



UNM2000

**Network Convergence
Management System V2.0R4SP6**

Operation Guide

Version: B

Code: MN000003316

FiberHome Telecommunication Technologies Co., Ltd.

April 2018 二零一八年四月

Thank you for choosing our products.

We appreciate your business. Your satisfaction is our goal. We will provide you with comprehensive technical support and after-sales service. Please contact your local sales representative, service representative or distributor for any help needed at the contact information shown below.

Fiberhome Telecommunication Technologies Co., Ltd.

Address: No. 67, Guanggu Chuangye Jie, Wuhan, Hubei, China

Zip code: 430073

Tel: +6 03 7960 0860/0884 (for Malaysia)

+91 98 9985 5448 (for South Asia)

+593 4 501 4529 (for South America)

Fax: +86 27 8717 8521

Website: <http://www.fiberhomegroup.com>

Legal Notice

烽火通信®

FiberHome®

GONST®

FONST®

e-Fim®

CiTRANS®

E-jet®

IBAS®

Freelink®

FonWeaver®

OTNPlanner™

SmartWeaver™

are trademarks of FiberHome Telecommunication Technologies Co., Ltd.
(Hereinafter referred to as FiberHome)

All brand names and product names used in this document are used for identification purposes only and are trademarks or registered trademarks of their respective holders.

All rights reserved

No part of this document (including the electronic version) may be reproduced or transmitted in any form or by any means without prior written permission from FiberHome.

Information in this document is subject to change without notice.

Preface

Version

Version	Description
A	Initial version, corresponding to the UNM2000 V2.0R4 version.
B	Updated version, corresponding to the UNM2000 V2.0R4SP6 version.

Related Documentation

Document	Main Content	Phase to Use
<i>UNM2000 Network Convergence Management System Product Description</i>	Product positioning, features, basic functions, network and application, and technical specification.	Network planning
<i>UNM2000 Network Convergence Management System Standalone System Installation and Deployment Guide (Based on Windows)</i>	Introduces how to install the UNM2000 Network Convergence Management System on the Windows operating system.	Service deployment
<i>UNM2000 Network Convergence Management System Standalone System Installation and Deployment Guide (Based on SUSE Linux)</i>	Introduces how to install the UNM2000 Network Convergence Management System on the SUSE Linux operating system.	Service deployment
<i>UNM2000 Network Convergence Management System Operation Guide</i>	Introduces the operation guidelines of the UNM2000 Network Convergence Management System.	Network maintenance
<i>UNM2000 Network Convergence Management System GUI Reference</i>	The meaning and usage constraints of shortcut menu items and buttons in the menus and windows.	Service deployment / network maintenance

Intended Readers

This manual is intended for the following readers:

- ◆ Commissioning engineers
- ◆ Operation and maintenance engineers

To utilize this manual, these prerequisite skills are necessary:

- ◆ Data communication technology
- ◆ Access network technology

Terminology Conventions

Terminology	Convention
UNM2000	FiberHome UNM2000 Network Convergence Management System

Symbol Conventions

Symbol	Convention	Description
	Note	Important features or operation guide.
	Caution	Possible injury to persons or systems, or cause traffic interruption or loss.
	Warning	May cause severe bodily injuries.
	Jump	Jumps to another step.
	Cascading menu	Connects multi-level menu options.
	Bidirectional service	The service signal is bidirectional.
	Unidirectional service	The service signal is unidirectional.

Operation Safety Rules



The network management computer should be placed away from direct sunlight, electromagnetic interference, heat source, humidity and dust, and with at least 8cm distance from other objects in order to keep good ventilation.



Use UPS power supply to avoid loss of network management data caused by accidental power failure.



The computer case, UPS power supply and switch (or hub) should be connected to protection earth ground.



To shut down the network management computer, exit the operation system normally and then shut off the power supply.



Do not exit the network management system when it is working normally. Exiting the network management system does not interrupt traffic in the network, but precludes centralized control of the networked equipment.



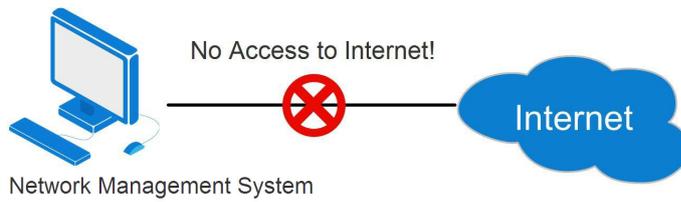
The network management computer cannot be used for purposes other than network management. Use of unidentified memory devices should be prohibited so as to avoid computer viruses.



Do not delete any file in the network management system randomly or copy any irrelevant file into the network management computer.

