the configuration is as shown in the figure below:

Port Management				
BasicInfo	OTU2 BasicInfo *			
Port Configuration >	Tool			∧ 2
CTU2	Administrative State	Enabled •	Degrade Interval	2
	Operational State	Up	Degrade Threshold	12304
	Availability State	Normal	Near End ALS	No
	Loopback	NONE	FEC Type	G709FEC •
	TIM Mode	NONE	Expected SAPI	NoFEC G709FEC
	TIM AIS Insertion	False v	Expected DAPI	I.4EFEC I.7EFEC
	Rx SAPI		Tx SAPI	
	Rx DAPI	'E:ý′ܜޥeóÓ1	Tx DAPI	
	Rx Operator	⊥\¢øV8òd¤Bmg}Sœþœþ	Tx Operator	
				DCN Apply Close

Figure 5-32 FEC Configuration of FMX-100G-MXP10 Client Side (OTU2) Port

Port Management				×
BasicInfo	OTU2e OTU2 * BasicInfo	ж		
	Tool			^ C
OTU2e	Administrative State	Enabled v	FEC Type	G709FEC •
SE ODU2e	Operational State	Up	Loopback	NoFEC
	Availability State	Normal	Near End ALS	I.4EFEC
				1.7EFEC
	Degrade Interval	2	Degrade Threshold	12/48
	TIM Mode	NONE	Expected SAPI	
	TIM AIS Insertion	False v	Expected DAPI	
	Rx SAPI		Tx SAPI	
	Rx DAPI	'E:ý'ŪœÞ¥eóÔ1	Tx DAPI	
	Rx Operator	⊥\¢øV8òd¤Bmg}Sœþœþ	Tx Operator	
				DCN Apply Close

Figure 5-33 FEC Configuration of FMX-100G-MXP10 Client Side (OTU2e) Port

5.3.2. FMX-100G-TMXP2

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

5.3.2.1. Service Type

Line Side Port

Select NE-Slot 5, right click on "Port 3" and select "Port Configuration", the operation steps are as shown in the figure below:



Figure 5-34 FMX-100G-TMXP2 Line Side Port Information

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



Port Management			
■ BasicInfo■ Port Configuration	BasicInfo > Tool		
	Administrative State	Enabled	
	Operational State	Up	
	Availability	Normal	
	Port Mode	OCh(OTU4)	
		OTU4 OCh(OTU4)	þ

Figure 5-35 FMX-100G-TMXP2 Line Side Port Interface

Client Side 100G Port

Select NE-Slot 5, right click on "Port 1" and select "Port Configuration", the operation steps are as shown in the figure below:

		0	0	×
 Slot1 FMX-100G-MXP10 : initializing Slot2 FMX-100G-TMXP2 : operational 	• N1		۰ ۲۰۰۰ ۵	
Portal FPOrt Configuration FPluggable Configuration Solof3 FMX-100G-NMU : operational		0		
▲ MGMT1 ▲ MGMT2		10.32.130.118		EN .

Figure 5-36 FMX-100G-TMXP2 Client Side 100G Port Information

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

Port Management			
BasicInfo Port Configuration >	BasicInfo Tool		
	Administrative State	Enabled	•
	Operational State	Down	
	Availability	NotInstalled	
	Port Mode	HGE_GMP T	•
		OTU4 HGE GMP	h
		HGE_GFPF	

Figure 5-37 FMX-100G-TMXP2 Client Side 100G Port Interface

Client Side 40G Port

The current module mode is 100G; you need to change the card mode to 40G mode. Select NE (192.168.21.72)-Slot 2, right click on "Slot 2" and select "Card Configuration", as shown in the figure below:



Figure 5-38 Operation Steps of FMX-100G-TMXP2 Card Configuration

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

ard Configuration		
Card Mode	FMX-100G-TMXP2	•
ouru mode	FMX-40G-TMXP2	
	FMX-100G-TMXP2	

Figure 5-39 Selection of FMX-40G-TMXP2 Card Mode

Apply FMX-40G-TMXP2 mode.

System Management		Fault Management Perform:					
		Cara Contiguration			≽13	69	
		Card Mode	FMX-40G-TMXP2	•			
				Apply Close			
				1 W.			
UPSM : operational					1		
UPSM : operational	A Please make sure th	e cross connection or SNC configura	tion related to this card has beer	n removed successfully, otherwise this o	peration will be failed.		
					Apply Cancel		
operational					Cancer		1.
1XP10 : initializing MXP2 : operational		O I	они 0: 0 со 0:		• • •		

Figure 5-40 Apply FMX-40G-TMXP2 Module Mode

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





After a moment, NE synchronization is performed. The latest mode of FMX-40G-TMXP2 module is synchronized. The operation steps are as follows: select NE, right click to select "*Synchronize NE*", the interface is as shown in the figure below:



Figure 5-42 NE Synchronization

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



Figure 5-43 Successful Switch of the Module Mode

At this time, 40G client side port mode can be selected: select NE—Slot 2, right click on"*Port 1*" and select "*Port Management*", the interface is as shown in the figure below:

Port Management			
BasicInfo Port Configuration >	BasicInfo Tool		
	Administrative State	Enabled	•
	Operational State	Down	
	Availability	Empty	
	Port Mode	FGE_GMP	•
		OTU3 FGE_GMP	

Figure 5-44 FMX-40G-TMXP2 Client Side 40G Port Interface

5.3.2.2. Time Slot Configuration

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

Select NE, right click on "Slot 1" and select "TP Multiplexing Structure", the steps are as shown in the figure below:



Figure 5-45 Operation Steps of FMX-100G-TMXP2 TP Multiplexing

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

TP Multiplexing Structu	ıre		
Port	3	Ŧ	
DU4(0)			
			ODU2 ODU2e ODU3 Clear All Close

Figure 5-46 FMX-100G-TMXP2 -Demultiplexing Configuration Interface

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

TP Multiplexing Stru	ODU4 To ODU3					;	x	×
Port	ParentName	ODU4		TP ID	2	•		
	TS(#1)	TS(#2)	TS(#3)	TS(#4)	TS(#5)	TS(#6)		
	TS(#7)	TS(#8)	TS(#9)	TS(#10)	TS(#11)	TS(#12)	Clear All	Close
	TS(#13)	TS(#14)	TS(#15)	TS(#16)	TS(#17)	TS(#18)		
	TS(#19)	TS(#20)	TS(#21)	TS(#22)	TS(#23)	TS(#24)		
.21.72)	TS(#25)	TS(#26)	TS(#27)	TS(#28)	TS(#29)	TS(#30)		
WD DC 10U Long	TS(#31)	TS(#32)	TS(#33)	TS(#34)	TS(#35)	Image: Image		
FAH_DC_100 . ope	Image: Image	✓TS(#38)	Image: Image	✓TS(#40)	Image: Image	Image: Image		
M1H2_100G Transp	Image: Image	Image: Image	Image: Image	Image: Image	Image: Image	Image: Image		
Empty : available	Image: Image	TS(#50)	TS(#51)	TS(#52)	✓TS(#53)	Image: Image		
M1H2 40G Muxpon	Image: Image	✓TS(#56)	TS(#57)	Image: Image	✓TS(#59)	TS(#60)		
1	TS(#61)	TS(#62)	TS(#63)	TS(#64)	TS(#65)	TS(#66)		8
2	TS(#67)	TS(#68)	TS(#69)	TS(#70)	TS(#71)	TS(#72)		
3	TS(#73)	TS(#74)	TS(#75)	TS(#76)	TS(#77)	TS(#78)		
Empty : available	TS(#79)	TS(#80)						
T4H_DCO:operation DMD40:operationa						Apply Close		

Figure 5-47 Time Slot Configuration of FMX-100G-TMXP2 to Demultiplex ODU3

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

TP Multiplexing Stru	ucture						>
Port	3	¥					
DU4(0)	L)(TS:1,2,3,4,5,6,7,8,9,10 2)(TS:32,33,34,35,36,37,3	,11,12,13,14,15,16,17,18,19, 8,39,40,41,42,43,44,45,46,4	,20,21,22,23,24,25 7,48,49,50,51,52,5	5,26,27,28,29,30,31) 53,54,55,56,57,58,59,	60,61,62)		
					ODU3	Clear All	Close

Figure 5-48 Configuration Result of FMX-100G-TMXP2 to Demultiplex 2*ODU3

5.3.2.3. Cross-Connection Configuration

For example, if we need to create bidirectional cross-connection without protection of port 1 to port 3, the operation is as follows: Select FGE_GMP at the client side and select OCh (OTU4) at the line side, then ODU3 cross-connection is established correspondingly, as shown in the figure below:

Traffic Configuration				
■ SNC Configuration ■ OCH1+1 Configuration	Add SNC Configu Tool	ration *		^
	Label Capacity A	ODU3 •	Туре	2WAY •
	Shelf Port	1 v	Slot TP	5 v ODU3(0) v
	Z Shelf Port	1 •	Slot TP	5 ODU3(1)(TS:1,2,3,4,5,6,7,8,9,10,11,12,13,1 •
		·	,	Add Close

Figure 5-49 FMX-100G-TMXP2 Bidirectional Cross-Connection without Protection

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

Traffic Configuration										×
SNC Configuration	Add * SNC Configuration Show 25 ventries Search: Stot5									
		$ID \downarrow \uparrow$	Snc Type ↓↑	Circuit ID ↓↑	Src TpID	Des TpID	SrcProt TpID	DesProt T	oID ↓†	Оре
		3	2WAY		Slot5-port1-ODU3(0)	Slot5-port3-ODU3(1)				Delete
	Showing 1 to 1 of 1 entries filtered from 31 total entries						Previous	1	Next	
								Delete	Add	Close

Figure 5-50 Successful Establishment of FMX-100G-TMXP2 Bidirectional Cross-Connection without Protection

5.3.2.4. FEC Configuration

FEC is only configurable on OUT layer.

Line Side Port

Select NE-Slot 4, right click on "*Port 3*" and select "*Port Management*", and then select OCh (OTU4) as the port mode. In "*OTU4*" interface under "*Port Configuration*", select "*FEC type*" to view the configuration. There are in all 4 FEC modes for FMX-100G-TMXP2 line side, which are respectively G.709FEC/SDFEC1/SDFEC2/SDFEC3. SDFEC3 is the default mode, as shown in the figure below:

Port Management						×
BasicInfo	OTU4 BasicInfo *					
Port Configuration >	Tool					∧ <i>C</i>
Interface	Administrative State	Fnabled	EEC Tune	SDEEC3		•
STU4	Administrative State		T LO Type	G709FEC		
E ODU4	Operational State	Up	Loopback	SDFEC1		
III ODU3	Availability State	Normal 🔻		SDFEC3		
	Degrade Interval	2	Degrade Threshold	128459		
	TIM Mode	NONE	Expected SAPI			
	TIM AIS Insertion	False v	Expected DAPI			
	Rx SAPI		Tx SAPI			
	Rx DAPI		Tx DAPI			
	Rx Operator		Tx Operator			
				DCN	Apply	Close

Figure 5-51 FEC Configuration of FMX-100G-TMXP2 Line Side Port

Client Side 100G Port

Select NE-Slot 4, right click on "*Port 1*" and select "*Port Management*", and then select OCh (OTU4) as the port mode. In "*OTU4*" interface under "*Port Configuration*", select "*FEC type*" to view the configuration. There is only one default FEC mode for 100G client side, which is G.709FEC, as shown in the figure below:

Port Management					
BasicInfo Port Configuration →	OTU4 BasicInfo * Tool			^ <i>C</i>	
■ OTU4 ■ ODU4	Administrative State	Enabled •	FEC Type	G709FEC V G709FEC	
	Availability State	Normal V	Near End ALS	No •	
	TIM Mode	NONE V	Expected SAPI		
	TIM AIS Insertion	Faise V	Expected DAPI		
	Rx DAPI Rx Operator	ı¤:â"ÖÆµF)ïF,Ð{ ïb §ò{;üþûØ)/ Zƒ7å@,[şÿl	Tx DAPI Tx Operator		
				DCN Apply Close	

Figure 5-52 FEC Configuration of FMX-100G-TMXP2 Client Side 100G Port

Client Side 40G Port

Select NE-Slot 5, right click on "*Port 1*" and select "*Port Management*", and then select OTU3 as the port mode. In "*OTU3*" interface under "*Port Configuration*", select "*FEC type*" to view the configuration. There are in all 4 FEC modes for the client side 40G, which are respectively no FEC/G.709FEC/I.4EFEC/I.7EFEC. G.709FEC is the default mode, the configuration is as shown in the figure below:
Port Management						×
■ BasicInfo Port Configuration >	OTU3 BasicInfo * Tool				^	× 0
■ OTU3 ■ ODU3	Administrative State Operational State	Enabled •	Degrade Interval Degrade Threshold	2 49424		
	Availability State	Normal V	Near End ALS	No G709FEC		v
	TIM Mode	NONE V	Expected SAPI	NoFEC G709FEC I.4EFEC		
	TIM AIS Insertion	False V	Expected DAPI Tx SAPI	I./EFEC		
	Rx DAPI Rx Operator	ז¤:â"ÖÆµF)ïF,Đ{ ïb §ò{;üþûØ)/ Zƒ7å@[śŸl	Tx DAPI Tx Operator			
				DCN	Apply	Close

Figure 5-53 FEC Configuration of FMX-100G-TMXP2 Client Side 40G

5.4. Configuration Example

5.4.1. Service Transparent Transmission Configuration Example

Here we take site-to-site transmission between Site A and Site B of TMXP2 access GE service as an example.

Configure the service type of the client side port1 and port2 as FGE_GMP, and configure the mode of the line side port3 as ODU4. As the service type is ODU4, TP multiplexes the structure to ODU3.

Port Management		
BasicInfo	BasicInfo	
■ Port Configuration >	Tool	
	Administrative State	Disabled
	Operational State	Down
	Availability	Empty
	Port Mode	FGE_GMP
	Port Description	Can not contain /: *? " <> special characters



Port Management	n Manauennen – Paun Manauennen – Penunnance Manauennen	n Security mathaballatin Log mathaballatin OLP Agene	×
BasicInfo Port Configuration >	BasicInfo Tool		
	Administrative State	Enabled	•
	Operational State	Up	
	Availability	Normal	
	Port Mode	OCh(OTU4)	٣
	Port Description	Can not contain /:*?"<> special characters	
		Apply	Close



TP Multiplexing Structure		талениениенске тенопникет		
Port	3	•		
 ODU4(0) ODU3(1)(TS: ODU3(2)(TS: 	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 32,33,34,35,36,37,38,39,40,41,42,4	,16,17,18,19,20,21,22,23,24,25,26,27 3,44,45,46,47,48,49,50,51,52,53,54,5	,28,29,30,31) 55,56,57,58,59,60,61,62)	

Figure 5-56 ODU3 TP Multiplexing Structure

Create two-way cross-connection of ODU3 at the client side port3 to port1.

Traffic Configuration					×
SNC Configuration	Add SNC Configuration *				
	Tool				^
	Label		Туре	2WAY	٣
	Capacity	ODU3 •			
	A				
	Shelf	1 •	Slot	1	٣
	Port	3 •	TP	ODU3(1)(TS:1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19	,20,21. •
	Z				
	Shelf	1 •	Slot	1	•
	Port	1	ТР	ODU3(0)	٣
				Ac	d Close

Figure 5-57 Create Two-way Cross-Connection of ODU3

5.4.2. Configuration Example of Service Protection

Here we take Site A and Site B respectively acting as the primary and standby protection of MXP10 access 10GE service as an example.

Configure the service type of the client side port1-port10 as 10GE_BMP/GFPF/GFPF extp, and the mode of the line side port11 as OTU4.

Port Management		
BasicInfo	BasicInfo	
Port Configuration >	ТооІ	
	Administrative State	Enabled •
	Operational State	Down
	Availability	NotInstalled
	Port Mode	XGE_BMP v
		Apply Close

Figure 5-58 Configure Client Side Signal Mode

Port Management				×
EasicInfo	BasicInfo Tool			
	Administrative State	Enabled		•
	Operational State	Up		
	Availability	Normal		
	Port Mode	OCh(OTU4)		٣
	Port Description	Can not contain /:*?"<> special characters		
			Apply	Close

Figure 5-59 Configure Line Side Signal Mode

Create two-way SNC cross-connection with protection for ODU2 of the client side port1-port10 to port11.



Traffic Configuration					
SNC Configuration	Add SNC Configuration *				
	Tool				^
	Label		Туре	2WAY	٣
	Capacity	ODU2 T			
	A				
	Shelf	1 •	Slot	1	Ŧ
	Port	11 •	TP	ODU2(1)(TS:1,2,3,4,5,6,7,8)	Ŧ
	Z				
	Shelf	1 •	Slot	1	٣
	Port	1 •	TP	ODU2(0)	Ŧ
				A	dd Close

Figure 5-60 Create two-way cross-connection of ODU2

5.4.3. Configuration Example of Ring Network Service

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

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

Port Management		
■ BasicInfo■ Port Configuration	BasicInfo > Tool	
	Administrative State	Enabled
	Operational State	Down
	Availability	Notinstalled
	Port Mode	HGE_GMP T
		Apply Close

Figure 5-61 Configure Client Side Signal Mode

Port Management				×
 ■ BasicInfo ■ Port Configuration 	BasicInfo Tool			
	Administrative State	Enabled		•
	Operational State	Up		
	Availability	Normal		
	Port Mode	OCh(OTU4)		•
			Apply	Close

Figure 5-62 Configure Line Side Signal Mode

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

Traffic Configuration					x
SNC Configuration	Add SNC Configurat	tion *			
■ OCH1+1 Configuration	Tool				^
	Label		Туре	2WAYPR	Ŧ
	Capacity	ODU4	•		
	A				
	Shelf	1	▼ Slot	2	•
	Port	1	TP	ODU4(0)	T
	Z				
	Shelf	1	▼ Slot	2	Ŧ
	Port	3	TP	ODU4(0)	٣
	A Protection O				
	Shelf	1	▼ Slot	2	Ŧ
	Port	1	TP		٣
	Z Protection				
	Shelf	1	▼ Slot	3	•
	Port	3	TP	ODU4(0)	•
		L		[Add Close

Figure 5-63 Create Two-way Cross-Connection of ODU4

Build the environment according to the following diagram.

Rote

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





6. Overhead Configuration

6.1. Configuration Rules

The G.709 standard defines the overhead function of the OTN frame structure and the network of each layer. FMX 100G modules adopts a lot of overhead bytes, which provides great convenience for equipment maintenance.

FMX 100G modules usually configures overhead such as SM, PM, TCMi (i = $1 \sim 6$) etc. This chapter describes in detail the configuration methods of various overhead, including: configuration rules, configuration steps and configuration examples.

6.1.1. SM, PM & TCMi Overhead Introduction

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

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

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

6.1.2. Overhead Configuration Rules

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

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

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

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

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

6.1.3. TTI Configuration Rules

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

TTI includes SAPI and DAPI. SAPI value and DAPI value sent by single card at the opposite end are required to be consistent with SAPI value and DAPI value expected to be received by single card at the local end, and SAPI value and DAPI value sent by single card at the local end are consistent with SAPI value and DAPI value expected to be received at the opposite end. That is to say, the two network elements connected by the overhead should meet the rules as shown in table 6-1:

NE A		Set Relationship	NE B	
Send TTI	SAPI	=	SAPI	Receive ∏I
	DAPI	=	DAPI	

Receive TTI	SAPI	=	SAPI	Send TTI
	DAPI	=	DAPI	

Table 6-1 Overhead Establishment Rules

6.2. Configuration Steps

6.2.1. SM Configuration Steps

Here we take FMX-100G-MXP10 module as an example to introduce the SM configuration steps:

• Activate the connection and monitoring enablement of SM overhead.

In FMX NMS, the service XGE_GFPF is configured for port 1 of the local end and opposite end of FMX-100G-MXP10 module (Specific service is configured according to actual demand). OTU4 service is configured for port 11 of the local-end and opposite-end module (Specific service is configured according to actual demand). Demultiplex ODU4 to ODU2, configure service cross-connection, connect optical fiber and build the environment.