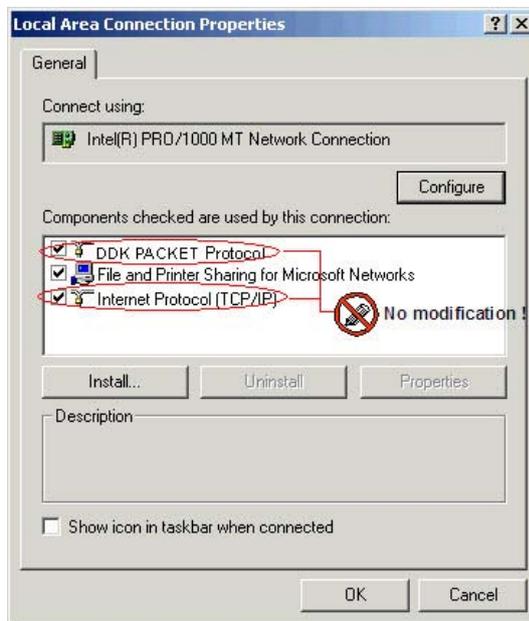


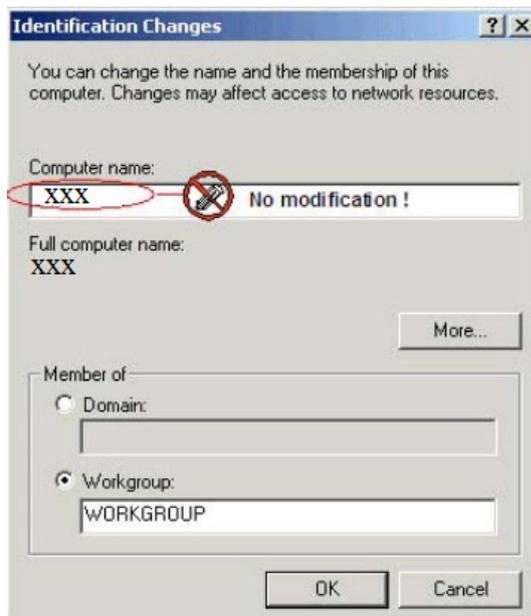
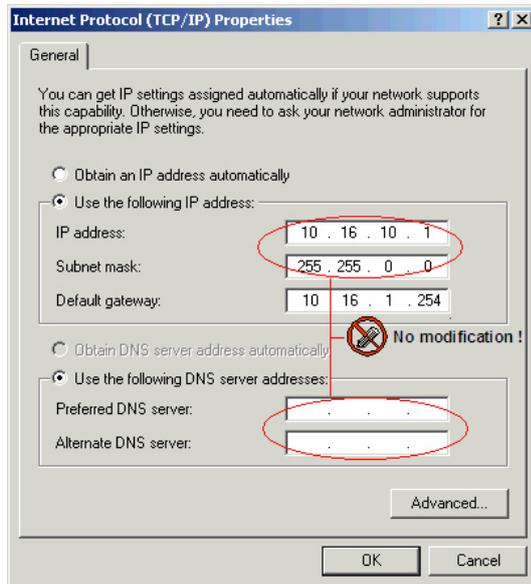
Do not visit Internet via the network management computer. Doing so may increase data flow in the net card and hence affects normal network management data transmission or results in other accidents.

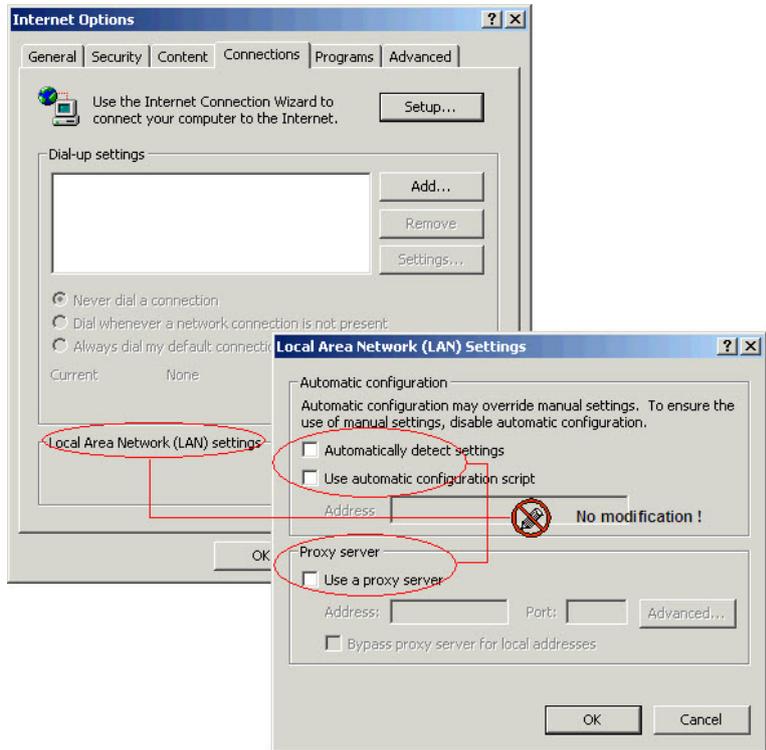


⚠ Do not perform service configuration or expansion during service busy hours via the network management system.