Configuration Steps

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



Figure 6-1 Enter Port Management Interface



Port Management		x
■ BasicInfo Port Configuration >	BasicInfo Tool	
	Administrative State	Enabled •
	Operational State	Up
	Availability	Normal
	Port Mode	OTU4 •
		Apply Close

Figure 6-2 Select Port Service

🖻 🔜 Shelf01	
Slot1 F	Card Current Alarm
- Port	TP Multiplexing Structure
📥 Port	Card ColdReboot
📥 Port	Card WarmReboot
📥 Port5	
📥 Port6	
📥 Port7	
📥 Port8	
📥 Port9	
Port1	0
Port1	1

Figure 6-3 Enter TP Multiplexing Interface

TP Multiple	exing Structure								
Port		11	•						
	<u>)U4(0)</u>								
						ODU2	ODU2e	Clear All	Close

Figure 6-4 TP Multiplexing Configuration Step 1

TP Multiplexing Stru	ODU4 To ODU2					\$	c x
Port	ParentName	ODU4		TP ID	9	T	
	TS(#1)	TS(#2)	TS(#3)	TS(#4)	TS(#5)	TS(#6)	
	TS(#7)	TS(#8)	TS(#9)	TS(#10)	TS(#11)	TS(#12)	Clear All Close
	TS(#13)	TS(#14)	TS(#15)	TS(#16)	TS(#17)	TS(#18)	
ot11 OMD40 : ope	TS(#19)	TS(#20)	TS(#21)	TS(#22)	TS(#23)	TS(#24)	
lot12 T6DH : opera	TS(#25)	TS(#26)	TS(#27)	TS(#28)	TS(#29)	TS(#30)	
lot13 Empty : avail	TS(#31)	TS(#32)	TS(#33)	TS(#34)	TS(#35)	TS(#36)	
lot14 T20X : absen	TS(#37)	TS(#38)	TS(#39)	TS(#40)	TS(#41)	TS(#42)	
lot15 Empty : initia	TS(#43)	TS(#44)	TS(#45)	TS(#46)	TS(#47)	TS(#48)	
lot16 M1H10 : ope	TS(#49)	TS(#50)	TS(#51)	TS(#52)	TS(#53)	TS(#54)	
Port1	TS(#55)	TS(#56)	TS(#57)	TS(#58)	TS(#59)	TS(#60)	
Port2	TS(#61)	TS(#62)	TS(#63)	TS(#64)	Image: Image	✓TS(#66)	
Port3	Image: Image	Image: Image	Image: Image	Image: Image	Image: Image	Image: Image	
Port4	TS(#73)	TS(#74)	TS(#75)	TS(#76)	TS(#77)	TS(#78)	•
Port5	TS(#79)	TS(#80)					
Port6						Apply Close	•
Port7							

Figure 6-5 TP Multiplexing Configuration Step 2

Port Management				×
BasicInfo Port Configuration	OTU4 BasicInfo *			A .C
Interface	Administrative State	Enabled •	FEC Type	G709FEC T
DU4	Operational State	Up	Loopback	NONE
	Availability State	Normal 🔻		
	Degrade Interval	2	Degrade Threshold	128459
	TIM Mode	NONE	Expected SAPI	
	TIM AIS Insertion	False	Expected DAPI	
	Rx SAPI		Tx SAPI	
	Rx DAPI		Tx DAPI	
	Rx Operator		Tx Operator	
				DCN Apply Close

Figure 6-6 Click to Enter OTU4 Port Interface

Port Management				
BasicInfo	Interface * OTU4 BasicInfe	» ×		
Port Configuration >	Тооі			∧ <i>Q</i>
	Administrative State	Enabled •	FEC Type	G709FEC •
CTU4	Operational State	Up	Loopback	NONE
	Availability State	Normal		
	Degrade Interval	2	Degrade Threshold	128459
	TIM Mode	SAPI_DAPI v	Expected SAPI	
	TIM AIS Insertion	True v	Expected DAPI	
	Rx SAPI		Tx SAPI	
	Rx DAPI		Tx DAPI	
	Rx Operator		Tx Operator	
				DCN Apply Close

Figure 6-7 Set SM Overhead

• TTI Configuration

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

Port Management				×
BasicInfo Port Configuration >	Interface * OTU4 BasicInfo	× (^ <i>C</i>
InterfaceOTU4	Administrative State	Enabled •	FEC Type	G709FEC •
CDU4	Operational State Availability State	Vp Normal •	Loopback	NONE
	Degrade Interval	2	Degrade Threshold	128459
	TIM Mode	SAPI_DAPI 🔻	Expected SAPI	Α
	TIM AIS Insertion	True v	Expected DAPI	В
	Rx SAPI		Tx SAPI	с
	Rx DAPI		Tx DAPI	D
	Rx Operator		Tx Operator	
				DCN Apply Close

Figure 6-8 Configure Local-End TTI

Port Management				
BasicInfo	Interface * OTU4 BasicInfe) [*]		
Port Configuration >	Tool			∧ <i>Q</i>
	Administrative State	Enabled •	FEC Type	G709FEC V
DU4	Operational State	Up	Loopback	NONE
	Availability State	Normal 🔻		
	Degrade Interval	2	Degrade Threshold	128459
	TIM Mode	SAPI_DAPI v	Expected SAPI	D
	TIM AIS Insertion	True 🔻	Expected DAPI	С
	Rx SAPI		Tx SAPI	В
	Rx DAPI		Tx DAPI	A
	Rx Operator		Tx Operator	
				DCN Apply Close

Figure 6-9 Configure Opposite-End TTI

Attention

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

6.2.2. PM Configuration Steps

• Activate the connection and monitoring enablement of PM overhead.

In FMX NMS, the service XGE_BMP is configured for port 1 of the local end and opposite end of FMX-100G-MXP10 module (Specific service is configured according to actual demand). OTU4 service is configured for port 11 of the local-end and opposite-end module (Specific service is configured according to actual demand). Demultiplex ODU4 to ODU2e, configure service cross-connection, connect optical fiber and build the environment.

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

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

🖻 📩 Shelf01	
🖻 😂 Slot1 FM	X-100G-MXP10 : operational
📥 Port1	
📥 Port2	
📥 Port3	
📥 Port4	
📥 Port5	
📥 Port6	
📥 Port7	
📥 Port8	
📥 Port9	
- Port10)
📥 Port 🗧	De la Cara Savaraliana
🗏 😂 Slot2 F	Port Configuration al
- Port:	Pluggable Configuration
Port2	

Figure 6-10 Enter Line Side Port Management Interface

Port Management				×
BasicInfo	ODU2e ODU4 *	BasicInfo *		
Port Configuration >	Tool			~
E OTU4	Ohavi (A) antijas		0	
CDU4	Show 10 v entries		Search	Search
DU2e	ODU2e 11	Administrative State	Operational State	Operation 1
	1	Enabled	Up	Management
	2	Enabled	Up	Management
	3	Enabled	Up	Management
	4	Enabled	Up	Management
	5	Enabled	Up	Management
	6	Enabled	Up	Management
	7	Enabled	Up	Management
	8	Enabled	Up	Management
	Showing 1 to 8 of 8 entrie	S	I	Previous 1 Next

Figure 6-11 Enter Line Side ODU2e Management Interface

Port Management				x
BasicInfo	ODU2e ODU4 * BasicInfo	» ×		
Port Configuration	Tool			~
OTU4	Administrative State	Enabled	OPU State	Intact
ODU4	Operational State	Up	Rx PT	
	Availability State	Normal	Tx PT	
	PLM AIS Insertion	•	Expected PT	
	Degrade Interval	2	Degrade Threshold	12748
	NIM	Enabled		
	TIM Mode	SAPI_DAPI v	Expected SAPI	
	Trace Identifier Mismatch(TIM) AIS Insertion	True	Expected DAPI	
	Rx SAPI	<u> </u>	Tx SAPI	
	Rx DAPI	<u> </u>	Tx DAPI	
	Rx Operator	<u> </u>	Tx Operator	
				DCN Apply Close

Figure 6-12 Set Line Side PM Overhead



Figure 6-13 Enter Client Side Port Management Interface

Port Management				
BasicInfo	ODU2e BasicInfo	x		
■ Port Configuration >	Tool			~
Interface				
DDU2e	Show 10 v entries		Sear	ch: Search
	ODU2e It	Administrative State	Operational State	Operation 1
	0	Enabled	Up	Management
	Showing 1 to 1 of 1 entries	5		Previous 1 Next

Figure 6-14 Enter Client Side ODU2 Management Interface

Port Management				×
BasicInfo	ODU2e BasicInfo *			
■ Port Configuration >	Tool			^
Interface	Administrative State	Enabled	OPU State	Client
ODU2e	Operational Otata	Un		0.2
	Operational State	Op	RXPI	020
	Availability State	Normal	TX PT	0x3
	PLM AIS Insertion	True	Expected PT	0x3
	Degrade Interval	2	Degrade Threshold	12748
	TIM Mode	SAPI_DAPI	Expected SAPI	
	Trace Identifier Mismatch(TIM) AIS Insertion	True	Expected DAPI	
	Rx SAPI		Tx SAPI	
	Rx DAPI		Tx DAPI	
	Rx Operator		Tx Operator	
				Apply Close

Figure 6-15 Set Client Side PM Overhead

• TTI Configuration

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

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

Port Management				×
BasicInfo	ODU2e ODU4 * BasicInfo	ж		
Port Configuration >	Tool			^
III OTU4 III ODU4	Administrative State	Enabled	OPU State	Intact
B ODU2e	Operational State	Up	Rx PT	
	Availability State	Normal	Tx PT	
	PLM AIS Insertion	•	Expected PT	
	Degrade Interval	2	Degrade Threshold	12748
	NIM	Enabled	can only configure Expected S	SAPI/DAPI
	TIM Mode	NONE	Expected SAPI	
	Trace Identifier Mismatch(TIM)	False	Expected DAPI	
	Rx SAPI	<u>ŸŸŸŸŸŸŸŸŸŸŸŸ</u>	Tx SAPI	
	Rx DAPI	<u> </u>	Tx DAPI	
	Rx Operator	<u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>	Tx Operator	
				DCN Apply Close

Figure 6-16 Configure Line Side Port TTI

Port Management				×
BasicInfo	ODU2e BasicInfo *			
Port Configuration >	Tool			^
Interface	Administrative State	Enabled	OPU State	Client
CDU2e	On anti-interal Oteta	Un	Dr. DT	02
	Operational State	op	RX PT	0X3
	Availability State	Normal v	Tx PT	0x3
	PLM AIS Insertion	True	Expected PT	0x3
	Degrade Interval	2	Degrade Threshold	12748
	TIM Mode	SAPI_DAPI v	Expected SAPI	A
	Trace Identifier Mismatch(TIM) AIS Insertion	True	Expected DAPI	В
	Rx SAPI		Tx SAPI	С
	Rx DAPI		Tx DAPI	D
	Rx Operator		Tx Operator	
				Apply Close

Figure 6-17 Configure Client Side Local End Port TTI

Port Management				×
BasicInfo	ODU2e BasicInfo *			
Port Configuration >	Tool			^
Interface	Administrative State	Enabled	OPU State	Client
	Operational State	Up	Rx PT	0x3
	Availability State	Normal	Tx PT	0x3
	PLM AIS Insertion	True v	Expected PT	0x3
	Degrade Interval	2	Degrade Threshold	12748
	TIM Mode	SAPI_DAPI v	Expected SAPI	С
	Trace Identifier Mismatch(TIM)	True 🔻	Expected DAPI	D
	AIS Insertion		TY CADI	Δ
	RX SAFI			R
	RX DAPI			
				Apply Close

Figure 6-18 Configure Client Side Opposite End Port TTI

😚 Hint

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

6.3. Configuration Examples

Application Environment:



Figure 6-19 Application Environment of SM/PM Overhead Configuration

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

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



Figure 6-20 Schematic Diagram of SM Overhead Configuration

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

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



Figure 6-21 Schematic Diagram of PM Overhead Configuration

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

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

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

7. SNC Protection Configuration

7.1. Introduction of SNC Protection

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

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



Figure 7-1 Schematic Diagram of SNC Protection Service Environment

7.2. Configuration Steps

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

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

Set reply mode—Reply Mode or Non-reply Mode.
If it is set as "non-reply mode", it indicates that after the service is reversed to the secondary channel, even if the primary channel recovers to normal, the service will still work on the secondary channel until failure occurs to the secondary channel.
If it is set as "reply mode", it needs to simultaneously set the reply waiting time. It indicates that after the service is reversed to the secondary channel, if the primary channel recovers to normal, the service will immediately return to the primary channel or recover to the primary channel after the reply waiting time.
The settings for the two ends of the protection equipment should keep consistent.
Manually select the issuing external command.
Manually delete the protection channel/working channel.

Table 7-1 SNC Configuration Process

7.3. Configuration Example

The SNC service types supported by various chassis and modules are listed in the following table.

Chassis Type	Module Type	Supported SNC Service Type
FMX-100G-CH2U	FMX-100G-MXP10	10G Business Module SNC protection 10G service cross module SNC protection
	FMX-100G-TMXP2	100G service cross module SNC protection

Table 7-2 Supported SNC Service Type Table

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

Service Rate	Service Type	Capacity Type
10G Service	XGE_BMP	ODU2e
	XGE_GFPF	ODU2
	XGE_GFPFextp	
	STM64_AMP/OC48_AMP	
	STM64_BMP/OC48_BMP	
	OTU2	
	OTU2e	ODU2e
40G Service	FGE_GMP	ODU3
	ОТИЗ	
100G Service	HGE_GMP	ODU4
	HGE_GFPF	
	OTU4	

Table 7-3 TP Mulltiplexing Capacity Table of SNC Service

Here we take the 10G service cross module protection of FMX-100G-MXP10 module as an example to introduce the configuration process of SNC services.

1. Insert a FMX-100G-MXP10 module in FMX-100G-CH2U and open the NMS interface to add the NE after the normal start-up of the module.

Add Equipment	×
Parent Node	Global View
Display Name	OTN
IP Address	10.32.130.116
Subnet Mask	255.255.255.0
Trap Name	moon
Trap Host	10.32.130.19
	Apply Close

Figure 7-2 Add NE

Select a client side port (Port 1-10), (here we take Port 1 of Slot 16 as the client side signal port), then right click on the port and select "Port Management".



Figure 7-3 Select Client Side Port

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

Port Management				×
BasicInfo	>	BasicInfo		
		Administrative State	Enabled	¥
		Operational State	Up	
		Availability	Normal	
		Port Mode	XGE_GRPP XGE_GPPF	-
s Siot1 FIT_DOO TOPERATIONAL SIOt11 OMD40 : operational SIOt11 OMD40 : operational SIOt12 T6DH : operational SIOt13 Empty : available	Π		XGE_GFPFexp STM64_AMP OCT02_AMP OTU2 OTU2 OTU2 OTU2 OTU2 OTU2 OTU2 DAPPO OTU2 DAPPO OTU2 DAPPO DAPO DA	

Figure 7-4 Configure Client Side Service

2. Here we take Port 11 of Slot 16 and Port 11 of pair Slot 17 as the line side port. Right click on the port and select "*Port Management*". Then select the needed service type according to the optical module type of the line side, enable the port and click on "*Apply*".

Port Management		x
E BasicInfo	BasicInfo > Tool	
	Administrative State	Enabled v
	Operational State	Up
	Availability	Normal
	Port Mode	OTU4 v
		OTU4 OCh(OTU4)

Figure 7-5 Configure Line Side Service

3. Right click on the Business Module and select "TP Multiplexing Structure".



Figure 7-6 TP Multiplexing Structure

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

TP Multiplexing Structure	ODU4 To ODU2						×	×
Port	ParentName	ODU4		TP ID	9		•	
■ODU4(0)	TS(#1)	TS(#2)	TS(#3)	TS(#4)	TS(#5)	TS(#6)		٦.
	TS(#7)	TS(#8)	TS(#9)	TS(#10)	TS(#11)	TS(#12)	IZe Clear All Close	
	TS(#13)	TS(#14)	TS(#15)	TS(#16)	TS(#17)	TS(#18)		
1000 Transponder Lipitio	TS(#19)	TS(#20)	TS(#21)	TS(#22)	TS(#23)	TS(#24)		<u> </u>
_100G fransponder . mida	TS(#25)	TS(#26)	TS(#27)	TS(#28)	TS(#29)	TS(#30)		
100G Transponder : opera	TS(#31)	TS(#32)	TS(#33)	TS(#34)	TS(#35)	TS(#36)		
· available	TS(#37)	TS(#38)	TS(#39)	TS(#40)	TS(#41)	TS(#42)		
CO : operational	TS(#43)	TS(#44)	TS(#45)	TS(#46)	TS(#47)	TS(#48)		
0 : operational	TS(#49)	TS(#50)	TS(#51)	TS(#52)	TS(#53)	TS(#54)		
CO : operational	TS(#55)	TS(#56)	TS(#57)	TS(#58)	TS(#59)	TS(#60)		
20-2X100G : operational	TS(#61)	TS(#62)	TS(#63)	TS(#64)	Image: Image	Image: Image		
40 : operational	Image: Image	Image: Image	Image: Image	Image: Image	Image: Image	Image: Image		
I : operational	TS(#73)	TS(#74)	TS(#75)	TS(#76)	TS(#77)	TS(#78)		
y : available	TS(#79)	TS(#80)						
: absent						Apply	Close	
y : initializing								

Figure 7-7 Select Time Slot Demultiplexing

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

Traffic Configuration						
SNC Configuration	Add SNC Configuration *					
CCH1+1 Configuration	Tool					^
	Label		Туре	2WAY		•
	Capacity	ODU0 T		2WAY 1WAY		
	A			2WAYPR 1WAYPR		
	Shelf	1 *	Slot	2		۳
	Port	1 *	ТР			۳
	Z					
	Shelf	1 *	Slot	2		۳
	Port	1 *	ТР			۳
					Add	Close

Figure 7-8 Select Cross-Connection Type

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

Traffic Configuration						×
SNC Configuration	Add SNC Configuration *					
CCH1+1 Configuration	Tool					^
	Label		Туре	2WAY		•
	Capacity	0000]			
	A	ODU0 ODU1				
	Shelf	ODU2 ODU2e	Slot	2		٣
	Port	ODU3 ODU4	TP			٣
	Z	ODUFlex				
	Shelf	1 •	Slot	2		٣
	Port	1	TP			٣
					Add	Close

Figure 7-9 Select Service Capacity

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

Traffic Configuration					×
SNC Configuration	Add SNC Configuration *				
CCH1+1 Configuration	Tool				^
	Label		Туре	2WAYPR	•
	Capacity	ODU2e 🔹			
	A				
	Shelf	1	Slot	16	٣
	Port	11 •	TP	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	٣
	Z				
	Shelf	1 *	Slot	16	•
	Port	1 •	TP	ODU2e(0)	*
	A Protection				
	Shelf	1 *	Slot	16	٣
	Port	1 *	TP		•
	Z Protection				
	Shelf	1 *	Slot	16	•
	Port	11 💌	TP	ODU2e(1)(TS:1,2,3,4,5,6,7,8)	•
					Add Close

Figure 7-10 Select Protection Mode

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

SNC	Configura	ition									
Show	10 🔻	entries						S	earch: Slot		
	ID ↓†	Snc Type ↓↑	Circuit ID	Src TpID	Des TpID ↓↑	SrcProt TpID 1	DesProt TpID		Operat	ion	J1
	1	2WAYPR	111	Slot3-port1-ODU1(0)	Slot4-port4-ODU2e(0)		Slot4-port4-ODU2e(0)	Delete	Unprotect	PPG	Switch
	2	2WAYPR		Slot14-port1-ODU2e(0)	Slot14-port11-ODU2e(0)		Slot14-port12-ODU2e(0)	Delete	Unprotect	PPG	Switch
	4	2WAY	16-1	Slot16-port2-ODU2e(0)	Slot16-port11-ODU2e(2)			Delete	Protect		

Figure 7-11 Click Protection Group

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

Traffic Configuration						
SNC Configuration	PPG SNC Configuration *					
CCH1+1 Configuration	Tool					~
	Availability State		Protection Type	SNC/N		•
	Working TpID		Protecting TpID			
	Switch Type	Uni-directional v	Wait to Restore(s)			
	Revertive Mode	Non Revertive 🔻				
					Apply	Close
L						

Figure 7-12 Select Protection Type

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

Traffic Configuration					×
SNC Configuration	PPG SNC Configuration * Tool				^
	Availability State	Protecting	Protection Type	SNC/N	Ŧ
	Working TpID	Slot14-port11-ODU2e(0)	Protecting TpID	Slot14-port12-ODU2e(0)	
	Switch Type	Uni-directional	Wait to Restore(s)	300	
	Revertive Mode	Non Revertive v			
		Non Revertive Revertive			Apply Close

Figure 7-13 Reply Wait Settings

9. Click on "Protection Switching" option of the created SNC protection cross-connection.

Traffic Configuration													
SNC Configuration	Switch Show 1	0 v	G * SNC Cont	iguration					Se	earch: Slot			
		ID J1	Snc Type 🔱	Circuit ID	Src TpID	Des TpID	SrcProt TpID	DesProt TpID		Operat	ion	ļ	
		1	2WAYPR	111	Slot3-port1-ODU1(0)	Slot4-port4-ODU2e(0)		Slot4-port4-ODU2e(0)	Delete	Unprotect	PPG	Switch	
		2	2WAYPR		Slot14-port1-ODU2e(0)	Slot14-port11-ODU2e(0)		Slot14-port12-ODU2e(0)	Delete	Unprotect	PPG	Switch	
		4	2WAY	16-1	Slot16-port2-ODU2e(0)	Slot16-port11-ODU2e(2)			Delete	Protect			

Figure 7-14 Protection Switching Settings

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

Traffic Configuration		x
SNC Configuration	Switch PPG * SNC Configuration * Tool	^
	Current Request External Command	Signal Fai_W Forced Switch_Working *
Slatt Empty - available		Clear Lockout for Protection Forced Switch,
Slot7 T4H_DCO : operational Slot8 OMD40 : operational Slot8 T4H_DCO : operational	o	Marual Switch Portection Manual Switch Working Exercise



10. Click on "Delete Protection" option of the created SNC protection cross-connection.

Traffic Configuration												×
ENC Configuration	Switc	h * PP	G * SNC Cont	figuration					Se	earch: Slot		
		ID J1	Snc Type 🔱	Circuit ID 11	Src TpID	Des TpID 11	SrcProt TpID	DesProt TpID		Operati	on	
		1	2WAYPR	111	Slot3-port1-ODU1(0)	Slot4-port4-ODU2e(0)		Slot4-port4-ODU2e(0)	Delete	Unprotect	PPG	Switch
		2	2WAYPR		Slot14-port1-ODU2e(0)	Slot14-port11-ODU2e(0)		Slot14-port12-ODU2e(0)	Delete	Unprotect	PPG	Switch
		4	2WAY	16-1	Slot16-port2-ODU2e(0)	Slot16-port11-ODU2e(2)			Delete	Protect		

Figure 7-16 Delete Protection

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

Traffic Configuration			
SNC Configuration	UnProtect Switch * PPG * SNC Configuration *		
CCH1+1 Configuration	Tool		^
	Туре	2WAY	v
	Point to Delete	Working	٣
		Working Protecting	

Figure 7-17 Delete Working Channel or Protection Channel

8. Alarm Management

8.1. Alarm Management Introduction

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

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

8.2. Main Interface of Alarm Management

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



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 8-1 Alarm Management

8.2.1. Current Alarm

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

٢	•	Home	System	Management	Configuration Ma	anagement Fault Management P	Performance Management	Security Manage	ment Lo	og Management O	LP Route
								▶125 C	79	029 017	@0 root
Show ;	25 • entries						Acknowledge Unackno	wledge Filter	All Refres	h Search: s	Search
	Operation 1	Detail	Number	Severity 1	NE II	Alarm Source	Alarm Name	Alarm Type 1	State 11	Raised Time	Acknowledge State
	*	0	1	Critical	192.168.126.1_126	Location_Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Set	2000/02/28 01:52:00	Unacknowledge
	*	0	2	Critical	192.168.126.1_126	Location_Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Set	2000/02/28 01:52:00	Unacknowledge
	*	0	3	Critical	192.168.126.1_126	Location_Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Set	2000/02/28 01:51:50	Unacknowledge
0	*	0	4	Critical	192.168.126.1_126	Location_Shelf1_Slot1_Port9_ETYn	ETY_LOS	Communication	Set	2000/02/28 01:30:25	Unacknowledge
	*	0	5	Major	192.168.126.1_126	Location_Shelf1_Slot1_Port2_ETYn	ETY_CSF_OPU	Communication	Set	2000/02/28 01:29:02	Unacknowledge
	*	0	6	Critical	192.168.126.1_126	Location_Shelf1_Slot1_Port2_Pluggable	Pluggable_Missing	Equipment	Set	2000/02/28 01:28:58	Unacknowledge
8	*	0	7	Major	192.168.126.1_126	Location_Shelf1_Slot6	EQPT_Power_Supply_Issue	Equipment	Set	2000/02/28 01:26:40	Unacknowledge
	*	0	8	Minor	192.168.126.1_126	Location_Shelf1_Slot1_Port5_ODU4(0)	ODU_OCI	Communication	Set	2000/02/27 11:04:10	Unacknowledge
	4	0	9	Minor	192.168.126.1_126	Location_Shelf1_Slot1_Port6_ODU4(0)	ODU_OCI	Communication	Set	2000/02/27 11:04:10	Unacknowledge

Figure 8-2 Current Alarm

The upper left area of the navigation bar can filter the number of alarms displayed on the current page, and the number of displayed alarms per page can be adjusted to 25, 50, 75 and 100 (as shown below).



Figure 8-3 Show Number of Current Alarms

The right-hand area in the middle of the navigation bar shows the "Confirm", "Cancel Confirmation", "Clear", "Filter", "All", "Refresh/Close" buttons. The functions of these buttons are:

• The function of "Confirm" 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 "confirmed" and the "confirmation" icon becomes green with specific confirmation person and confirmation time. The specific operation is: select the alarm to be confirmed→click the "confirm" button→click on "apply" → confirm the alarm.

🕜 Hint

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

Show	25 • entries						Acknowledge Unackno	wledge Filter	All Refres	Search: S	earch
	Operation 1	Detail	Number	Severity 1	NE	Alarm Source 11	Alarm Name ↓↑	Alarm Type 🕼	State 1	Raised Time	Acknowledge State
۲	🔦 🖌 Ackno	wledge	1	Critical	192.168.126.1_126	Location_Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Set	2000/02/28 01:55:03	Unacknowledge
	*	0	2	Critical	192.168.126.1_126	Location_Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Set	2000/02/28 01:54:56	Unacknowledge
	*	0	3	Critical	192.168.126.1_126	Location_Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Set	2000/02/28 01:54:45	Unacknowledge
	*	0	4	Critical	192.168.126.1_126	Location_Shelf1_Slot1_Port9_ETYn	ETY_LOS	Communication	Set	2000/02/28 01:30:25	Unacknowledge
	*	0	5	Major	192.168.126.1_126	Location_Shelf1_Slot1_Port2_ETYn	ETY_CSF_OPU	Communication	Set	2000/02/28 01:29:02	Unacknowledge
	*	0	6	Critical	192.168.126.1_126	Location_Shelf1_Slot1_Port2_Pluggable	Pluggable_Missing	Equipment	Set	2000/02/28 01:28:58	Unacknowledge
	*	0	7	Major	192.168.126.1_126	Location_Shelf1_Slot6	EQPT_Power_Supply_Issue	Equipment	Set	2000/02/28 01:26:40	Unacknowledge

Figure 8-4 Select to Confirm Current Alarm

show ;	25 🔻	entries						Acknowledge Unacknow	wledge Filter	All Refrest	Search:	Search
	Operati	ion ↓†	Detail	Number	Severity 1	NE J†	Alarm Source	Alarm Name 🕼	Alarm Type 1	State 11	Raised Time	Acknowledge State
	*		0	1	Critical	192.168.126.1_126	Location_Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Set	2000/02/28 01:56:12	Unacknowledge
	ĸ		0	2	Critical	192.168.126.1_126	Location_Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Set	2000/02/28 01:55:47	Unacknowledge
	ĸ		0	3	Critical	192.168.126.1_126	Location_Shelf1_Slot1_Port9_ETYn	ETY_LOS	Communication	Set	2000/02/28 01:30:25	Unacknowledge
	ĸ		0	4		192.168.126.1_126	Location_Shelf1_Slot1_Port2_ETYn	ETY_CSF_OPU	Communication	Set	2000/02/28 01:29:02	Unacknowledge
	ĸ		0	5	Critical	192.168.126.1_126	Locatio	ing	Equipment	Set	2000/02/28 01:28:58	Unacknowledge
	ĸ		0	6		192.168.126.1_126	Locatio	Supply_Issue	Equipment	Set	2000/02/28 01:26:40	Unacknowledge
	ĸ		0	7	Minor	192.168.126.1_126	Locatio Apply	Cancel	Communication	Set	2000/02/27 11:04:10	Unacknowledge
			0	-						-		

Figure 8-5 Carry Out Confirmation of Current Alarm

Show :	25 v entries									Acknowledge Unacknowle	idge Filter All <mark>Refres</mark> t	Search). Search
04	Operation 11	Detail	Number	Sevenity 1	NE II	Alarm Source	Alarm Name	Alarm Type	State 11	Raised Time	Acknowledge State	Acknowledge User	Acknowledge Time
8	4	0	1	Minor	192.168.21.72_72	Location_Shelf1_Slot16_Port4_OTUk	OTU_BDI	Communication	Set	2019/02/27 01:22:20	Acknowledge	root	2019/02/27 10:09:54
8	*	0	2	Critical	192.168.21.72_72	Location_Shelf1_Slot17_Port4_OTUk	OTU_LOF	Communication	Set	2019/02/26 21:34:19	Acknowledge	root	2019/02/27 10:09:58
8	*	0	3	Minor	192.168.21.72_72	Location_Shelf1_Slot9_Port4_ODU4(0)	ODU_OCI	Communication	Set	2019/02/26 19:48:16	Acknowledge	root	2019/02/27 10:10:01
8	*	0	4	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port3_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
8	*	0	5	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port1_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
8	*	0	6	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port4_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
8	×	0	7	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port2_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
8	e.	0	8	Minor	192.168.21.72_72	Location_Shelf1_Slot12_Port1_ODU4(0)	ODU_OCI	Communication	Set	2019/02/26 19:47:29	Unacknowledge		
8	*	0	9	Critical	192.168.21.72_72	Location_Shelf1_Slot12_Port1_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:47:26	Unacknowledge		

Figure 8-6 Complete Confirmation of Current Alarm

• The function of "*Cancel Confirmation*" 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 "Cancel confirmation" button→click on "Apply"→ The alarm is not confirmed.

🕜 Hint

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

Show	• entries									Acknowledge Unacknowle	adge Filter All Refrest	Search	E Search
04	Operation 1	Detail	Number	Severity 1	NE II	Alarm Source 11	Alarm Name	Alanni Type 👘	State 1	Raised Time 11	Acknowledge State	Acknowledge User	Acknowledge Time
۲	*	0	1	Minor	192.168.21.72_72	Location_Bheil1_stot16_Port4_OTUk	OTU_BDI	Communication	Set	2019/02/27 01:22:20	Acknowledge	root	2019/02/27 10:09:54
	× _	0	2	Critical	192.168.21.72_72	Location_Shelf1_Slot17_Port4_OTUk	OTU_LOF	Communication	Set	2019/02/26 21:34:19	Acknowledge	root	2019/02/27 10:09:58
	~	0	3	Minor	192.168.21.72_72	Location_Shelf1_Slot9_Port4_ODU4(0)	ODU_OCI	Communication	Set	2019/02/26 19:48:16	Acknowledge	root	2019/02/27 10:10:01
۲	~	0	4	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port3_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
	~	0	5	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port1_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
۲	~	0	6	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port4_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
	*	0	7	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port2_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
	*	0	8	Minor	192.168.21.72_72	Location_Shelf1_Slot12_Port1_ODU4(0)	ODU_OCI	Communication	Set	2019/02/26 19:47:29	Unacknowledge		
	*	0	9	Critical	192.168.21.72_72	Location_Shelf1_Slot12_Port1_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:47:26	Unacknowledge		

Figure 8-7 Cancel Confirmation of Current Alarm

Show 2	5 • entries									Acknowledge Unacknowle	idge Filter All <mark>Refres</mark> t	Search	t: Search
(B 11	Operation 11	Detail	Number	Severity 11	NE []	Alarm Source	Alarm Name	Alarm Type	State 11	Raised Time	Acknowledge State	Acknowledge User	Acknowledge Time
	*	0	1	Minor	192.168.21.72_72	Location_Shelf1_Slot16_Port4_OTUk	OTU_BDI	Communication	Set	2019/02/27 01:22:20	Acknowledge	root	2019/02/27 10:09:54
8	*	0	2	Critical	192.168.21.72_72	Location_Shelf1_Slot17_Port4_OTUk	OTU_LOF	Communication	Set	2019/02/26 21:34:19	Acknowledge	root	2019/02/27 10 09 58
8	*	0	3	Minor	192.168.21.72_72	Location_Shelf1_Slot9_Port4_ODU4(0)	ODU_OCI	Communication	Set	2019/02/26 19 48:16	Acknowledge	root	2019/02/27 10:10:01
	*	0	4	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port3_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
۲	*	0	5	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port1_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
8	*	0	6	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port4_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
	*	0	7	Critical	192 168 21.72_72	Location_Shelf1_Slot9_Port2_Pluggable	Pluqqable Missing	Equipment	Set	2019/02/26 19:48:14	Acknowledge	root	2019/02/27 10:08:45
٠	4	0	8	Minor	192.168.21.72_72	Location_Shelf1_Slot12_Port1_ODL	Are you sure to perform	this operation?	Set	2019/02/26 19.47.29	Unacknowledge		
8	4	0	9	Critical	192 168 21 72 72	Location_Shelf1_Slot12_Port1_Plug			Set	2019/02/26 19:47:26	Unacknowledge		
8	4	0	10	Minor	192.168.21.72_72	Location_Shelf1_Slot16_Port9_ODL	Appl	Cancel	Set	2019/02/26 16:39:53	Unacknowledge		

Figure 8-8 Cancel Confirmation

Show 2	5 v entries									Acknowledge Unacknowl	odge Filler All <mark>Refres</mark> t	Search	Search
0 11	Operation 11	Detail	Number	Severity 11	NE II	Alarm Source	Alarm Name 11	Alarm Type 11	State 11	Raised Time	Acknowledge State	Acknowledge User 11	Acknowledge Time
۵	4	0	1	Minor	192.168.21.72_72	Location_Shelf1_Slot16_Port4_OTUk	OTU_BDI	Communication	Set	2019/02/27 01:22:20	Unacknowledge		
۵	<i>d</i> ,	0	2	Critical	192.168.21.72_72	Location_Shelf1_Slot17_Port4_OTUk	OTU_LOF	Communication	Set	2019/02/26 21:34:19	Unacknowledge		
۵	4	0	3	Minor	192.168.21.72_72	Location_Shelf1_Slot9_Port4_ODU4(0)	ODU_OCI	Communication	Set	2019/02/26 19:48:16	Unacknowledge		
۵	4	0	4	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port3_Pluggable	Pluggable_Missing	Equipment.	Set	2019/02/26 19:48:14	Unacknowledge		
۵	4,	0	5	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port1_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/25 19:48:14	Unacknowledge		
8	4	0	6	Critical	192.168.21.72_72	Location_Shelf1_Slot9_Port4_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 19:48:14	Unacknowledge		
0	4	0	7	Critical	192.168.21.72_72	Location_Sheif1_Slot9_Port2_Pluggable	Pluqoable Missing	Equipment	Set	2019/02/26 19:48:14	Unacknowledge.		
۵	4	0	8	Minor	192.168.21.72_72	Location_Shelf1_Slot12_Port1_ODU4(0)	 Success! 	on	Set	2019/02/25 19:47:29	Unacknowledge		
0	4	0	9	Critical	192.168.21.72_72	Location_Shelf1_Slot12_Port1_Pluggable			Set	2019/02/25 19:47:25	Unacknowledge		
0	4	0	10	Minor	192.168.21.72_72	Location_Shelf1_Slot16_Port9_ODU2(0)		Apply on	Set	2019/02/26 16:39:53	Unacknowledge		

Figure 8-9 Complete Confirmation Cancellation of Current Alarm

• The function of "Filter" 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.

Filte	r Conditio	ons									
IP				192.168.21.72	Ŧ	Slot				All	•
Port					•					All 1	÷
Rais	sed Time Fro	om:				Raised Time	To:			2	
Clea	ared Time Fr	rom:				Cleared Tim	e To:			4 5 6	
Sev	erity:	Major			Vinor				Warning	7 8	
		Critica	al							9 10	
Ack	nowledge	Ackno	wiedge	Unacknowledg	je					11 12	
5181	e									13 14 15	
(-	MINOF	192.168.126.1 126	Location Shell'I Sidt Ports ODU4(0)			Communication	Set	2000/02/27 11:0	16	- 1 k
0	8	Minor	192.168.126.1_126	Location_Shelf1_Slot1_Port8_ODU4(0)	ODU_OCI		Communication	Set	2000/02/27 11:0	18 19	-

Figure 8-10 IP Filter Current Alarm

Filter Conditions	;			×
IP		192.168.21.72	Slot	5 •
Port		All		
Raised Time From:		All 1	Raised Time To:	1
Cleared Time From	ι.	3	Cleared Time To:	
Severity:	Major	Minor	Warning	
	Critical			
Acknowledge State	Acknowledge	Unacknowledge		
				Apply Close

Figure 8-11 Filter Current Alarm for Slots & Ports

Filter Conditions															
IP		192.168.21.72		Ŧ] :	Slot							5		•
Port		2	_	۳						_					
Raised Time From:					1	Raised	I Time	To:							
Cleared Time From:			T	+		二月 <mark>2</mark>	019		•						
Severity: Ma	jor tical	Minor		日 27: 3	- : 28 2 4	二 三 29 30 5 6	四 31 7	五 ; 1 ; 8 ;	六 2 9			Warning			
Acknowledge Ack State	knowledge	Unacknowledge		10 17 24	11 1 18 1 25 2	12 13 19 20 26 27	14 21 28	15 1 22 2 1 :	16 23 2					Apply	Close
S S Minor	192.168.126.1_126 Loc 192.168.126.1_126 Loc	ation_Shelf1_Slot1_Port5_ODU4(0) ODU_		3	4	5 6 今月	7 F	8	9	nt ication	Set	2000/02/28 01.28 2000/02/27 11:04	58 Unacknowledge 10 Unacknowledge		

Figure 8-12 Create Time to Filter Current Alarm

Severity:	Major Critical	Minor	Warning	
Acknowledge State	☑Acknowledge	Unacknowledge		Annly Close

Figure 8-13 Filter Current Alarm According to Alarm Level & Confirmation Status

🕜 Hint

$\label{eq:constraint} The method to filter IP, slot and port is: IP \rightarrow Slot \rightarrow Port or IP \rightarrow Slot or IP. It is not allowed to select slot or port separately.$

• The function of "*All*" button is to show all alarms for all NE devices.

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

The upper-right area of the navigation bar is the search area: By entering specified content, it can get all the alarms that contain that content, as shown in the following figure.

- w	25 V entries								Acknowl	edge Unacknowledge	Filter All Refresh	Search	Portal
11	Operation 11	Detail	Number	Severity 11	NE II	Alarm Source II	Alarm Name 11	Alarm Type	State 11	Raised Time	Acknowledge State 11	Acknowledge User 11	Acknowledge Time
	4	0	1	Critical	192.168.126.1_126	Location_Shelf1_Slot Port9_ET/n	ETY_LOS	Communication	Set	2000/02/28 01:30:25	Unacknowledge		
	4	0	2	Minor	192.168.126.1_126	Location_Shelf1_Slot Port9_ODU4(0)	ODU_OCI	Communication	Set	2000/02/27 11:04:10	Unacknowledge		
	4	0	3	Critical	192.168.21.104_104	Location_Shelf1_Slot*_Port9_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/26 21:23:30	Unacknowledge		
	R.	0	4	Minor	192.168.21.72_72	Location_Shelf1_Slot 6_Port9_ODU2(0)	ODU_OCI	Communication	Set	2019/02/26 16:39:53	Unacknowledge		
	*	0	5	Critical	192.168.21.72_72	Location_Shelf1_Slot 6_Port9_Pluggable	Pluggable_Missing	Equipment	Set	2019/02/22 11:20:36	Unacknowledge		
	4	0	6	Critical	192.168.21.72_72	Location_Shelf1_Slot 7_Port9_Puggable	Pluggable_Missing	Equipment	Set	2019/02/22 11:20:06	Unacknowledge		

Figure 8-14 Search Current Alarm

□ ↓ Dperation ↓↑	Detail Number Severity 1	NE IT	Alarm Source	1 Alarm Name	Alarm Type 🕸	State 11	Raised Time	Acknowledge State 1	Acknowledge User $\downarrow \uparrow$	Acknowledge Time
	I Critical	192.168.126.1_126	Location_Shelf1_Slot1_Port9_ETYn	ETY_LOS	Communication	Set	2000/02/28 01:30:25	Unacknowledge		
NE:	192.168.126.1_126									
Alarm Source:	Location_Shelf1_Slot1_Port9_E	TYn								
Alarm Name:	ETY_LOS									
Probable Cause:	ETY_LOS									
Recommend Measures	: Document Links									
Alarm Type:	Communication									
Severity:	Critical									
State:	Set									
Raised Time:	2000/02/28 01:30:25									
Cleared Time:										
Acknowledge State:	Unacknowledge									
Acknowledge User:										
Acknowledge Time:										

Figure 8-15 Alarm Details

	\leftarrow .	→ C	 loc 	calhost:9090	/alarm	/alarmde	etail.htm	I#FTY I	()	1	ŝ
--	----------------	-----	-------------------------	--------------	--------	----------	-----------	---------	---	---	---	---

Directory

Shelf_Temp_Major Shelf_Temp_Critical EQPT Missing EQPT Mismatch EQPT Power Supply Issue EQPT_Temp_Major EQPT_Temp_Critical EQPT_Comm_Fail EQPT_Latch_Open EQPT_FAN_Critical Pluggable_Missing Pluggable_Fail Pluggable Mismatch Pluggable_TxFail Pluggable_Power_Too_High_Rx Pluggable Power Too Low Rx Pluggable_Power_Too_High_Tx Pluggable Power Too Low Tx Pluggable BiasCurrent Too High Pluggable_BiasCurrent_Too_Low Pluggable_Temp_Too_High Pluggable_Temp_Too_Low Pluggable_Vcc_Too_High

Shelf_Temp_Major

- ProbleCause:
- Shelf inlet Temperature High Recommended Actions:
 - 1. check the environmental temperature of the room, if the temperature is too
 - high, you need to exclude the cooling equipment failure in the room 2. make sure the fan card is working normal otherwise troubleshoot fan faults
 - based on fan alarms

 - 3. make sure that the service card is working normal, otherwise troubleshoot card faults based on fan alarms
 - 4. if the alarm still exists, please contact the maintenance engineer

Shelf_Temp_Critical

- ProbleCause:
- Shelf inlet Temperature too High
- Recommended Actions:
 - 1. check the environmental temperature of the room, if the temperature is too high, you need to exclude the cooling equipment failure in the room • 2. make sure the fan card is working normal,otherwise troubleshoot fan faults
 - based on fan alarms
 - o 3. make sure that the card is working normal, otherwise troubleshoot card faults
 - based on fan alarms
 - · 4. if the alarm still exists, please contact the maintenance engineer

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

Figure 8-16 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, operation, details, serial number, alarm level, NE, alarm source, alarm name, alarm type, status, generation time, clearance time, confirmation status, confirmer and confirmation time.

- 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.
- There is one icon-



in the operation bar. Their functions are the same as the functions of

Confirm and Cancel Confirmation buttons, however, icon buttons in the operation bar are only valid for the alarm on the line.

- You can get the details by clicking icon. After clicking the icon, the alarm will be expanded and the alarm details are displayed. Details include: network element, alarm source, alarm name, alarm reason, recommended measures, alarm type, alarm level, status, generation time, clearance time, confirmation status, confirmer and confirmation time. Among them, the network element, alarm source, alarm name, alarm type, status, generation time, clearance time, confirmer and confirmation status, confirmer and confirmation status, confirmer and confirmation time need to be consistent with the contents of the header. The alarm reason refers to the causes of current alarm. Recommended measures are shown by linked content. After clicking on the "*Document Link*", an alarm document page is generated in a new window of the browser, which can view the possible causes and suggested measures of the alarm, so as to help engineers to troubleshoot problems.
- 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 (light yellow), warning level (blue).
- Network element is the IP of network equipment that generates alarm.
- The alarm source is the specific slot or port information of NE which generates alarm.
- Alarm name, alarm type, status, generation time, clearance time, confirmation status, confirmer and confirmation time are relatively simple, we will not go into much detail here.

8.2.2. History Alarm

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

2	} ••	Hon	ne System Mana	agement Configur	ation Management	ault Management	Performar	nce Manageme	ent Security Manageme	nt Log Management	OLP Route		
											≽122 (77 🕜28 😋17	o root
Show	25	entries										Filter All	Delete ALL Export
	Detail	Number	NE	Alarm Source	Alarm Name	Alarm Type	Severity	State	Raised Time	Cleared Time	Acknowledge State	Acknowledge User	Acknowledge Time
	0	1	192.168.126.1	Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:25:20	2000/02/28 02:25:20	Acknowledge	Auto Acknowledge	2019/02/27 10:35:02
	0	2	192.168.126.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:25:19	2000/02/28 02:25:19	Acknowledge	Auto Acknowledge	2019/02/27 10:35:02
	0	3	192.168.126.1	Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:24:17	2000/02/28 02:24:17	Acknowledge	Auto Acknowledge	2019/02/27 10:35:01
	0	4	192.168.126.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:25:05	2000/02/28 02:25:05	Acknowledge	Auto Acknowledge	2019/02/27 10:34:52
	0	5	192.168.126.1	Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:24:46	2000/02/28 02:24:46	Acknowledge	Auto Acknowledge	2019/02/27 10:34:48
	0	6	192.168.126.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:23:43	2000/02/28 02:23:43	Acknowledge	Auto Acknowledge	2019/02/27 10:34:39
	0	7	192.168.126.1	Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:23:32	2000/02/28 02:23:32	Acknowledge	Auto Acknowledge	2019/02/27 10:34:14
	0	8	192.168.126.1	Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:23:45	2000/02/28 02:23:45	Acknowledge	Auto Acknowledge	2019/02/27 10:33:36
	0	9	192.168.126.1	Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:22:59	2000/02/28 02:22:59	Acknowledge	Auto Acknowledge	2019/02/27 10:33:18
	0	10	192.168.126.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:23:08	2000/02/28 02:23:08	Acknowledge	Auto Acknowledge	2019/02/27 10:33:15
	0	11	192.168.126.1	Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:22:59	2000/02/28 02:22:59	Acknowledge	Auto Acknowledge	2019/02/27 10:33:05

Figure 8-17 History Alarm

The left area of the navigation bar can filter the number of alarms displayed on the current page, and the number of displayed alarms per page can be adjusted to 25, 50, 75 and 100.

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

- Functions of "Filter" and "All" 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.

how	25	• entrie	es											Delete Delete ALL E
5	Detail	Na	mber	NE	Alarm Source	Alarm Name	Alarm Type	Sevenity	State	Raised Time	Cleared Time	Acknowledge State	Acknowledge User	Acknowledge Tim
	0	1	1	92.168.126.1	Sheif1_Slot4	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:25:20	2000/02/28 02:25:20	Acknowledge	Auto Acknowledge	2019/02/27 10:35:02
	0	2	1	92.168.126.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:25:19	2000/02/28 02:25:19	Acknowledge	Auto Acknowledge	2019/02/27 10:35:02
	0	3	1	92.168.126.1	Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:24:17	2000/02/28 02:24:17	Acknowledge	Auto Acknowledge	2019/02/27 10:35:01
	0	4	1	92.168.126.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:25:05	2000/02/28 02:25:05	Acknowledge	Auto Acknowledge	2019/02/27 10:34:5
	0	5	1	92.168.126.1	Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:24:46	2000/02/28 02:24:46	Acknowledge	Auto Acknowledge	2019/02/27 10:34:4
	0	6	1	92.168.126.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:23:43	2000/02/28 02:23:43	Acknowledge	Auto Acknowledge	2019/02/27 10:34:3
	0	7	1	92.168.126.1	Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:23:32	2000/02/28 2 23:32	Acknowledge	Auto Acknowledge	2019/02/27 10:34:1
	0	8	1	92.168.126.1	Sheif1_Slot5	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:23:45	29 0 02/28 02:23:45	Acknowledge	Auto Acknowledge	2019/02/27 10:33:3
	0	9	1	92.168.126.1	Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02 22 59	2000/02/28 02:22:59	Acknowledge	Auto Acknowledge	2019/02/27 10:33 1
	0	10	1	92.168.128.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	C A		B	2000/02/28 02:23:08	Acknowledge	Auto Acknowledge	2019/02/27 10:33
	0	11	1	92.168.126.1	Shelf1_Slot4	EQPT_FAN_Critical	Equipment	C A	Jo you want to c	elete these data?	2000/02/28 02:22:59	Acknowledge	Auto Acknowledge	2019/02/27 10:33:0
	0	12	1	92.168.126.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	C	10	Cascal	2000/02/28 02:23:00	Acknowledge	Auto Acknowledge	2019/02/27 10:32:4
	0	13	1	92.168.126.1	Shelf1_Slot5	EQPT_FAN_Critical	Equipment	C	- AP	Cancer 7	2000/02/28 02:22:47	Acknowledge	Auto Acknowledge	2019/02/27 10:32:3
	0	14	1	92.168.126.1	Shelt1_Slot4	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:21:54	2000/02/28 02:21:54	Acknowledge	Auto Acknowledge	2019/02/27 10:32:3
	0	15	1	92.168.126.1	Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:22:31	2000/02/28 02:22:31	Acknowledge	Auto Acknowledge	2019/02/27 10:32.1
	0	16	1	92.168.126.1	Shelf1_Slot3	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:22:09	2000/02/28 02:22:09	Acknowledge	Auto Acknowledge	2019/02/27 10:32
	0	17	1	92.168.126.1	Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:22:01	2000/02/28 02:22:01	Acknowledge	Auto Acknowledge	2019/02/27 10:31
	0	18	1	92.168.126.1	Shelf1_Slot5	EQPT_FAN_Critical	Equipment	Critical	Auto clear.	2000/02/28 02:21:31	2000/02/28 02:21:31	Acknowledge	Auto Acknowledge	2019/02/27 10:31:3
	0	19	्य	92.168.126.1	Shelf1_Slot4	EQPT_FAN_Critical	Equipment	Critical	Auto clear	2000/02/28 02:21:29	2000/02/28 02:21:29	Acknowledge	Auto Acknowledge	2019/02/27 10:31:2
4	22							CONTRACTOR NO.	A CONTRACTORS					

Figure 8-18 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, it will prompt to save the path. The exported data is saved in Excel format.

				-		Eliston Alarm				
25	entries			FileName		Printing-Asianni		pply Close		
								Time		
0			EGPT_FAN_Critical		Critical	Auto clear				
0			EGPT_FAN_Critical		Critical	Auto clear				
0			EOPT_FAN_CRICIN		Critical	Auto clear				
0			EGPT_FAN_Critical		Critical	Auto clear				
0			EQPT_FAN_Critical		Critical	Auto clear				
0			EQPT_FAN_Critical		Critical	Auto clear				
0					Critical	Auto clear				
0					Cubeal	Auto clear	2000/02/28 02 23:45			
0			EQPT_FAN_Critical		1. Sugar		10 (220) 20 (20) (20) (20) (20)			
0			EGPT_FAN_Critical		 Exp 	ort all datas succe	essiThe file is stored in			
0					the report	_out directory of	the installation director			
0					2.					
0							Apply			
0							obba			
0					Critical	Auto clear				
0			EQPT_FAN_Critical		Critical	Auto clear				
0					Critical	Auto clear				

Figure 8-19 Export History Alarm

🕜 Hint

The path to save the data is: NMS Installation Root Directory \rightarrow report_out Folder \rightarrow historyAlarm Folder \rightarrow File Name.xls.

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

8.3. Alarm Configuration

8.3.1. Alarm Configuration

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

Alarm Configuration		x
Show 10 • entries		Search: Search
Alarm Name 🕼	Alarm Severity Configuration	Alarm Shielding Configuration
TCA_UAS	Major 🔻	No 🔻
TCA_SES	Major 🔻	No 🔻
TCA_ES	Major 🔻	No v
TCA_BBE	Major 🔻	No 🔻
SW_STORAGE_FULL	Major 🔻	No 🔻
SW_MISMATCH	Major •	No 🔻
SW_MIB_MISMATCH	Major v	No 🔻
SW_MIB_FAIL	Major 🔻	No 🔻
SW_DOWNLOAD_FAIL	Major v	No 🔻
SNR_Abnormal	Critical	No v
Showing 1 to 10 of 141 entries	Previous 1 2	2 3 4 5 15 Next
		Apply

Figure 8-20 Alarm Configuration

The left area of the alarm configuration can filter the number of alarms displayed on the current page, and the number of displayed alarms per page can be adjusted to 10, 25, 50 and 100.



Figure 8-21 Number of Alarms Displayed in Alarm Configuration

The right 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.

Alarm Configuration		
Show 10 • entries		Search: mismatch
Alarm Name	Alarm Severity Configuration	Alarm Shielding Configuration
SW_MISMATCH	Major 🔻	No 🔻
SW_MIB_MISMATCH	Major 🔻	No 🔻
Pluggable_Mismatch	Major 🔻	No 🔻
EQPT_Mismatch	Major 🔻	No 🔻
Showing 1 to 4 of 4 entries filtered from 141 total ent	ries	Previous 1 Next
		Apply

Figure 8-22 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.)

8.3.2. Alarm Notification Configuration

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

= • 🗸	alarm	Notice	Configu	ratior
-------	-------	--------	---------	--------

- Critical
- Major
- 🗉 🔄 🦲 Warning

A	n	n	1
	М	μ	ı y

Figure 8-23 Alarm Notification Configuration

🕜 Hint

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

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

8.3.3. **Alarm Mailbox Server configuration**

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

Alarm Mailbox Server Co	onfiguration	×
send_name	send_name	
Email Authorization Code	Email Authorization Code	
send_user	send_user	
value_smtp	value_smtp	
value_smtp_port	25	
SSL		
	Apply	

Figure 8-24 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.

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

🕜 Hint

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

8.3.4. **Enable the Alarm Sound**

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



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).

9. Performance Management

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

9.1. Performance Management Introduction

9.1.1. Filter Box

Click on "Performance Management" and select "Performance Monitoring Point Management", then click on "Performance Monitoring Point Management", as shown in the figure below:

• 🥩	Home System Management Configuration M	lanagement Fault Management Performan	ce Management Security Managemen	nt Log Mana	igement OLP	Route
			≽ 59 0 51	0 6	02	0 root
NE 192.168.21.72	Slot ALL Port ALL	PM Granularity 15min	PMP Status ALL	• Apply		
Show 25 • ent	ries		Enable PMP Disable PMP Enable TCA	Disable TCA	Search: Sea	irch
	Name 11	PMP Status	TCA Status		Operat	e
	192.168.21.72_Slot5_Port1_OCh_Ingress_NearEnd	Enabled PMP			Disable	PMP
	192.168.21.72_Slot5_Port1_Optical_Ingress_NearEnd	Enabled PMP			Disable	PMP
0	192.168.21.72_Slot5_Port1_Optical_Egress_NearEnd	Enabled PMP			Disable	PMP
	192.168.21.72_Slot5_Port1_OTU_Ingress_NearEnd	Enabled PMP	Disabled TCA		Disable PMP	Enable TCA
	192.168.21.72_Slot5_Port1_OTU_Ingress_FarEnd	Enabled PMP	Disabled TCA		Disable PMP	Enable TCA
	192.168.21.72_Slot5_Port1_OTU-FEC_Ingress_NearEnd	Enabled PMP			Disable	PMP
	192.168.21.72_Slot5_Port1_ODU4(1)_Ingress_NearEnd	Enabled PMP	Disabled TCA		Disable PMP	Enable TCA
	192.168.21.72_Slot5_Port1_ODU4(1)_Ingress_FarEnd	Enabled PMP	Disabled TCA		Disable PMP	Enable TCA
	192.168.21.72_Slot5_Port1_ODU4(2)_Ingress_NearEnd	Enabled PMP	Disabled TCA		Disable PMP	Enable TCA

Figure 9-1 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 "*Apply*" at the upper right corner, as shown in the figure below.

•	Home	System Management	Configuration Management	Fault Manager	ment P	erformance Mar	nagement	Security M	lanagement	Log Mana	gement (OLP Route	
								≽56	6 48	€ 6	02	@ 0	root
NE Please Select	▼ Slot		• Port	 PM Granularity 	/ 15min	٣	PMP Status	5 ALL	,	Apply			
Show 25 • entries						En	able PMP	Disable PMP	Enable TCA	Disable TCA	Search:	Search	
		Name 4	† PMP S	tatus			TCA	Status			Op	perate	
				No data	available in	n table							
Showing 0 to 0 of 0 entries	5											Previou	s Next

Figure 9-2 Show Monitoring Management Information

9.1.2. Performance Monitoring Point Introduction

- The performance monitoring point is determined by monitoring point ID, monitoring point location, monitoring point direction and monitoring cycle.
- Performance monitoring point location: far end and near end (for OTUk and ODUk).
- Near-end monitoring point: according to received BIP8.
- Far-end monitoring point: according to received BEI.
- The direction of performance monitoring points: ingress and egress.
- Monitoring Cycle: 15 minutes, 24 hours.

9.1.3. Enable Performance Monitoring Point

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

	• 🥩	Home System Management Configuration N	lanagement Fault Management Performance	e Management Security Management	Log Mana	gement O	LP Route	
				<u>≽</u> 59 ₿ 51	<u>0</u> 6	02	@0 root	
1	NE 192.168.21.72	Slot ALL Port ALL	PM Granularity 15min	PMP Status ALL	Apply			
ŝ	Show 25 • ent	ries		Enable PMP Disable PMP Enable TCA	Disable TCA	Search:	Search	
		Name 🕴	PMP Status	TCA Status		Ope	erate 👘	
		192.168.21.72_Slot5_Port1_OCh_Ingress_NearEnd	Enabled PMP			Disa	able PMP	
		192.168.21.72_Slot5_Port1_Optical_Ingress_NearEnd	Enabled PMP			Disa	able PMP	
		192.168.21.72_Slot5_Port1_Optical_Egress_NearEnd	Enabled PMP			Disa	able PMP	
		192.168.21.72_Slot5_Port1_OTU_Ingress_NearEnd	Enabled PMP	Disabled TCA		Disable PMF	Enable TCA	
		192.168.21.72_Slot5_Port1_OTU_Ingress_FarEnd	Enabled PMP	Disabled TCA		Disable PMF	P Enable TCA	
		192.168.21.72_Slot5_Port1_OTU-FEC_Ingress_NearEnd	Enabled PMP			Disa	able PMP	
		192.168.21.72_Slot5_Port1_ODU4(1)_Ingress_NearEnd	Enabled PMP	Disabled TCA		Disable PMF	P Enable TCA	
		192.168.21.72_Slot5_Port1_ODU4(1)_Ingress_FarEnd	Enabled PMP	Disabled TCA		Disable PMF	P Enable TCA	
		192.168.21.72_Slot5_Port1_ODU4(2)_Ingress_NearEnd	Enabled PMP	Disabled TCA		Disable PMF	Enable TCA	

Figure 9-1 Enable Monitoring Points

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

R	Home System Management Configuration Management	Fault Management	Performance Managem	ent Security Managemen	nt Log Managem	ent OLP Route	
				≽ 101 0 66	() 8 ()2:	2 @5	root
NE 1	92.168.21.72 • Slot ALL • Port ALL •	PM Granularity 15min	n 🔻 PMP S	tatus ALL	• Apply		
Show	100 v entries		Enable PMP	Disable PMP Enable TCA	Disable TCA S	earch: Search	
Ø	Name		PMP Status	TCA Status		Operate	
Ø	192.168.21.72_Slot3_Port1_Optical_Ingress_NearEnd		Disabled PMP			Enable PMP	
	192.168.21.72_Slot3_Port1_Optical_Egress_NearEnd		Disabled PMP			Enable PMP	
	192.168.21.72_Slot3_Port1_Ethernet_Ingress_NearEnd		PMP			Enable PMP	
×	192.168.21.72_Slot3_Port1_Ethernet_Egress_NearEnd	A Failure!	PMP			Enable PMP	
	192.168.21.72_Slot3_Port1_ODU2e(0)_Egress_NearEnd		Apply	Disabled TCA	Enab	le PMP Enable TCA	4
	192.168.21.72_Slot3_Port1_ODU2e(0)_Egress_FarEnd	_	PMP	Disabled TCA E		e PMP Enable TCA	4
I192.168.21.72_Slot3_Port2_Optical_Ingress_NearEnd			Disabled PMP			Enable PMP	
	192.168.21.72. Slot3. Port2. Ontical Europe NearEnd		Disabled PMP			Enable DMD	

Figure 9-2 Operation Failure

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

			*	03 🚺 05	V V	2		1001	
NE 192.168.21.72	Slot 7 Port ALL	PM Granularity 15min	PMP Status ALL	•	Apply				
Show 25 ren	tries		Enable PMP Disable PM	MP Enable TCA Dis	sable TCA S	Search: s	earch		
	Name 11	PMP Status	TCA St	atus		Oper	ate		
	192.168.21.72_Slot7_Port1_OCh_Ingress_NearEnd	Disabled PMP				Enab	le PMP		
	192.168.21.72_Slot7_Port1_Optical_Ingress_NearEnd	Disabled PMP				Enabl	le PMP		
	192.168.21.72_Slot7_Port1_Optical_Egress_NearEnd	Disabled PMP				Enab	le PMP		
	192.168.21.72_Slot7_Port1_OTU_Ingress_NearEnd		Disable	ed TCA	E	nable PMP	Enable	TCA	
	192.168.21.72_Slot7_Port1_OTU_Ingress_FarEnd	Successi	Disable	Disabled TCA		nable PMP	Enable	Enable TCA	
	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearEnd	Apply				Enab	le PMP		
	192.168.21.72_Slot7_Port2_Optical_Ingress_NearEnd	Disabled PMP				Enab	le PMP		
	192.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	Disabled PMP				Enab	le PMP		
	192.168.21.72_Slot7_Port2_ODU4(0)_Egress_NearEnd	Disabled PMP	Disable	ed TCA	E	nable PMP	Enable	TCA	

Figure 9-3 Enable A Single Monitoring Point
To realize batch enabling operations on multiple pieces of data, you can select the previous multiple checkboxes, then click the button on the table (Enable Performance Monitoring) to enable the monitoring of selected performance, as shown in the figure below:

NE	192.168.21.72	Slot 7 Port ALL	PM Granularity 15min	• PMP	Status ALL	* Apply			
Show	25 • er	ntries		Enable PM	P Disable PMP Enable TCA	Disable TCA	Search: Sea	arch	
	×	Name	PMP Status		TCA Status		Opera	le	
	R	192.168.21.72_Slot7_Port1_OCh_Ingress_NearEnd	Enabled PMP				Disable	PMP	
	2	192.168.21.72_Slot7_Port1_Optical_Ingress_NearEnd	Disabled PMP				Enable	PMP	
	2	192.168.21.72_Slot7_Port1_Optical_Egress_NearEnd	Disabled PMP				Enable	PMP	
	ø	192.168.21.72_Slot7_Port1_OTU_Ingress_NearEnd			Disabled TCA		Enable PMP	Enable TCA	
		192.168.21.72_Slot7_Port1_OTU_Ingress_FarEnd	Are you sure you want to operate the	se data?	Disabled TCA		Enable PMP	Enable TCA	
	2	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearEnd	Apply	Cancel			Enable	PMP	
		192.168.21.72_Slot7_Port2_Optical_Ingress_NearEnd	Disabled PMP				Enable	PMP	
		192.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	Disabled PMP				Enable	PMP	
	2	192.168.21.72_Slot7_Port2_ODU4(0)_Egress_NearEnd	Disabled PMP		Disabled TCA		Enable PMP	Enable TCA	
		192.168.21.72_Slot7_Port2_ODU4(0)_Egress_FarEnd	Disabled PMP		Disabled TCA		Enable PMP	Enable TCA	
	8	192.168.21.72_Slot7_Port3_OCh_Ingress_NearEnd	Disabled PMP				Enable	PMP	

Figure 9-4 Batch Enabling Monitoring Point

Select multiple enabled performance monitoring, then select *Enable Performance Monitoring* at the upper right corner, click OK, it will display "There is no modification", as shown in the figure below.

NE 192.168.21.72	NE 192.168.21.72 • Slot 7 • Port ALL • PM Granularity 15min • PMP Status ALL • Apply										
Show 25 • en	tries	Enable PMP Disable PMP Enable TCA Disable	e TCA S	earch: Search							
×	Name 🎼	PMP Status	TCA Status		Operate						
۲	192.168.21.72_Slot7_Port1_OCh_Ingress_NearEnd	Enabled PMP			Disable PMP						
۲	192.168.21.72_Slot7_Port1_Optical_Ingress_NearEnd	Enabled PMP			Disable PMP						
۲	192.168.21.72_Slot7_Port1_Optical_Egress_NearEnd	Enabled PMP			Disable PMP						
ø	192.168.21.72_Slot7_Port1_OTU_Ingress_NearEnd		Disabled TCA	Dis	able PMP Ena	ble TCA					
۲	192.168.21.72_Slot7_Port1_OTU_Ingress_FarEnd	A Not Modified!	Disabled TCA	Dis	able PMP Ena	ble TCA					
ø	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearEnd	Apply			Disable PMP						
Ø	192.168.21.72_Slot7_Port2_Optical_Ingress_NearEnd	Enabled PMP			Disable PMP						
	192.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	Enabled PMP			Disable PMP						

Figure 9-5 No Modification of Monitoring Point Status

9.1.4. Disable Performance Monitoring Point

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

NE 192.168.21.72	Slot 7 Port ALL	PM Granularity 15min	PMP Status ALL Ap	ply	
Show 25 v en	tries		Enable PMP Disable PMP Enable TCA Disable	le TCA Search:	Search
	Name 11	PMP Status	TCA Status	Op	perate 11
	192.168.21.72_Slot7_Port1_OCh_Ingress_NearEnd	Disabled PMP		E	nable PMP
	192.168.21.72_Slot7_Port1_Optical_Ingress_NearEnd	Disabled PMP		E	nable PMP
	192.168.21.72_Slot7_Port1_Optical_Egress_NearEnd	Disabled PMP		E	nable PMP
	192.168.21.72_Slot7_Port1_OTU_Ingress_NearEnd	Disabled PMP	Disabled TCA	Enable PM	IP Enable TCA
	192.168.21.72_Slot7_Port1_OTU_Ingress_FarEnd	Disabled PMP	Disabled TCA	Enable PM	IP Enable TCA
	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearEnd	Disabled PMP		E	nable PMP
	192.168.21.72_Slot7_Port2_Optical_Ingress_NearEnd	Disabled PMP		E	nable PMP
	192.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	Disabled PMP		E	nable PMP
	192.168.21.72_Slot7_Port2_ODU4(0)_Egress_NearEnd	Disabled PMP	Disabled TCA	Enable PN	IP Enable TCA
	192.168.21.72_Slot7_Port2_ODU4(0)_Egress_FarEnd	Disabled PMP	Disabled TCA	Enable PN	IP Enable TCA

Figure 9-6 Disable Monitoring Point

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

NE 192.168.21.72	192.168.21.72 • Slot 7 • Port ALL • PM Granularity 15mm • PMP Status ALL • Appy											
Show 25 ren	tries			Enable PMP Disable PMP Enable	TCA Disable TCA	Searc	h: Search					
	Name Iî	PMP Status		TCA Status			Operate					
	192.168.21.72_Slot7_Port1_OCh_Ingress_NearEnd	Disabled PMP					Enable PN	/IP				
	192.168.21.72_Slot7_Port1_Optical_Ingress_NearEnd	Enabled PMP					Disable PN	ИР				
	192.168.21.72_Slot7_Port1_Optical_Egress_NearEnd	Enabled PMP					Disable PN	ИР				
	192.168.21.72_Slot7_Port1_OTU_Ingress_NearEnd			Disabled TCA		Disable	PMP E	inable TCA				
	192.168.21.72_Slot7_Port1_OTU_Ingress_FarEnd	✓ Success!		Disabled TCA		Disable	PMP E	nable TCA				
	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearEnd	A	pply				Disable PN	ИР				
	192.168.21.72_Slot7_Port2_Optical_Ingress_NearEnd	Enabled PMP					Disable PN	ИР				

Figure 9-7 Disable A Single Monitoring Point

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

NE 192.168.21.72	2 Slot 7 Port ALL	PM Granularity 15min	* PMP	Status ALL	* Apply			
Show 25 + e	entries		Enable PM	Disable PMP Enable TCA	Disable TC	A Sean	ch: Sean	.h
8	Name	PMP Status		TCA Status			Operate	
8	192.168.21.72_Slot7_Port1_OCh_Ingress_NearEnd	Disabled PMP					Enable P	MP
2	192.168.21.72_Slot7_Port1_Optical_Ingress_NearEnd	Disabled PMP					Enable P	MP
8	192.168.21.72_Slot7_Port1_Optical_Egress_NearEnd	Disabled PMP					Enable P	MP
×	192.168.21.72_Slot7_Port1_OTU_Ingress_NearEnd			Disabled TCA		Enabl	e PMP	Enable TCA
8	192.168.21.72_Slot7_Port1_OTU_Ingress_FarEnd	Are you sure you want to operate these	data?	Disabled TCA		Enable	e PMP	Enable TCA
8	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearEnd	Apply	ancel				Enable P	MP
8	192.168.21.72_Slot7_Port2_Optical_Ingress_NearEnd	Disabled PMP					Enable P	MP
8	192.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	Disabled PMP					Enable P	MP
R	192.168.21.72_Slot7_Port2_ODU4(0)_Egress_NearEnd	Disabled PMP		Disabled TCA		Enable	e PMP	Enable TCA
8	192.168.21.72_Slot7_Port2_ODU4(0)_Egress_FarEnd	Disabled PMP		Disabled TCA		Enable	e PMP	Enable TCA

Figure 9-8 Disable Batch Monitoring Points

Select multiple disabled performance monitoring, then select *Disable Performance Monitoring* at the upper right corner, click OK, it will display "There is no modification", as shown in the figure below.

NE 192.168.21	1.72 • Slot 7 • Port ALL	PM Granularity 15min	PMP Status ALL AL	ply	
Show 25	• entries		Enable PMP Disable PMP Enable TCA Disab	e TCA Search: Se	iarch
2	Name 17	PMP Status	TCA Status	Opera	ite I1
8	192.168.21.72_Slot7_Port1_OCh_Ingress_NearEnd	Disabled PMP		Enable	PMP
8	192.168.21.72_Slot7_Port1_Optical_Ingress_NearEnd	Disabled PMP		Enable	PMP
ø	192.168.21.72_Slot7_Port1_Optical_Egress_NearEnd	Disabled PMP		Enable	PMP
8	192.168.21.72_Slot7_Port1_OTU_Ingress_NearEnd		Disabled TCA	Enable PMP	Enable TCA
8	192.168.21.72_Slot7_Port1_OTU_Ingress_FarEnd	Not Modified!	Disabled TCA	Enable PMP	Enable TCA
8	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearEnd	Apply		Enable	PMP
8	192.168.21.72_Slot7_Port2_Optical_Ingress_NearEnd	Disabled PMP		Enable	PMP
8	192.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	Disabled PMP		Enable	PMP
8	192.168.21.72_Slot7_Port2_ODU4(0)_Egress_NearEnd	Disabled PMP	Disabled TCA	Enable PMP	Enable TCA
8	192.168.21.72_Slot7_Port2_ODU4(0)_Egress_FarEnd	Disabled PMP	Disabled TCA	Enable PMP	Enable TCA

Figure 9-11 No Modification of Monitoring Point Status

9.1.5. Attentions for Monitoring Performance

- When monitoring points are enabled, they will be disabled in several cases:
 - (1) Manually disable a single monitoring point or batch monitoring points.
 - (2) After the module mode is switched, all the 15-minute and 24-hour monitoring points of the port are automatically disabled.

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

9.2. Current Performance Statistics

Click on "Current Performance Statistics", you can find the following performance statistics at the right side:

--current performance statistics of optical power

--current performance statistics of OCh

--current performance statistics of FEC

--current performance statistics of OUT/ODU

--current performance statistics of SDH regeneration segment

--current performance statistics of Ethernet

As shown in the figure below:

Filter	r Conditio	INS	Contiguration ivia		normanice manauc	anchi occu	пи манадетен	LUU WZ	inductrient O	LE IXUUC		×
IP				192.168.21.72	Ŧ	Slot				All		•
Port	Port				٣				All 1		-	
Raised Time From:						Raised Time To:				2		
Cleared Time From:					Cleared Time To:				4			
Seve	Severity:				Minor				7 Warning 8			
		Critica	al						, in the second s	9 10		
Ackr	nowledge	Ackno	owledge	Unacknowled	ge					11 12		
State	e									13 14		
•		NIIDO	197 168 176 1 176	Location Shell's Sign Ports Outlaten			Communication	Set	2000/02/27 11:0	15 16		
0	8	Minor	192.168.126.1_126	Location_Shelf1_Slot1_Port8_ODU4(0)	ODU_OCI		Communication	Set	2000/02/27 11:0	18 19		-



9.2.1. Monitoring of Optical Power

9.2.1.1. Introduction of Optical Power Monitoring Parameters

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



NE Please Select Slot	▼ Port	• PM G	Granularity 15min	• Refresh				
Show 10 r entries						Reset	Search: Search	
□ Name ↓↑ MaxPower ↓↑ MaxPower Threshold ↓	MaxPower Stamp 1	MinPower 1	MinPower Threshold $\downarrow\uparrow$	MinPower Stamp 1	AvgPower 1	Suspect Interval Flag 1	Elapsed Time $\downarrow\uparrow$	Threshold O
No data available in table								
howing 0 to 0 of 0 entries Next								

Figure 9-13 Display Monitoring Parameters

9.2.1.2. View Optical Power Monitoring Information

Select the appropriate network elements, slots, ports and monitoring cycle through the selection box above the menu, the optical power value of a certain network element/slot/port will be displayed. Optical power includes two monitoring points for near-end transmission and near-end reception. Optical module is inserted into the monitoring port. Data of the maximum and minimum optical power and of the corresponding generation timestamp 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.

NE	192.168.21.72 • Slot 7	Port 1	▼ PM Gra	inularity 15min	• Ref	resh						
Show	Show 10 • entries Search: Search											
	Name 41	MaxPower ↓↑	MaxPower Threshold $\downarrow \uparrow$	MaxPower Stamp $\downarrow\uparrow$	$MinPower \downarrow \uparrow$	MinPower Threshold $\downarrow \uparrow$	MinPower Stamp 1	AvgPower ↓↑	Suspect Interval F			
	192.168.21.72_Slot7_Port1_Optical_Ingress_NearEnd	-7.8	0	2019/02/26 14:24:30	-7.9	-20	2019/02/26 14:20:40	-7.8	False			
	192.168.21.72_Slot7_Port1_Optical_Egress_NearEnd	-4.9	0	2019/02/26 14:20:40	-5.0	-20	2019/02/26 14:20:41	-4.9	False			
Show	ring 1 to 2 of 2 entries							Previo	us 1 Next			

Figure 9-14 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.

NE	192.168.21.72 • Slot 7	Port 1	▼ PM Gra	nularity 24h	▼ Ref	resh					
Sho	Show 10 • entries Search: Search.										
	Name I1	MaxPower 1	MaxPower Threshold $\downarrow \uparrow$	MaxPower Stamp $\downarrow\uparrow$	$MinPower \ \downarrow \uparrow \\$	MinPower Threshold $\downarrow\uparrow$	MinPower Stamp $\downarrow\uparrow$	AvgPower 1	Suspect Interval F		
	192.168.21.72_Slot7_Port1_Optical_Ingress_NearEnd	-7.8	0	2019/02/26 14:28:31	-7.9	-20	2019/02/26 14:28:11	-7.8	False		
	192.168.21.72_Slot7_Port1_Optical_Egress_NearEnd	-4.9	0	2019/02/26 14:28:11	-5.0	-20	2019/02/26 14:28:13	-4.9	False		
Sho	Showing 1 to 2 of 2 entries 1 Next										

Figure 9-15 24-Hour Monitoring Point Data of Optical Power

9.2.1.3. Reset Optical Power Monitoring Data

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

NE 1	92 168 21 72 • Slot	7	Port	• PM Gra	anularity 24h	• Re	efresh			
Show	10 • entries							Reset	Search: Search	
wer 11	MaxPower Threshold	MaxPower Stamp	MinPower 1	MinPower Threshold	MinPower Stamp	AvgPower II	Suspect Interval Flag	Elapsed Time 41	Threshold Operate	Operate 1
.8	0	2019/02/26 14:28:31	-7.9	-20	2019/02/26 14:28:11	-7.8	False	30	Modify Threshold	Reset
.9	0	2019/02/26 14:28:11	-5.0	-20	2019/02/26 14:28:13	-4.9	False	30	Modify Threshold	Reset
Showin	g 1 to 2 of 2 entries			🔺 Are you	sure you want to operate	these data? Cancel			Previous	1 Next

Figure 9-16 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 timestamp and the minimum optical power timestamp 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.

NE 18	12.168.21.72 • Slot	7	Port 1	▼ PM Gra	anularity 24h	* Re	rfresh					
Show	10 • entries							Reset	Search: Search			
wer 11	MaxPower Threshold	MaxPower Stamp 11	MinPower 1	MinPower Threshold	MinPower Stamp	AvgPower 1	Suspect Interval Flag	Elapsed Time 11	Threshold Operate	Operate 11		
0	0	1970/01/01 08:00:00	0.0	-20	1970/01/01 08:00:00	0.0	False	0	Modify Threshold	Reset		
.0	0	1970/01/01 08:00:00	0.0	-20	1970/01/01 08:00:00	0.0	False	0	Modify Threshold	Reset		
Showing	Showing 1 to 2 of 2 entries											
Apply												

Figure 9-17 Successful Reset Operation

9.2.1.4. Optical Power Monitoring Data Shown as NA

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

- (1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.
- (2) Optical module is inserted into the port but it is mismatched and the port is enabled.

At this time, both the maximum and minimum optical power will be shown as NA. The timestamp 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:

NE	192.168.21.72 v Slot 9	Port 1	• PM Gra	nularity 15min	* Ref	iresh				
Sho	w 10 v entries						Reset	Search: Search	h	
	Name 11	MaxPower 1	MaxPower Threshold $\downarrow \uparrow$	MaxPower Stamp $\downarrow \uparrow$	MinPower 1	MinPower Threshold $\downarrow \uparrow$	MinPower Stamp $\downarrow\uparrow$	AvgPower 1	Suspect Interval F	
	192.168.21.72_Slot9_Port1_Optical_Ingress_NearEnd	N/A	0	//:	N/A	-20	/	N/A	False	
	192.168.21.72_Slot9_Port1_Optical_Egress_NearEnd	N/A	0	//::	N/A	-20	/::	N/A	False	
Sho	Previous 1 Next									

Figure 9-18 Optical Module of Optical Power Not in Position

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

(1) When the module is not in position or is pre-configured with an empty slot and the port for the module is enabled, the maximum and minimum optical power will be shown as NA. The timestamp 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.

NE 192.168.21.72 • S	ilot 9	• Port 3	▼ PM G	ranularity 15mi	n • Refre	esh						
Show 10 • entries	Now 10 + entries Reset Search. Search.											
Name 11	MaxPower ↓↑	MaxPower Threshold $\downarrow\uparrow$	MaxPower Stamp $\downarrow \uparrow$	MinPower ↓↑	MinPower Threshold $\downarrow\uparrow$	MinPower Stamp 1	AvgPower 1	Suspect Interval Flag $\downarrow\uparrow$	Elapsed Time 👃			
_Port3_Optical_Ingress_NearEnd	N/A	0	//::	N/A	-20	//::	N/A	False	0			
_Port3_Optical_Egress_NearEnd	N/A	0	/::	N/A	-20	//::	N/A	False	0			
Showing 1 to 2 of 2 entries	owing 1 to 2 of 2 entries 1 Next											

Figure 9-19 Optical Power Monitoring Data

When the module is mismatched and the port for the module is enabled, the maximum and minimum optical power will be shown as NA. The timestamp 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:

NE 192.168.21.72	NE 192.168.21.72 Slot 9 Port 2 PM Granularity 15min Refresh											
Show 10 • entries	W 10 • entries Reset Search. Search.											
Name J†	MaxPower 1	MaxPower Threshold $\downarrow\uparrow$	MaxPower Stamp 1	MinPower $\downarrow \uparrow$	MinPower Threshold $\downarrow\uparrow$	MinPower Stamp 1	AvgPower 1	Suspect Interval Flag $\downarrow\uparrow$	Elapsed Time 1			
Port2_Optical_Ingress_NearEnd	N/A	0	//::	N/A	-20	//::	N/A	False	426			
Port2_Optical_Egress_NearEnd	Dical_Egress_NearEnd N/A 0 N/A -20 N/A False 426											
Showing 1 to 2 of 2 entries	wing 1 to 2 of 2 entries 1 Next											



9.2.2. OCh Current Performance Statistics

9.2.2.1. OCh Monitoring Parameters Introduction

Monitoring parameters of OCh monitoring points include maximum differential group delay (DGD), maximum differential group delay (DGD) timestamp, minimum differential group delay (DGD) timestamp, average differential group delay (DGD), maximum chromatic dispersion (CD), maximum chromatic dispersion (CD), maximum chromatic dispersion (CD), maximum chromatic dispersion (CD) timestamp, average chromatic dispersion (CD), maximum optical signal-to-noise ratio (OSNR), maximum optical signal-to-noise ratio (OSNR) timestamp, 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.

NE	Please S	elect	* 5	Slot	• Port		 PM Granu 	larity 15min	¥	Refresh				
Show	10	• entries										Res	set Search:	Search
	Name	It MaxDo	GD 11	MaxDGD Stamp 1	MinDGD 1	MinDGD Stamp ↓↑	AvgDGD 1	MaxCD ↓†	MaxCD Stamp 1	MinCD ↓	↑ MinCD Stamp ↓↑	AvgCD 1	MaxOSNR 1	MaxOSNR Stamp ↓↑
											No data avail	able in table		
Show	ving 0 to) of 0 entries	6											Previous Next

Figure 9-21 OCh Monitoring Parameters

9.2.2.2. View OCh Monitoring Information

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

NE	NE 192.168.21.72 Slot 7 Port 3 PM Granularity 15min Refresh										
Show	iow 10 • entries									Search: Search	
	Name I1	MaxDGD ↓↑	MaxDGD Stamp 1	MinDGD 1	MinDGD Stamp 1	AvgDGD 1	MaxCD 1	MaxCD Stamp 1	MinCD ↓↑	MinCD Stamp 1	AvgCD 1
	192.168.21.72_Slot7_Port3_OCh_Ingress_NearEnd	4	2019/02/26 14:45:12	2	2019/02/26 14:46:37	3	-831	2019/02/26 14:46:06	-938	2019/02/26 14:46:14	-886
Show	ing 1 to 1 of 1 entries									Previous 1	Next

Figure 9-22 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:

NE	192.168.21.72 • Slot 7	• Port 3	٣	PM Granulari	ty 24h	• Refres	h				
Show	10 • entries		Reset	Search: Search							
	Name 11	MaxDGD 1	MaxDGD Stamp 1	MinDGD 11	MinDGD Stamp 1	AvgDGD 1	MaxCD 🕼	MaxCD Stamp 1	MinCD 1	MinCD Stamp 1	AvgCD 1
	192.168.21.72_Slot7_Port3_OCh_Ingress_NearEnd	5	2019/02/26 14:31:02	2	2019/02/26 14:28:16	3	-823	2019/02/26 14:36:36	-948	2019/02/26 14:37:46	-884
Show	ring 1 to 1 of 1 entries									Previous 1	Next

Figure 9-23 24-Hour OCh Monitoring Data

9.2.2.3. Reset OCh Monitoring Data

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

NE	192.168.21.72 • Slot 7	• Port 3	٠	PM Granulari	ty 24h	• Refrest	1				
Show	10 • entries								Reset	Search: Search	
۲	Name 1†	MaxDGD 1	MaxDGD Stamp 🕼	MinDGD 1	MinDGD Stamp 1	AvgDGD 1	MaxCD 1	MaxCD Stamp 🗍	MinCD ↓↑	MinCD Stamp	AvgCD 1
	192.168.21.72_Slot7_Port3_OCh_Ingress_NearEnd	5	2019/02/26 14:31:02	2	2019/02/26 14:28:16	3	-823	2019/02/26 14:36:36	-948	2019/02/26 14:37:46	-884
Show	Previous 1 Next										
	Are you sure you want to operate these data?										

Figure 9-10 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 timestamps are updated to the latest time to read the value, and other data will be updated to that read at the latest time.

NE	NE 192.168.21.72 Slot 7 Port 3 PM Granularity 24h Refresh											
Show 10 • entries Reset Search. Search.												
	Name 11	MaxDGD ↓↑	MaxDGD Stamp 1	MinDGD 1	MinDGD Stamp 1	AvgDGD	MaxCD ↓↑	MaxCD Stamp 🗍	MinCD ↓↑	MinCD Stamp	AvgCD 1	
	192.168.21.72_Slot7_Port3_OCh_Ingress_NearEnd	0	1970/01/01 08:00:00	0	1970/01/01 08:00:00	0	0	1970/01/01 08:00:00	0	1970/01/01 08:00:00	0	
Show	Previous 1 Next											
	✓ Success! Apply											

Figure 9-25 Successful Resetting of OCh

9.2.2.4. OCh Monitoring Data Shown as NA

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

- (1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.
- (2) Optical module is inserted into the port but it is mismatched and the port is enabled.

(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 NA. The timestamp 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:

NE 192.168.21.72	▼ Slot	9	• Port	1	 PM Granularity 	15min	• Refresh				
Show 10 • entries									Reset	Search: Search	
I↑ MaxCD Stamp ↓↑	MinCD ↓↑	MinCD Stamp 1	AvgCD 1	MaxOSNR 1	MaxOSNR Stamp $\downarrow \uparrow$	MinOSNR 1	MinOSNR Stamp 1	AvgOSNR 1	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time $\downarrow\uparrow$	Operate ↓↑
/::	N/A	//::	N/A	N/A	//::	N/A	/:	N/A	False	42	Reset
Showing 1 to 1 of 1 entri	es									Previous	1 Next

Figure 9-11 Optical Module of OCh Not In Position

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

(1) When the module is not in position or is pre-configured with an empty slot and the port for the module is enabled, the maximum and minimum data will be shown as NA. The timestamp 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.

NE 192.16	8.21.72	• Slot	9	• Port	1	 PM Granularity 	15min	• Refresh				
Show 10	 entries 									Reset	Search: Search	
MaxCD	Stamp ↓↑	MinCD 1	MinCD Stamp ↓↑	AvgCD ↓↑	MaxOSNR 1	MaxOSNR Stamp $\downarrow\uparrow$	MinOSNR 1	MinOSNR Stamp 1	AvgOSNR 1	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time $\downarrow \uparrow$	Operate $\downarrow\uparrow$
/	/:	N/A	//::	N/A	N/A	/::	N/A		N/A	False	0	Reset
Showing 1 to	1 of 1 entrie	es									Previous	1 Next

Figure 9-27 OCh Monitoring Data

(2) When the module is mismatched and the port for the module is enabled, the maximum and minimum data will be shown as NA. The timestamp 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:

NE	192.168.21.72	▼ Slot	9	• Port	1	 PM Granularity 	15min	• Refresh				
Show	10 • entries									Reset	Search: Search	
l† I	MaxCD Stamp ↓†	MinCD 1	MinCD Stamp $\downarrow\uparrow$	AvgCD ↓↑	MaxOSNR 1	MaxOSNR Stamp $\downarrow\uparrow$	MinOSNR 1	MinOSNR Stamp $\downarrow \uparrow$	AvgOSNR 1	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time $\downarrow\uparrow$	Operate 1
	//:	N/A	//::	N/A	N/A	/!:	N/A	/	N/A	False	42	Reset
Show	ving 1 to 1 of 1 entrie	is									Previous	1 Next

Figure 9-28 OCh Monitoring Data When Mismatched

9.2.3. FEC Current Performance Statistics

9.2.3.1. FEC Monitoring Parameters Introduction

As shown in the figure, the monitoring parameters of FEC monitoring points include maximum error correction rate, maximum error correction rate timestamp, 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 9-29 FEC Monitoring Parameters

9.2.3.2. View FEC Monitoring Information

As shown in the figure, select the appropriate network elements, slots, ports and monitoring cycle through the selection box above the menu, the FEC value of a certain network element/slot/port will be displayed. There is only one entrance-near end monitoring point for FEC. Optical module is inserted into the monitoring port. FEC data and corresponding generation timestamp 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.

NE	192.168.21.72 v Slot 7	Port 1	 PM Granularit 	y 15min	• Refresh			
Show	v 10 v entries					Reset	Search: Search	
	Name	↑ PreFECBER ↓↑	PreFECBER Threshold 1	Max Corrected BER 1	Max Corrected BER Stamp $\downarrow \uparrow$	Avg Corrected BER 1	Suspect Interval Flag $\downarrow\uparrow$	Elap
	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearE	d 1.8621118E-6	1015222895	2.2133077E-6	2019/02/26 14:46:12	1.9431004E-6	True	
Show	ving 1 to 1 of 1 entries						Previous 1 Ne	ext



Optical module is inserted into the monitoring port. FEC 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:

NE	192.168.21.72 • Slot 7	Port 1	 PM Granularit 	y 24h	• Refresh			
Show	v 10 ▼ entries					Reset	Search: Search	
	Name It	PreFECBER 1	PreFECBER Threshold $\downarrow \uparrow$	Max Corrected BER $\downarrow \uparrow$	Max Corrected BER Stamp $\downarrow\uparrow$	Avg Corrected BER $\downarrow \uparrow$	Suspect Interval Flag $\downarrow\uparrow$	Elaps
	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearEnd	1.9847198E-6	1015222895	2.2918316E-6	2019/02/26 14:42:43	1.920875E-6	False	
Show	wing 1 to 1 of 1 entries						Previous 1 Ne	ext

Figure 9-31 24-Hour Monitoring Data of FEC

9.2.3.3. Reset FEC Monitoring Data

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

NE	192.168.21.72 • Slot 7 •	Port 1	PM Granularit	ly 24h	• Refresh			
Show	10 • entries					Reset	Search: Search	
۲	Name 11	PreFECBER	PreFECBER Threshold	Max Corrected BER	Max Corrected BER Stamp	Avg Corrected BER	Suspect Interval Flag	Elap:
۲	192.168.21.72_Slot7_Port1_OTU-FEC_Ingress_NearEnd	1.9847198E-6	1015222895	2.2918316E-6	2019/02/26 14:42:43	1.920875E-6	False	
Show	ing 1 to 1 of 1 entries						Previous 1	Next
			Are you sure yo	ou want to operate these dat	ta? cel			

Figure 9-32 FEC Reset

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

NE 19	2.168.21.72	▼ Slot 7	▼ Port 1	PM Granularity 15n	nin 🔻 Re	efresh			
Show	10 • entries						Reset	Search: Search	
11	PreFECBER	PreFECBER Threshold	Max Corrected BER 1	Max Corrected BER Stamp $\downarrow \uparrow$	Avg Corrected BER $\downarrow\uparrow$	Suspect Interval Flag 🕼	Elapsed Time $\downarrow\uparrow$	Threshold Operate 1	Operate ↓†
learEnd	1.5709556E-6	1015222895	1.5709556E-6	2019/02/26 15:43:16	1.5709556E-6	False	1	Modify Threshold	Reset
Showing	1 to 1 of 1 entries							Previous	1 Next
				✓ SuccessI Q ∰¥	Apply				

Figure 9-12 FEC Successfully Reset

9.2.3.4. FEC Monitoring Data Shown as NA

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

- (1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.
- (2) Optical module is inserted into the port but it is mismatched and the port is enabled.

At this time, all the non-timestamp data will be shown as NA and all the timestamps 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:

NE 192.168.21.72 • Slot 9	Port 1	▼ PM G	ranularity 15min	• Refresh			
Show 10 • entries					Res	et Search: Search	
Name It	PreFECBER 1	PreFECBER Threshold $\downarrow \uparrow$	Max Corrected BER $\downarrow \uparrow$	Max Corrected BER Stamp $\downarrow \uparrow$	Avg Corrected BER $\downarrow \uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time
2.168.21.72_Slot9_Port1_OTU-FEC_Ingress_NearEnd	N/A	1015222895	N/A	/	N/A	False	14
Showing 1 to 1 of 1 entries						Previous	1 Next

Figure 9-13 Optical Module of FEC Not In Position

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

(1) When the module is not in position or is pre-configured with an empty slot and the port for the module is enabled, all the nontimestamp data will be shown as NA and all the timestamps 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.

NE 19	2.168.21.72	• Slot 5	Port 1	PM Granularity 15n	nin 🔻 Re	efresh			
Show 1	10 • entries						Reset	Search: Search	
	PreFECBER 1	PreFECBER Threshold 1	Max Corrected BER $\downarrow\uparrow$	Max Corrected BER Stamp $\downarrow\uparrow$	Avg Corrected BER $\downarrow\uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time $\downarrow\uparrow$	Threshold Operate $\downarrow\uparrow$	Operate 1
learEnd	N/A	1015222895	N/A	/	N/A	False	0	Modify Threshold	Reset
Showing	1 to 1 of 1 entries							Previous	1 Next

Figure 9-14 FEC Monitoring Data

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

NE 192.168.21.72 • Slot 9	Port 1	▼ PM G	ranularity 15min	• Refresh			
Show 10 • entries					Res	et Search: Search	
Name 11	PreFECBER 1	PreFECBER Threshold $\downarrow \uparrow$	Max Corrected BER $\downarrow\uparrow$	Max Corrected BER Stamp $\downarrow\uparrow$	Avg Corrected BER $\downarrow\uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time
2.168.21.72_Slot9_Port1_OTU-FEC_Ingress_NearEnd	N/A	1015222895	N/A	/	N/A	False	14
Showing 1 to 1 of 1 entries						Previous	1 Next

Figure 9-15 FEC Monitoring Data When Mismatched

9.2.4. OTUk/ODUk Current Performance Statistics

9.2.4.1. OTUk/ODUk Monitoring Parameters Introduction

As shown in the figure, the monitoring parameters of OTUk / ODUk monitoring points include background error block (BBE), error second (ES), serious error second (SES), unavailable second (UAS), suspicious interval marker, runtime (S) and reset operation. The performance parameters of OTUk / ODUk will be enabled or disabled at the same time.



NE Please Select •	Slot	• Port	 PM Granul 	arity 15mi	n v	Refresh			
Show 10 • entries							R	eset Search: Search.	
Name ↓↑ BBE ↓↑ BBE	Threshold 1 ES 1	ES Threshold 1 SE	ES ↓↑ SES Threshold ↓↑	UAS ↓†	UAS Threshold $\downarrow\uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time $\downarrow \uparrow$	Threshold Operate $\downarrow\uparrow$	Reset Operate
			No	data availab	le in table				
Showing 0 to 0 of 0 entries								P	revious Next

Figure 9-16 OTUk/ODUk Monitoring Parameters

9.2.4.2. View OTUk/ODUk Monitoring Information

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

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

NE	192.168.21.72 • Slot 7	• Por	t 1	۲P	M Granularity 15m	in	• Refresh						
Show	Show 10 • entries Reset Search												
	Name 11	BBE ↓↑	BBE Threshold $\downarrow\uparrow$	ES ↓↑	ES Threshold $\downarrow\uparrow$	SES 11	SES Threshold $\downarrow\uparrow$	UAS 🕸	UAS Threshold $\downarrow\uparrow$	Suspect Interval Flag	Elapsed Time $\downarrow \uparrow$		
	192.168.21.72_Slot7_Port1_OTU_Ingress_NearEnd	0	9000	0	5	0	2	0	2	True	866		
	192.168.21.72_Slot7_Port1_OTU_Ingress_FarEnd	0	9000	0	5	0	2	0	2	True	866		
Shov	ving 1 to 2 of 2 entries									Prev	vious 1 Next		

Figure 9-17 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:

NE	192.168.21.72 • Slot 7	▼ Por	t 1	۲P	M Granularity 24h		• Refresh						
Show	Now 10 • entries Search												
	Name 11	BBE ↓↑	BBE Threshold $\downarrow\uparrow$	ES ↓↑	ES Threshold $\downarrow \uparrow$	SES 11	SES Threshold $\downarrow\uparrow$	UAS ↓↑	UAS Threshold 1	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time $\downarrow\uparrow$		
	192.168.21.72_Slot7_Port1_OTU_Ingress_NearEnd	0	864000	0	480	0	192	0	192	False	5524		
	192.168.21.72_Slot7_Port1_OTU_Ingress_FarEnd	0	864000	0	480	0	192	0	192	False	5524		
Show	ing 1 to 2 of 2 entries									Previ	ious 1 Next		

Figure 9-18 24-Hour OTUk/ODUk Monitoring Data

9.2.4.3. Error Generation Conditions for Monitoring Parameters

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

- Equipment Missing
- Equipment Mismatch
- Equipment Failure
- OTUk defects: OTU-LOS, OTU-LOF, OTU-LOM, OTU-AIS and OTU-TIM.
- ODUk defects: alarms of the Server layer (e.g. LOS, LOF, LOM), ODU-AIS, ODU-LCK, ODU-TIM, ODU-OCI and ODU-PLM.
- When alarms are generated at the far end, SES counts generate.

- BDI.
- When low-rate bit error is inserted by the meter, BBE and ES generate.
- ES and SES are generated when high-rate bit error is inserted by the meter. The continuous 10S of SES will become a UAS. If the high-rate bit error of the meter keeps, then ES and SES stops counting but UAS will count all the time.

NE 192.168.21.7	▼ Slot 7		Port 1		 PM Granularit 	y 15min	* R	lefresh				
Show 10 •	entries									Reset	Search: Search	
	BBE ↓↑	BBE Threshold 1	ES ↓↑	ES Threshold $\downarrow\uparrow$	SES ↓↑	SES Threshold 1	UAS 🕸	UAS Threshold 1	Suspect Interval Flag $\downarrow\uparrow$	Elapsed Time 🕸	Threshold Operate $\downarrow\uparrow$	Reset Operate
ngress_NearEnd	0	9000	0	5	0	2	0	2	True	183	Modify Threshold	Reset
ngress_FarEnd	0	9000	0	5	0	2	0	2	True	183	Modify Threshold	Reset
Showing 1 to 2 of	2 entries										Previous	1 Next

Figure 9-19 UAS Always Counts

9.2.4.4. OTUk/ODUk Monitoring Data Reset

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

NE	192.168.21.72 * Slot 5	Port		PM Granularity 15min Ref							
Shov	10 • entries								R	eset Search: Search	
۲	Name 11	BBE ↓↑	BBE Threshold $\downarrow\uparrow$	ES ↓↑	ES Threshold 1	SES 11	SES Threshold $\downarrow\uparrow$	UAS ↓†	UAS Threshold $\downarrow\uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time
۲	192.168.21.72_Slot5_Port3_OTU_Ingress_NearEnd	2760	9000	3	5	0	2	0	2	True	110
	192.168.21.72_Slot5_Port3_OTU_Ingress_FarEnd	742	9000	3	5	0	2	0	2	True	110
	192.168.21.72_Slot5_Port3_ODU4(0)_Ingress_NearEnd	1029	9000	3	5	0	2	21	2	True	110
	192.168.21.72_Slot5_Port3_ODU4(0)_Ingress_FarEnd	523	9000				2	0	2	True	110
Shov	ving 1 to 4 of 4 entries			Are yo	u sure you want to op	oly C	data?			Previous	1 Next

Figure 9-20 OTUk/ODUk Reset

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

NE	NE 192 198 21.72 Slot 5 Port 3 PM Granularity 15min Refresh												
Show	v 10 v entries								R	eset Search: Search			
	Name ↓↑	BBE ↓†	BBE Threshold 1	ES ↓†	ES Threshold 1	SES 11	SES Threshold 1	UAS ↓↑	UAS Threshold 1	Suspect Interval Flag 🎼	Elapsed Time		
	192.168.21.72_Slot5_Port3_OTU_Ingress_NearEnd	0	9000	0	5	0	2	0	2	False	0		
	192.168.21.72_Slot5_Port3_OTU_Ingress_FarEnd	0	9000	0	5	0	2	0	2	False	0		
	192.168.21.72_Slot5_Port3_ODU4(0)_Ingress_NearEnd	0	9000	0	5	0	2	0	2	False	0		
	192.168.21.72_Slot5_Port3_ODU4(0)_Ingress_FarEnd	0	9000				2	0	2	False	0		
Show	ving 1 to 4 of 4 entries			Í	Success!	Apply				Previous	1 Next		

Figure 9-21 OTUk/ODUk Successfully Reset

9.2.4.5. OTUk/ODUk Monitoring Data Shown as NA

Here are the situations when the OTUk/ODUk monitoring data 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 or untrustworthy (after 900/86400 seconds). The running time is normal and counts from 0, as shown in the figure below:

NE 192.188.21.72														
Show 10	how 10 • entries Reset Search													
	$BBE{\downarrow}{\uparrow}$	BBE Threshold 1	ES ↓↑	ES Threshold $\downarrow\uparrow$	SES ↓↑	SES Threshold $\downarrow\uparrow$	UAS 🕼	UAS Threshold 1	Suspect Interval Flag $\downarrow\uparrow$	Elapsed Time $\downarrow\uparrow$	Tł	hreshold Operate 1	Rese	t Operate
ess_NearEnd	N/A	9000	N/A	5	N/A	2	N/A	2	False	280		Modify Threshold		Reset
ess_FarEnd	N/A	9000	N/A	5	N/A	2	N/A	2	False	280		Modify Threshold		Reset
Showing 1 to 2	owing 1 to 2 of 2 entries 1 Next													

Figure 9-22 Optical Module of OTUk/ODUk Not In Position

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

(1) When the module is not in position or is pre-configured with an empty slot and the port for the module 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 the figure below.

NE	192.168.21.72 • Slot 5 • Port 3 • PM Granularity 15min • Refresh												
Show	Show 10 • entries Reset Search. Search.												
	Name 11	BBE ↓↑	BBE Threshold $\downarrow\uparrow$	ES ↓↑	ES Threshold $\downarrow\uparrow$	SES 11	SES Threshold $\downarrow\uparrow$	UAS ↓↑	UAS Threshold $\downarrow\uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time		
	192.168.21.72_Slot5_Port3_OTU_Ingress_NearEnd	0	9000	0	5	0	2	0	2	False	0		
	192.168.21.72_Slot5_Port3_OTU_Ingress_FarEnd	0	9000	0	5	0	2	0	2	False	0		
	192.168.21.72_Slot5_Port3_ODU4(0)_Ingress_NearEnd	0	9000	0	5	0	2	0	2	False	0		
	192.168.21.72_Slot5_Port3_ODU4(0)_Ingress_FarEnd	0	9000	0	5	0	2	0	2	False	0		
Show	howing 1 to 4 of 4 entries 1 Next												

Figure 9-23 OTUk/ODUk Monitoring Data

(2) When the module is mismatched and the port for the module 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:

NE	192.168.21.72 • Slot 5	Port	3	• PM G	ranularity 15min		• Refresh							
Show	Now 10 • entries Search: Search													
	Name 11	BBE ↓↑	BBE Threshold $\downarrow\uparrow$	ES ↓↑	ES Threshold 1	SES 11	SES Threshold $\downarrow\uparrow$	UAS 🕸	UAS Threshold $\downarrow\uparrow$	Suspect Interval Flag $\downarrow\uparrow$	Elapsed Time			
	192.168.21.72_Slot5_Port3_OTU_Ingress_NearEnd	0	9000	0	5	0	2	0	2	False	0			
	192.168.21.72_Slot5_Port3_OTU_Ingress_FarEnd	0	9000	0	5	0	2	0	2	False	0			
	192.168.21.72_Slot5_Port3_ODU4(0)_Ingress_NearEnd	0	9000	0	5	0	2	0	2	False	0			
	192.168.21.72_Slot5_Port3_ODU4(0)_Ingress_FarEnd	0	9000	0	5	0	2	0	2	False	0			
Show	Showing 1 to 4 of 4 entries 1 Next													

Figure 9-24 OTUk/ODUk Monitoring Data When Mismatched

9.2.5. Current Performance Statistics of SDH Regeneration Segment

9.2.5.1. Monitoring Parameters Introduction of SDH Regeneration Segment

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

NE Please	e Select	▼ Slot		• Port		▼ PM Gra	nularity	15min	▼ Refresh				
Show 10 • entries Search: Search												ì	
Name J†	BBE 11	BBE Threshold $\downarrow \uparrow$	$ES\downarrow\uparrow$	ES Threshold 1	SES 11	SES Threshold $\downarrow\uparrow$	UAS 🕸	UAS Threshold $\downarrow\uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time $\downarrow\uparrow$	Threshold Operate	∋ J↑ F	Reset Operate 🔱
No data available in table													
Showing 0 t	o 0 of 0 en	tries											Previous Nevt



9.2.5.2. View Monitoring Information of SDH Regeneration Segment

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

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

NE	192.168.21.72 • Slot 16	Port 9		PM Gr	anularity 15min		* Refresh						
Show	Now 10 • entries Search												
	Name It	BBE ↓↑	BBE Threshold 1	ES ↓↑	ES Threshold $\downarrow\uparrow$	SES 11	SES Threshold $\downarrow\uparrow$	UAS ↓↑	UAS Threshold $\downarrow\uparrow$	Suspect Interval Flag $\downarrow\uparrow$	Elapsed Time		
	192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd	0	9000	0	5	0	2	256	2	False	256		
Show	Showing 1 to 1 of 1 entries 1 Next												

Figure 9-26 15-Minute SDH Monitoring Data

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

NE	192.168.21.72 • Slot 16											
Show	thow 10 • entries Search: Search.											
	Name	BBE ↓↑	BBE Threshold 1	ES ↓↑	ES Threshold 1	SES ↓↑	SES Threshold $\downarrow\uparrow$	UAS 🕸	UAS Threshold $\downarrow\uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time	
	192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEn	0 1	864000	0	480	0	192	229	192	False	229	
Show	Previous 1 Next											

Figure 9-27 24-Hour SDH Monitoring Data

9.2.5.3. SDH Regeneration Segment Monitoring Data Reset

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

NE	E 192 168 21 72 Slot 16 Port 9 PM Granularity 24h Refesh													
Sho	Show 10 • entries Reset Search: Search.													
Ø	Name	BBE 1	BBE Threshold 1	SES ↓↑	SES Threshold $\downarrow\uparrow$	UAS ↓↑	UAS Threshold 1	Suspect Interval Flag J↑	Elapsed Time					
Image: 192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd 0 864000 0 480 0 192 229 192 False														
Sho	Previous 1 Next													
	Are you sure you want to operate these data?													

Figure 9-28 SDH Regeneration Segment Reset

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

NE 192.168.21.72 Slot 16 Port 9 PM Granularity 24h Refresh													
Shov	IOW 10 • entries Reset Search Search												
Name II BBE II BBE Threshold II ES II ES Threshold II SES II SES Threshold II UAS II UAS Threshold II Suspect Interval Flag II Elapsed													
	192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd 0 864000 0 480 0 192 0 192 Faise 0												
Shov	howing 1 to 1 of 1 entries Previous 1 Next												
				~	Success!	Apply							

Figure 9-29 SDH Regeneration Segment Successfully Reset

9.2.5.4. Monitoring Data of SDH Regeneration Segment Shown as NA

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

- (1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.
- (2) The port and the module are normal and the port is enabled.
- (3) Optical module is inserted into the port but it is mismatched and the port is enabled.

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

NE 192.168.21.72 • Slot 16	• Po	9	v	PM Granularity 15	min	• Refresh							
Show 10 • entries	how 10 • entries Reset Search												
Name	↑ BBE ↓↑	BBE Threshold 1	ES ↓†	ES Threshold 1	SES 11	SES Threshold $\downarrow\uparrow$	UAS 🕸	UAS Threshold $\downarrow\uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time 1			
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEr	d O	9000	0	5	0	2	238	2	True	238			
Showing 1 to 1 of 1 entries									Pre	vious 1 Next			

Figure 9-30 Optical Module of SDH Regeneration Segment Not In Position

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

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

¢	System Management Configu	uration Mana	gement	Fault Managemen	t Per	formance Manager	ment	Security Management	Log M	lanagement OLP	Route
							3	197 🚯 116	<mark>⊗</mark> 41	<mark>(3</mark> 39 🙆 1	root
NE	192.168.21.73 • Slot 2	• Por	t 1	▼ PM (Granulari	ty 15min	T F	efresh			
Show 10 v entries Reset Search. Search.											
	Name		BBE ↓↑	BBE Threshold $\downarrow\uparrow$	ES ↓↑	ES Threshold 1	SES ↓↑	SES Threshold 1	UAS ↓↑	UAS Threshold 1	Suspect Interva
	192.168.21.73_Slot2_Port1_SDH-RS_Ingress	s_NearEnd	N/A	9000	N/A	5	N/A	2	N/A	2	False
Show	ing 1 to 1 of 1 entries									Previou	s 1 Next

Figure 9-31 SDH Regeneration Segment Monitoring Data

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

(Image: Weight and the system Management Configuration Management Fault Management Performance Management Security Management Log Management OLP Route											
								1 97 🚯116	€241	(39 🙆 1	root	
NE	NE 192.168.21.73 V Slot 2 V Port 1 V PM Granularity 15min V Refresh											
Show	10 • entries								R	eset Search: Se	arch	
	Name		$BBE \downarrow \uparrow$	BBE Threshold ↓↑	ES ↓↑	ES Threshold 1	SES ↓↑	SES Threshold $\downarrow\uparrow$	UAS ↓↑	UAS Threshold 1	Suspect Interval	
	192.168.21.73_Slot2_Port1_SDH-RS_Ingress_NearEnd N/A 9000 N/A 5 N/A 2 N/A 2 False											
Show	owing 1 to 1 of 1 entries 1 Next											



9.2.6. Current Performance Statistics of Ethernet

9.2.6.1. Ethernet Monitoring Parameters Introduction

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





9.2.6.2. View Ethernet Monitoring Information

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

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

NE	192.168.21.72 • Slot 5	Port 1	• PM (Granularity 15min	• Refres	h								
Sho	3how 10 • entries Reset Search													
	Name 11	Good Frame J1	Unicast Frame 1	Multicast Frame 1	Broadcast Frame 1	CRC Error Frame $\downarrow\uparrow$	Alignment Error Frame $\downarrow\uparrow$	Frame Too Long $\downarrow\uparrow$	Jabber					
	192.168.21.72_Slot5_Port1_Ethernet_Ingress_NearEnd	0	0	0	0	0	0	0						
	192.168.21.72_Slot5_Port1_Ethernet_Egress_NearEnd	0	0	0	0	N/A	N/A	N/A						
Sho	wing 1 to 2 of 2 entries							Previous 1	Next					

Figure 9-34 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:

NE	192.168.21.72 • Slot 16	Port 9	,	PM Gr	anularity 24h		• Refresh				
Show	how 10 • entries Search: Search.										
	Name 11	BBE ↓↑	BBE Threshold $\downarrow\uparrow$	ES ↓↑	ES Threshold $\downarrow\uparrow$	SES 11	SES Threshold $\downarrow\uparrow$	UAS 🕸	UAS Threshold $\downarrow \uparrow$	Suspect Interval Flag $\downarrow \uparrow$	Elapsed Time
	192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd	0	864000	0	480	0	192	1759	192	False	1759
Show	Showing 1 to 1 of 1 entries 1 Next										



9.2.6.3. Ethernet Monitoring Data Reset

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

NE	NE 192.168.21.72 Slot 5 Port 1 PM Granularity 15min Refresh										
Show	v 10 v entries						Reset Sea	arch: Search			
	Name 11	Good Frame 🕼	Unicast Frame 🕼	Multicast Frame 1	Broadcast Frame 🕼	CRC Error Frame 1	Alignment Error Frame $\downarrow\uparrow$	Frame Too Long 🕼	Jabber		
Ø	192.168.21.72_Slot5_Port1_Ethernet_Ingress_NearEnd	0	0	0	0	0	0	0			
۲	192.168.21.72_Slot5_Port1_Ethernet_Egress_NearEnd	0	0	0	0	N/A	N/A	N/A			
Show	ving 1 to 2 of 2 entries				_			Previous 1	Next		
			🛕 Are	you sure you want to op	erate these data?						
				App	oly Cancel						

Figure 9-36 Ethernet Reset

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

NE	192.168.21.72 v Slot 5	Port 1	* PM	Granularity 15min	• Refres	h				
Shov	10 • entries						Reset Sea	Irch: Search		
	Name 11	Good Frame ↓↑	Unicast Frame $\downarrow\uparrow$	Multicast Frame $\downarrow\uparrow$	Broadcast Frame $\downarrow\uparrow$	CRC Error Frame 1	Alignment Error Frame $\downarrow\uparrow$	Frame Too Long $\downarrow\uparrow$	Jabber	
	192.168.21.72_Slot5_Port1_Ethernet_Ingress_NearEnd	0	0	0	0	0	0	0		
	192.168.21.72_Slot5_Port1_Ethernet_Egress_NearEnd	0	0	0	0	N/A	N/A	N/A		
Showing 1 to 2 of 2 entries 1 M										
				 Success! 						
					Apply					

Figure 9-37 Ethernet Successfully Reset

9.2.6.4. Ethernet Monitoring Data Shown as NA

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

- (1) When optical module is not inserted into the port, the optical module is not in position but the port is enabled.
- (2) The port and the module are normal and the port is enabled.
- (3) Optical module is inserted into the port but it is mismatched and the port is enabled.

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

NE 192.168.21.72 • Slot	5	• Port 1	۲P	M Granularity 15min	• Refr	esh				
Show 10 • entries Search										
Name It	Good Frame 1	Unicast Frame 1	Multicast Frame 1	Broadcast Frame 1	CRC Error Frame $\downarrow\uparrow$	Alignment Error Frame $\downarrow\uparrow$	Frame Too Long $\downarrow\uparrow$	Jabber Frame 1	Fragment F	
5_Port1_Ethernet_Ingress_NearEnd	0	0	0	0	0	0	0	0	0	
5_Port1_Ethernet_Egress_NearEnd	0	0	0	0	N/A	N/A	N/A	N/A	N/A	
howing 1 to 2 of 2 entries 1 Next										

Figure 9-38 Optical Module of Ethernet Not In Position

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

(1) When the module is not in position or is pre-configured with an empty slot and the port for the module 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:

NE 192.168.21.72 Slot 5 Port 1 PM Granularity 15min Refresh											
Show 10	• entries						Reset	Search: Search			
	Name	It Good Fra	me 11 Unicast Frame 11	Multicast Frame 1	Broadcast Frame J1	CRC Error Frame	Alignment Error Frame	Frame Too Long	Jabber		
192.168.	21.72_Slot5_Port1_Ethernet_In	gress_NearEnd N/A	N/A	N/A	N/A	N/A	N/A	N/A			
192.168.21.72_Slot5_Port1_Ethernet_Egress_NearEnd N/A N/A N/A N/A N/A											
Showing 1 to 2 of 2 entries 1 Next											
NE 192.168.2	1.72 • Slot 5	• Port	r PM	Granularity 15min	 Refresh 	h					
Show 10	▼ entries						Reset	Search: Search			
Byte Frame 🗐	512-1023 Byte Frame	1024-1518 Byte Frame	1519-Maximun Frame	Oversize Frame	Good Pause Frame	J↑ Total Frame J↑	Suspect Interval Flag 1	Elapsed Time $\downarrow\uparrow$	Operate 1		
N/A	N/A	N/A	N/A	N/A	N/A	N/A	False	0	Reset		
N/A	N/A	N/A	N/A	N/A	N/A	N/A	False	0	Reset		
Showing 1 to 2	Showing 1 to 2 of 2 entries 1 Next										

Figure 9-39 Ethernet Monitoring Data

(2) When the module is mismatched and the port for the module 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:

NE 192.168.21.72 Slot 5 Port 1 PM Granularity 15min Refresh											
Show 10	• entries						Reset S	earch: Search			
•	Name	↓↑ Good Fra	me 🕼 Unicast Frame 🕼	Multicast Frame $\downarrow\uparrow$	Broadcast Frame 1	CRC Error Frame 1	Alignment Error Frame	Frame Too Long	g ↓† Jabber		
□ 192.168.2	21.72_Slot5_Port1_Ethernet_In	ngress_NearEnd N/A	N/A	N/A	N/A	N/A	N/A	N/A			
192.168.21.72_Slot5_Port1_Ethernet_Egress_NearEnd N/A N/A N/A N/A N/A											
Showing 1 to 2 of 2 entries 1 Next											
NE 192.168.21	1.72 • Slot 5	Port 1	▼ PM	Granularity 15min	• Refresh						
Show 10	• entries						Reset	Search: Search			
3yte Frame ↓†	512-1023 Byte Frame 🕼	1024-1518 Byte Frame	1519-Maximun Frame	Oversize Frame	Good Pause Frame	l↑ Total Frame ↓↑	Suspect Interval Flag J1	Elapsed Time 🕼	Operate 11		
N/A	N/A	N/A	N/A	N/A	N/A	N/A	False	0	Reset		
N/A	N/A	N/A	N/A	N/A	N/A	N/A	False	0	Reset		
Showing 1 to 2	Showing 1 to 2 of 2 entries 1 Next										



9.3. History Performance Statistics

9.3.1. History Performance Statistics of Optical Power

9.3.1.1. History Monitoring Parameters Introduction of Optical Power

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

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

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

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





9.3.1.2. 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 9-42 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:

NE Please Select	Slot	• Port	• PM (Granularity 15min	Ŧ				
Chart Table									
Show 10 ventries				Export	Search: Search.		Time Interval	Please Select	•
Name 🕼 MaxPower 🎼	MaxPower Stamp 1	MinPower 1	MinPower Stamp 1	AvgPower 11 Suspe	ct Interval Flag 斗	Time Stamp 1	Time Duration		
		No	data available in table						
Showing 0 to 0 of 0 entries					F	Previous Next			

Figure 9-43 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:

w 10 v entries					Export	Search:	Search	Time Interval	Last Three Days
Name 44	MaxPower 1	MaxPower Stamp	MinPower 1	MinPower Stamp	AvgPower 1	Suspect Interval Flag	Time Stamp 1	Time Duration	2019/02/25 - 2019/02/27
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 10:00:01	1.2	2019/02/27 10:00:01	1.2	True	2019/02/27 10:15:00		
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 10:15:01	1.2	2019/02/27 10:15:01	1.2	True	2019/02/27 10:30:00		
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 10:30:01	1.2	2019/02/27 10:30:01	1.2	True	2019/02/27 10:45:00		
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 10:45:01	1.2	2019/02/27 10:45:01	1.2	True	2019/02/27 11:00:00		
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 11:00:01	1.2	2019/02/27 11:00:01	1.2	True	2019/02/27 11:15:00		
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 11:15:01	1.2	2019/02/27 11:15:01	1.2	True	2019/02/27 11:30:00		
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 11:30:01	1.2	2019/02/27 11:30:01	1.2	True	2019/02/27 11:45:00		
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 11:45:01	1.2	2019/02/27 11:45:01	1.2	True	2019/02/27 12:00:00		
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 12:00:01	1.2	2019/02/27 12:00:01	1.2	True	2019/02/27 12:15:00		
2.168.21.72_Slot7_Port2_Optical_Egress_NearEnd	1.2	2019/02/27 12:15:01	1.2	2019/02/27 12:15:01	1.2	True	2019/02/27 12:30:00		
wing 1 to 10 of 28 entries						Previous	1 2 3 Next		

Figure 9-44 15-Minute Tabular History Data of Optical Power

9.3.1.3. Export History Monitoring Information of Optical Power

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

192 168 21 72 * Slot 7		Port 2	FileName	Can not cor	ntain /:*?*<> spec	tial characters			
Table						Apply Close			
10 • entries					Export	Search	Search	Time Interval	Last Three Days
Name II.	MaxPower II	MaxPower Stamp 11	MinPower 11	MinPower Stamp 11	AvgPower II	Suspect Interval Flag	Time Stamp 11	Time Duration	2019/02/25 - 2019/02/27
68.21.72_Skot7_Port2_Optical_Egress_NearEnd		2019/02/27 10:00:01				True	2019/02/27 10:15:00		
68.21.72_Slot7_Port2_Optical_Egress_NearEnd					1.2	True	2019/02/27 10:30:00		
68.21.72_Siol7_Porl2_Optical_Egress_NearEnd		2019/02/27 10:30:01		2019/02/27 10:30:01		True	2019/02/27 10:45:00		
68 21.72_Stol7_Port2_Optical_Egress_NearEnd		2019/02/27 10.45:01		2019/02/27 10.45:01		True	2019/02/27 11:00:00		
68 21 72_Siol7_Port2_Optical_Egress_NearEnd		2019/02/27 11:00:01		2019/02/27 11:00:01		True	2019/02/27 11:15:00		
68.21.72_Slot7_Port2_Optical_Egress_NearEnd		2019/02/27 11:15:01		2019/02/27 11:15:01	12	True	2019/02/27 11:30:00		
68.21.72_Stof7_Port2_Optical_Egress_NearEnd		2019/02/27 11:30:01			1.2	True	2019/02/27 11:45:00		
68 21 72_Slot7_Port2_Optical_Egress_NearEnd		2019/02/27 11:45:01		2019/02/27 11:45:01		True	2019/02/27 12:00:00		
68.21.72_Slof7_Port2_Optical_Egress_NearEnd				2019/02/27 12:00:01	1.2	True	2019/02/27 12:15:00		
68.21.72_Slot7_Port2_Optical_Egress_NearEnd						True	2019/02/27 12:30:00		
g 1 to 10 of 28 entries						Previous	2 3 Next		

Figure 9-45 Export History Data of Optical Power

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

102.160.21.72 ¥ Slot 7	• Port 2	FileName	Optical_pow	10					
hart Table		<u> </u>			Apply Close				
ow 10 + entries							Time Interval	Last Three Days	
		1.2			True				
		1.2	 Export all datas suc 	cessIThe file is stored	True				
		12	the 'report out' directory of	of the installation direc	tor				
		1.2	V.		True				
		1.2			True				
				Apr	NY Drawning	1 2 3 3			

Figure 9-46 Successfully Export Data of Optical Power

The exported data is saved in the directory of *NMS Installation* and the folder name is report_out. Open the folder to check the folder named Performance, which is all the exported data stored in Excel form. Analysis and troubleshooting can be made through the history data.

Data (D:) > NMS11037 > NM	S > report_out > performance	
~		
Optical_power.xls	2019/2/27 13:39	XLS

Figure 9-47 Successfully Exported Data of Optical Power

9.3.2. OCh History Performance Statistics

9.3.2.1. OCh History Monitoring Parameters Introduction

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

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

Performance Monitoring Point: entrance-near end.

Performance Monitoring Parameters: maximum differential group delay (DGD), minimum differential group delay (DGD), average differential group delay (DGD), maximum chromatic dispersion (CD), minimum chromatic dispersion (CD), average chromatic dispersion (CD), maximum optical signal-to-noise ratio (OSNR), minimum optical signal-to-noise ratio (OSNR), average optical signal-to-noise ratio (OSNR).

NE Please Select Slot	• Port	PM Granularity 15min			
Chart Table					
0.6			<u>тро</u> я	Time Interval Time Duration PM Point Select All	Please Select Please Select
0.4					⊒MinOSNR ∃AvgOSNR
0.2					
					Apply

Figure 9-48 OCh History Performance Parameters

9.3.2.2. 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.





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:

NE 192.168.66.111 V Port 1 V PM Granularity 15min	Ŧ	
Chart Table		
Show 10 • entries	Export Search: Search Time Interval Please Select	٣
Name II MaxDGD II MaxDGD Stamp II MinDGD II MinDGD Stamp II AvgDGD II MaxCD II MaxCD Stamp II Min	CD II MinCD Stamp II AvgCD II MaxOSNR II MaxOSNI Time Duration	
	No data available in table	
Showing 0 to 0 of 0 entries	Previous Next	
	Apply	7
		_



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:

now 10 v entries						Export	5	learch: Se	arch	Time Interval	Last Three Days	
Name 4	MaxDGD	MaxDGD Stamp	MinDGD	MinDGD Stamp	AvgDGD	MaxCD 11	MaxCD Stamp	MinCD	MinCD Stamp	Time Duration	2019/02/25 - 2019/02/27	
92.168.66.111 Slot1 Port1 OCh Ingress NearEn	1 3	2000/02/28 03:00:04	1	2000/02/28 03:01:39	2	12	2000/02/28 03:05:55	-11	2000/02/28 03:04:3			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEn	1 3	2019/02/28 03:15:01	1	2019/02/28 03:16:11	2	13	2019/02/28 03:17:31	-10	2019/02/28 03:22:1			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEn	1 3	2019/02/28 03:30:01	1	2019/02/28 03:30:05	2	13	2019/02/28 03:41:39	-9	2019/02/28 03:34:2			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEn	1 3	2019/02/28 03:45:57	:1	2019/02/28 03:45:22	2	12	2019/02/28 03:45:55	-9	2019/02/28 03:47:5			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEn	1 3	2019/02/28 04:00:07	:1	2019/02/28 04:00:03	2	12	2019/02/28 04:06:59	-13	2019/02/28 04:11:4			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEn	1 3	2019/02/28 04:15:21	1	2019/02/28 04:16:20	2	13	2019/02/28 04:23:12	-13	2019/02/28 04:22:0			
192.168.66.111_Slot1_Port1_OCh_Ingress_NearEn	1 3	2019/02/28 04:30:22	1	2019/02/28 04:30:01	2	13	2019/02/28 04:32:21	-9	2019/02/28 04:31:0			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEn	1 3	2019/02/28 04:45:19	1	2019/02/28 04:46:48	2	11	2019/02/28 04:58:34	-13	2019/02/28 04:49:5			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEn	1 3	2019/02/28 05:00.01	1	2019/02/28 05:00:05	2	13	2019/02/28 05:10:07	-10	2019/02/28 05:07:2			
192.168.66.111_Slot1_Port1_OCh_Ingress_NearEn	1 3	2019/02/28 05:15:22	1	2019/02/28 05:15:02	2	11	2019/02/28 05:23:16	-10	2019/02/28 05:23:1			
192 168 66 111_Slot1_Port1_OCh_Ingress_NearEn 192 168 66 111_Slot1_Port1_OCh_Ingress_NearEn 192 168 66 111_Slot1_Port1_OCh_Ingress_NearEn	1 3 1 3 1 3	2019/02/28 04 45 19 2019/02/28 05 00 01 2019/02/28 05 15 22	1	2019/02/28 04:46:48 2019/02/28 05:00:05 2019/02/28 05:15:02	2 2 2	11 13 11	2019/02/28 04 58:34 2019/02/28 05 10:07 2019/02/28 05:23:16	-13 -10 -10	2019/02/28 04:49:5 2019/02/28 05:07:2 2019/02/28 05:23:1			



9.3.2.3. 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:

2 192 188 66 111 * Slot 1 hart Table	Port 1	FileNa	ame	Can not conta	in /:*?*<≻∣sp	Apply C	ose				
10W 10 Tentries					Export]	earch: Search		Time Interval	Last Three Days	
Name II M	MaxDGD Stamp			AvgDGD 11		MaxCD Stamp			Time Duration	2019/02/25 - 2019/02/27	
	2000/02/28 03:00:04			2							
92.168.66.111 Slot1 Port1_OCh Ingress_NearEnd		1									
92 168 66 111_Slot1_Port1_OCh_ingress_NearEnd	2019/02/28 03:30:01		2019/02/28 03:30:05			2019/02/28 03:41:39	-9	2019/02/28 03:34.2			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEnd	2019/02/28 03:45:57		2019/02/28 03.45.22	.2		2019/02/28 03:45:55	-9	2019/02/28 03 47 5			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEnd	2019/02/28 04:00:07		2019/02/28 04:00:03	2		2019/02/28 04 06:59		2019/02/28 04:11:4			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEnd	2019/02/28 04:15:21		2019/02/28 04:16:20			2019/02/28 04:23:12		2019/02/28 04:22.0			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEnd	2019/02/28 04:30:22		2019/02/28 04:30:01			2019/02/28 04:32:21	-9	2019/02/28 04:31:0			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEnd	2019/02/28 04:45:19	1	2019/02/28 04:46:48			2019/02/28 04:58:34		2019/02/28 04 49:5			
92.168.66.111_Slot1_Port1_OCh_Ingress_NearEnd			2019/02/28 05:00:05								
		1			11	2019/02/28 05:23.16		2019/02/28 05 23:1			

Figure 9-52 Export History Data of OCh

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

	+ Slot 1	Point	FileN	ame	Och_data							
art Table							Apply C	lose				
ow 10 v entre										Time Interval	Last Three Days	
				2019/00			04.23.12					
				2019/00 - Expo	rt all datas succ	essIThe file is a	tored in 04:32:21					
				2019/01 the 'report	out' directory of	the installation	director 04 58 34					
				2019/05 V.			05:10:07					
				2019/03			05.23.16					
							Apply	1	and the second second			

Figure 9-53 Successfully Export Data of OCh

The exported data is saved in the directory of *NMS Installation* and the folder name is report_out. Open the folder to check the folder named Performance, which is all the exported data stored in Excel form. Analysis and troubleshooting can be made through the history data.

Data (D:) > NMS11037 > NMS >	${\sf report_out} \ > \ {\sf performance}$	
~		
Och_data.xls	2019/2/27 13:46	XLS
Optical_power.xls	2019/2/27 13:39	XLS

	Figure 9-54	Successfully	Exported	Data of	OCh
--	-------------	--------------	----------	---------	-----

9.3.3. FEC History Performance Statistics

9.3.3.1. FEC History Monitoring Parameters Introduction

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

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

Performance Monitoring Point: entrance-near end.

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



Figure 9-55 FEC History Performance Parameters

9.3.3.2. 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 9-56 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:

NE 192.168.66.111 * Slot 1	• Port 1	PM Granularity 15min	٣			
Chart Table						
Show 10 v entries			Export	Search: Search	Time Interval	Please Select V
Name 11 Max Corrected BER	11 Max Corrected BER Stamp	11 Avg Corrected BER	Suspect Interval Flag	11 Time Stamp	Time Duration	
	No data	a available in table				
Showing 0 to 0 of 0 entries				Previous Next		

Figure 9-57 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:

w 10 ¥ entries			Export	Search:	Search	Time Interval	Last Three Days	31
Name 41	Max Corrected BER	Max Corrected BER Stamp	Avg Corrected BER	Suspect Interval Flag 41	Time Stamp	Time Duration	2019/02/25 - 2019/02/27	
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.3445244E-4	2000/02/28 03:07:07	5.0351827E-4	False	2019/02/28 03:15:00			
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.326878E-4	2019/02/28 03:22:26	4.9740606E-4	True	2019/02/28 03:30:00			
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.3293124E-4	2019/02/28 03:31:31	4.895418E-4	True	2019/02/28 03:45:00			
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.274613E-4	2019/02/28 03:59:14	4.892528E-4	True	2019/02/28 04:00:00			
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.353003E-4	2019/02/28 04:01:00	5.0815113E-4	True	2019/02/28 04:15:00			
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.348025E-4	2019/02/28 04:18:38	5.039168E-4	True	2019/02/28 04:30:00			
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.2572496E-4	2019/02/28 04:31:35	4.989819E-4	True	2019/02/28 04:45:00			
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.2454683E-4	2019/02/28 04:53:05	4.935537E-4	True	2019/02/28 05:00:00			
2 168.66 111_Stot1_Port1_OTU-FEC_Ingress_NearEnd	5.2883785E-4	2019/02/28 05:05:31	4.962627E-4	True	2019/02/28 05:15:00			
2 168 66 111 Slot1 Port1 OTU-FEC Ingress NearEnd	5.154095E-4	2019/02/28 05:23:32	4.8634468E-4	True	2019/02/28 05:30:00			



9.3.3.3. Export FEC History Monitoring Information

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

102 168 66 111 * Stat 1	* Post 1	FileName	Can not contain 7:*?*<> sg	ecial characters				
art Table				Apply Close				
w 10 v entities			Export	Search:	Search.	Time Interval	Last Three Days	
Name Jš	Max Corrected BER	Max Corrected BER Stamp	Avg Corrected BER	Suspect Interval Flag	Time Stamp 11	Time Duration	2019/02/25 - 2019/02/27	
2 168 66 111 Slot1 Port1 OTU-FEC Ingress NearEnd	5.3445244E-4		5.0351827E-4	False				
2.168.66 111 Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.326878E-4	2019/02/28 03:22:26	4.9740606E-4	True	2019/02/28 03 30.00			
2 168 66 111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.3293124E-4		4.895418E-4	True	2019/02/28 03:45:00			
2 168.66 111_Stot1_Port1_OTU-FEC_Ingress_NearEnd	5.274613E-4	2019/02/28 03 59 14	4.892528E-4	True	2019/02/28 04:00:00			
2 168 66 111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.353003E-4	2019/02/28 04:01:00	5.0815113E-4	True	2019/02/28 04 15:00			
2 168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5:348025E-4	2019/02/28 04:18:38	5.039188E-4	True	2019/02/28 04:30:00			
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.2572496E-4	2019/02/28 04:31:35	4.989819E-4	True	2019/02/28 04:45:00			
2.168.66.111_Slot1_Port1_OTU-FEC_Ingress_NearEnd	5.2454683E-4	2019/02/28 04:53:05	4.935537E-4	True	2019/02/28 05:00:00			
2 168 55 111_Slot1_Port1_OTU-FEC_ingress_NearEnd	5.2683785E-4	2019/02/28 05:05:31	4.962627E-4	True	2019/02/28 05 15:00			
2.168.66.111_Slot1_Pont1_OTU-FEC_Ingress_NearEnd	5.154095E-4		4 8634466E-4	True	2019/02/28 05:30:00			

Figure 9-59 Export History Data of FEC

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

Home System Management		Fault Management Perform	nance Management Secu			▶124 0 78 0 2		
NE 192.168.66.111 + Slot 1	• Port 1	FileName	FEC_data					
Chart Table				Apply Close				
Show 10 + entries						Time Interval	Last Three Days	•
Name 14								
192 168 66 111 Slott Port OTU-FEC Ingress NearEnd								
192 168 66 111 Skott Port1 OTU-FEC Ingress_NearEnd								
192 168 66 111_Skit1_Port1_OTU-FEC_ingress_NearEnd								
192.166.66.111_Stol1_Port1_OTU-FEC_Ingress_NearEnd								
192 168 55 111_Slot1_Pott1_OTU-FEC_Ingress_NearEnd								
192.168.66.111_Skit1_Pont1_OTU-FEC_Ingress_NearEnd		2019/02/28 04 18		True				
192.168.66.111_Slot1_Pon1_OTU-FEC_Ingress_NearEnd		2019/02/28 04 31	mont all datas success. The file is	stored in				
192 168 66 111_Slot1_Port1_OTU-FEC_Ingress_NearEnd		2019/02/26 04 53 the Yep	ort out directory of the installation	n director				
192 168 66 111_Slot1_Port1_OTU-FEC_ingress_NearEnd		2019/02/28 05 05		True				
192 168 66 111_Stol1_Port1_OTU-FEC_Ingress_NearEnd		2019/02/28 05 23		True				
Showing 1 to 10 of 10 entries				Apply	Previous: 1 Next			
							Ap	

Figure 9-60 Successfully Export Data of FEC

The exported data is saved in the directory of *NMS Installation* and the folder name is report_out. Open the folder to check the folder named Performance, which is all the exported data stored in Excel form. Analysis and troubleshooting can be made through the history data.

Data (D:) > NMS11037 > NMS >	report_out > performance	
-		
FEC_data.xls	2019/2/27 13:49	XLS

Figure 9-61 Successfully Exported Data of FEC

9.3.4. OTUk/ODUk History Performance Statistics

9.3.4.1. OTUk/ODUk History Monitoring Parametes Introduction

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

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

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

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



Figure 9-62 OTUk/ODUk History Performance Parameters

9.3.4.2. 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 9-63 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:

Chail Table Export Search Time Interval Passe Select Passe Select Passe Select Time Duration Name 11 BBE I ES I UAS Suspect Interval Flag I Time Stamp Time Duration	NE 192.168.66.111	▼ Slot 1		▼ Port 3		,	PM Granularity	y 15min	Ŧ				
Show 10 entries Expert Search Time Interval Passe Select Passe Select Passe Select Time Interval Time Interval	Chart Table												
Name II BBE ES II UAS Suspect Interval Flag Time Stamp Time Duration	Show 10 v entries							Expo	rt	Search: Search	Time Interval	Please Select	*
No data avaitable in table	Name 斗	BBE 11	ES 🌵	† SES		UAS		Suspect Interval Flag		Time Stamp 11	Time Duration		
					No	o data availab	ole in table						
Showing 0 to 0 of 0 entries Previous Next	Showing 0 to 0 of 0 entries									Previous Next			

Figure 9-64 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:

.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd .168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd	0	0 0				
168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd			0	False	2019/02/28 03:15:00	
	0	0 0	0	True	2019/02/28 03:30:00	
168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd	0	0 0	0	True	2019/02/28 03:45:00	
168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd	0	0 0	0	True	2019/02/28 04:00:00	
168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd	0	0 0	0	True	2019/02/28 04:15:00	
168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd	0	0 0	0	True	2019/02/28 04:30:00	
168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd	0	0 0	0	True	2019/02/28 04:45:00	
168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd	0	0 0	0	True	2019/02/28 05:00:00	
168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd	0	0 0	0	True	2019/02/28 05:15:00	
168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd	0	0 0	0	True	2019/02/28 05:30:00	

Figure 9-65 15-Minute Tabular History Data of OTUk/ODUk

9.3.4.3. Export OTUk/ODUk History Monitoring Information

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

								017 W O 1000
E 192.168.66.111 • Slot 1	Y P	ort 3	FileName		Can not contain /:*?" <> special characters			
Chart Table			_		Apply	y Close		
Show 10 🔻 entries					Export	Search: Search	Time Interval	Last Three Days
Name 👫				UAS II	Suspect Interval Flag	11 Time Stamp	Time Duration	2019/02/25 - 2019/02/27
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					False	2019/02/28 03:15:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					True	2019/02/28 03:30:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					True	2019/02/28 03:45:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					True	2019/02/28 04:00:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					True	2019/02/28 04:15:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					True	2019/02/28 04:30:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd		0			True	2019/02/28 04:45:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					True	2019/02/28 05:00:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					True	2019/02/28 05:15:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					True	2019/02/28 05:30:00		

Figure 9-66 Export History Data of OTUk/ODUk

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

Home System Management		Fault Manageme Export	nt Performanc	Co Managoment Security Manager	ment Log Management OLP Rou ×	te ≽121 0 76 0 28	⊜ 17 ⊜ 0 root
NE 192.168.66.111 • Slot 1	▼ Pc	FileName		оти-ори			
Chart Table				L	Apply Close		
Show 10 • entries						Time Interval	Last Three Days
Name 💵							
192.168.66.111 Slot1 Port3 ODU4(0) Egress FarEnd							
192.168.66.111 Slot1 Port3 ODU4(0) Egress FarEnd							
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd							
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd							
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd							
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					2019/02/28 04:30:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd			 Export 	all datas success!The file is stored in	2019/02/28 04:45:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd			the 'report o	ut directory of the installation director	2019/02/28 05:00:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd			y		2019/02/28 05:15:00		
192.168.66.111_Slot1_Port3_ODU4(0)_Egress_FarEnd					2019/02/28 05:30:00		
Showing 1 to 10 of 20 entries			_	Apply	Previous 1 2 Next	I	
							Apply

Figure 9-67 Successfully Export Data of OTUk/ODUk

The exported data is saved in the directory of *NMS Installation* and the folder name is report_out. Open the folder to check the folder named Performance, which is all the exported data stored in Excel form. Analysis and troubleshooting can be made through the history data.

Data (D:) > NMS11037 > NM	1S > report_out > performance
CC data via	2010/2/27 12:40
	2019/2/27 13:49
Och_data.xls	2019/2/27 13:46
Optical_power.xls	2019/2/27 13:39
OTU-ODU.xls	2019/2/27 13:58

Figure 9-68 Successfully Exported Data of OTUk/ODUk

9.3.5. History Performance Statistics of SDH Regeneration Segment

9.3.5.1. History Monitoring Parameters Introduction of SDH Regeneration Segment

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

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

Performance Monitoring Point: entrance-near end.

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





9.3.5.2. View SDH Regeneration Segment History Monitoring Information

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



Figure 9-70 15-Minute Chart Data of SDH Regeneration Segment

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

NE 192.168.21.72	▼ Slot 16		♥ Port 9		▼ PM	Granularity 15min	*				
Chart Table											
Show 10 v entries						Export		Search: Search	Time Interval	Please Select	*
Name 斗	BBE IT	ES	It SES	UAS		Suspect Interval Flag		Time Stamp ↓↑	Time Duration		
				No data avai	ilable in tabl	le					
Showing 0 to 0 of 0 entries								Previous Next			



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

10 v entries					Export	Search: Search	Time Interval	Last Three Days
Name	BBE	ES II	SES 11	UAS 🕸	Suspect Interval Flag	Time Stamp ↓↑	Time Duration	2019/02/25 - 2019/02/27
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEn	d 0	0	0	900	True	2019/02/27 10:14:59		
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEn	d 0	0	0	900	True	2019/02/27 10:29:59		
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEn	d 0	0	0	900	True	2019/02/27 10:44:59		
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEn	d 0	0	0	900	True	2019/02/27 10:59:59		
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEn	d 0	0	0	900	True	2019/02/27 11:14:59		
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEn	d 0	0	0	900	True	2019/02/27 11:29:59		
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEn	0 b	0	0	900	True	2019/02/27 11:44:59		
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearE	0 b	0	0	900	True	2019/02/27 11:59:59		
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearE	d 0	0	0	900	True	2019/02/27 12:14:59		
168.21.72_Slot16_Port9_SDH-RS_Ingress_NearE	d 0	0	0	900	True	2019/02/27 12:29:59		
ng 1 to 10 of 16 entries						Previous 1 2 Next		

Figure 9-72 15-Minute Tabular History Data of SDH Regeneration Segment

9.3.5.3. Export SDH Regeneration Segment History Monitoring Information

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

Home System Management	Configuration	Management	Fault Manageme Export	ent Performan	ce Management Security Management	Log Management OLP Route	▶123 () 78 ()28	⊜ 17 @ 0 root
NE 192.198.21.72 • Stot 16 Chart Table	•	Port 9	FileName		Can not contain <i>I</i> : * ? * <> special characters Apply	Ciose		
Show 10 🔻 entries					Export	Search: Search	Time Interval	Last Three Days
Name 45					Suspect Interval Flag	Time Stamp	Time Duration	2019/02/25 - 2019/02/27
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd				900	True	2019/02/27 10:14:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd				900	True	2019/02/27 10:29:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd				900	True	2019/02/27 10:44:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd				900	True	2019/02/27 10:59:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd				900	True	2019/02/27 11:14:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd				900	True	2019/02/27 11:29:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd				900	True	2019/02/27 11:44:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd				900	True	2019/02/27 11:59:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd				900	True	2019/02/27 12:14:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd	0			900	True	2019/02/27 12:29:59		
Showing 1 to 10 of 16 entries						Previous 1 2 Next		

Figure 9-73 Export History Data of SDH Regeneration Segment

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

Home System Management	Configuration Management	Fault Management Por Export	formanco Managament Security Manag	ement Log Management OLP Route	▶ 123 () 78 () 28	●17 ●0 root
NE 192.168.21.72 T Slot 16	• Port 9	FileName	SDH_data			
Chart Table				Apply Close		
Show 10 v entries					Time Interval	Last Three Days
Name 🕸						
192.168.21.72 Slot16 Port9 SDH-RS Ingress NearEnd						
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd						
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd						
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd						
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd						
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd		0		2019/02/27 11:29:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd		0	Export all datas success!The file is stored in	2019/02/27 11:44:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd		0 the	'report out' directory of the installation director	2019/02/27 11:59:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd		0 v.	,	2019/02/27 12:14:59		
192.168.21.72_Slot16_Port9_SDH-RS_Ingress_NearEnd		0		2019/02/27 12:29:59		
Showing 1 to 10 of 16 entries			Apply	Previous 1 2 Next		
						Apply

Figure 9-74 Successfully Export Data of SDH Regeneration Segment

The exported data is saved in the directory of *NMS Installation* and the folder name is report_out. Open the folder to check the folder named Performance, which is all the exported data stored in Excel form. Analysis and troubleshooting can be made through the history data.

Data (D:) > NMS11037 > NMS	> report_out > performance	
EFC data vis	2010/2/27 12:40	VIC
Ch data.xls	2019/2/27 13:49	XLS :
Optical_power.xls	2019/2/27 13:39	XLS
OTU-ODU.xls	2019/2/27 13:58	XLS]
SDH_data.xls	2019/2/27 14:02	XLS

Figure 9-75 Successfully Exported Data of SDH Regeneration Segment

9.3.6. History Performance Statistics of Ethernet

9.3.6.1. Ethernet History Monitoring Parameters Introduction

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

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

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

Performance Monitoring Parameters: The monitoring parameters of Ethernet monitoring point include normal frame number, unicast frame number, unicast 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.





9.3.6.2. 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.

NE 192	2.168.66.111	▼ Slot 1	Port 3	PM Granu	alarity 15min	Ŧ				
Chart	Table									
180	ר 0,000,000,000 T						110¥	Time Interval	Last Three Days	٣
	ĺ						0	Time Duration	2019/02/25 - 2019/02/27	
								PM Point	Ethernet_Ingress_NearEnd	٠.
150	0,000,000,000 -							Select All	Good Frame Unicast Frame Multicast Frame Broadcast Frame CCCC Error Frame	
120	0,000,000,000 -								Alignment Error Frame Frame Too Long Jabber Frame Fragment Frame	
90	0,000,000,000 ⁻								Characteristics of the second	
60	0,000,000,000 -								 ²256-511 Byte Frame ²512-1023 Byte Frame ²1024-1518 Byte Frame ²1024-1518 Ayte Frame ²1519-Maximun Frame 	
30	0,000,000,000 -									Apply
	0* NaN-NaN	NaN-NaN NaN-NaN	NaN:NaN NaN-NaN	NaN:NaN NaN-NaN	NaN:NaN NaN-NaN	NaN-NaN NaN-Na	, NaN:NaN			

Figure 9-77 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:

Chai Table Shor 10 + entries Export Search. Name: IL Good Frame: IL Multicast Frame: IL Broadcast Frame: IL Showing 0 to 0 of 0 entries Previous Next	NE 192.168.66.111 ¥ Port 3 ¥ PM Granularity 15min	٣				
Show Lopot Search. Time Interval Pieze Select Name IL Good Frame II Unicast Frame II Broadcast Frame II CRC Error Frame II Alignment Error Frame II Frame Too Long II Jabber Frame II Fragment Frame Showing 0 to 0 of 0 entries Piezoas Vectors Next	Chart Table					
Name II Good Frame II Unicast Frame II Multicast Frame II CRC Error Frame II Alignment Error Frame II Frame Too Long II Jabber Frame II Fragment Frame Showing 0 to 0 of 0 entres Previous Next	Show 10 v entries	Export	Search: Search	Time Interval	Please Select	٣
Showing 0 to 0 of 0 entries Previous Next	Name 🕸 Good Frame 🗊 Unicast Frame 🕸 Multicast Frame 🕸 Broadcast Frame 🗊 CRC Error Frame 🕸 Alignment Error Frame	e $\downarrow\uparrow$ Frame Too Long $\downarrow\uparrow$	Jabber Frame 🕸 Fragment Frame	Time Duration		
	Showing 0 to 0 of 0 entries		Previous Next			

Figure 9-78 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:

now 10 v entries					Export	Search: Search.		Time Interval	Last Three Days
Name 15	Good Frame $\downarrow\uparrow$	Unicast Frame 1	Multicast Frame 1	Broadcast Frame 1	CRC Error Frame 1	Alignment Error Frame 1	Frame Too Lor	Time Duration	2019/02/25 - 2019/02/27
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	175587871239	0	0	0	N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171570183614	0	0	0	N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171570217363	0	0	0	N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171719055322	0	0	0	N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171272576963	0	0	0	N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171421359150	0	0	0	N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171719055138	0	0	0	N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171421401917	0	0	0	N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171719018126	0	0	0	N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171421397803	0	0	0	N/A	N/A	N/A		
nowing 1 to 10 of 24 entries						Previous 1 2	3 Next		



9.3.6.3. Export Ethernet History Monitoring Information

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

Home System Management	t Configuration M	Management Fa	ult Management	Performance Manager	ent Security Mana	aement Loo Managemen	t OLP Route	⊳ 97 ⊘ 74 © 8	€17 60 root
NE 192.168.66.111 ¥ Slot 1	v P	ort 3	FileName	Can not cont	ain /:*?*<> special chara	acters			
Chart Table						Apply Close			
Show 10 v entries					Export	Search: Search.		Time Interval	Last Three Days
Name 👫	Good Frame 11	Unicast Frame 11	Multicast Frame 11	Broadcast Frame 1	CRC Error Frame 1	Alignment Error Frame	Frame Too Lor	Time Duration	2019/02/25 - 2019/02/27
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd					N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171570183614				N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171570217363				N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171719055322				N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171272576963				N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171421359150				N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171719055138				N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171421401917				N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd	171719018126				N/A	N/A	N/A		
192.168.66.111_Slot1_Port3_Ethernet_Egress_NearEnd					N/A	N/A	N/A		
Showing 1 to 10 of 24 entries						Previous 1 2	3 Next		

Figure 9-80 Export History Data of Ethernet

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

	▼ Slot 1	٣	FileName	Ethernet_dat	a				
Chart Table						Apply Close			
Show 10 v entrie								Time Interval	Last Three Days
			0			N/A			
			0	 Export all datas succ 	cess!The file is stored in	N/A			
			0	the 'report out' directory of	of the installation director	N/A			
			0	y /		N/A			
			0			N/A			
					Apply	Previous 1 2	3 Next		

Figure 9-81 Successfully Export Data of Ethernet

The exported data is saved in the directory of *NMS Installation* and the folder name is report_out. Open the folder to check the folder named Performance, which is all the exported data stored in Excel form. Analysis and troubleshooting can be made through the history data.



Figure 9-82 Successfully Exported Data of Ethernet

10. Abbreviation

This chapter introduces some Acronym Definition. It mainly includes:

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

OTU	Optical Transponder Unit
PM	Path Monitoring
РТ	Payload Type
SM	Section Monitoring
SNMP	Simple Network Management Protocol
ТП	Trail Trace Identifier

Table 10-1 Acronym Definition