⚠ Do not modify the network management computer's protocol settings, computer name or LAN settings. Doing so may result in abnormal operation of network management system.







Contents

Preface.....	I
Operation Safety Rules	III
1 Overview	1
1.1 Deployment of the UNM2000 in the TMN.....	2
1.2 Manageable Device Types.....	2
2 Basic Operations of the UNM2000	4
2.1 Login / Logout.....	5
2.1.1 Downloading Client End.....	5
2.1.2 Logging into the UNM2000 Client.....	6
2.1.3 Logging Out of the UNM2000 Client	7
2.2 Views the UNM2000 Version.....	7
2.3 GUI Introduction	7
2.3.1 GUI	8
2.3.2 Shortcut Icons.....	8
2.3.3 Common Shortcut Keys	11
2.4 Menu Description.....	12
2.4.1 System	12
2.4.2 View	14
2.4.3 Resource.....	15
2.4.4 Configuration	17
2.4.5 Alarm.....	18
2.4.6 Performance.....	20
2.4.7 Security	20
2.4.8 Window	21
2.4.9 Help	22
2.5 Setting UNM2000 System Parameters	22
2.5.1 Setting the Display of the Browse Tree	22
2.5.2 Setting the Time Mode	23
2.5.3 Setting the Topology Display	24

	2.5.4	Setting Ping Parameters	25
	2.5.5	Setting the Telnet / SSH Proxy Server	26
	2.5.6	Setting the Font	27
	2.5.7	Setting the Default Opening Page for NE Manager	27
	2.5.8	Setting the Personalization Switch	28
	2.5.9	Setting the GUI Display	29
	2.5.10	Setting the NE Manager	29
2.6		Setting the XFTP Server	30
2.7		Setting the Default Workspace	32
2.8		Basic Operations of the UNM2000	33
	2.8.1	Updating the License	33
	2.8.2	Modifying the User Password	34
	2.8.3	Locking the Terminal	35
	2.8.4	Logging Out Users	35
	2.8.5	Viewing the Message Platform	36
	2.8.6	Managing the Toolbar	36
	2.8.7	Customizing Views	38
3		Security Management	39
	3.1	User Security Concepts	40
	3.2	User Security Policy Management	43
	3.2.1	Setting the User Login Mode	43
	3.2.2	Setting the Access Control List	44
	3.2.3	Setting the Account Policy	45
	3.2.4	Setting the Password Policy	46
	3.3	Managing UNM2000 Users	47
	3.3.1	Operation Set Management	47
	3.3.2	Object Set Management	50
	3.3.3	Managing User Groups	53
	3.3.4	Managing Users	58
	3.4	Managing User Sessions	64
	3.4.1	Monitoring the User Session	64
	3.4.2	Logging Out Users	66
	3.4.3	Sending Messages to Online Users	67
	3.4.4	Monitoring User Activities	68

3.5	Authorization and Domain Division	69
4	Configuration Management	72
4.1	NE Communication Route Management	73
4.1.1	NE Management Program	73
4.1.2	Partition Policy Management	77
4.2	SNMP Parameter Template	78
4.2.1	Creating and Using the SNMP Parameter Template	78
4.2.2	Modifying / Deleting an SNMP Parameter Template	79
4.3	ONU Capability Set Template	80
4.3.1	Adding an ONU Capability Set Template	80
4.3.2	Modifying an ONU Capability Set Template	81
4.4	Managing Global Templates	82
4.4.1	Viewing the Global Template	82
4.4.2	Adding a Global Template	83
4.4.3	Modifying a Global Template	84
4.4.4	Binding / Unbinding a Global Template	85
4.4.5	Deleting a Global Template	86
4.5	Managing Global Configurations	87
4.5.1	Viewing Global Configurations	87
4.5.2	Adding the Global Configuration	88
4.5.3	Modifying the Global Configuration	88
4.5.4	Issuing the Global Configuration to Device	89
4.5.5	Deleting a Global Configuration Template	90
4.6	Tracing Signaling	91
4.7	Configuration Synchronization	92
4.8	Network Access Management	93
4.9	Pinging NEs	95
4.10	Telnet NE	95
4.11	The Tracert Function of the UNM2000 Server	96
4.12	Migrating the PON Configuration	97
5	Topology Management	98
5.1	Topology Creation Flow	99

5.2	Creating a Global Logical Domain	100
5.3	Creating NEs	101
5.3.1	Create Access NE	101
5.3.2	Automatic Discovery of NEs	102
5.4	Adding Cards	105
5.4.1	Adding Cards Automatically	105
5.4.2	Adding Cards Manually	106
5.5	Creating a Link	107
5.6	Editing an NE	108
5.6.1	Setting NE Attributes	108
5.6.2	Editing Icons	109
5.6.3	Setting the Displayed Content of the Icon	110
5.6.4	Tagging the NE	110
5.6.5	Querying a Label	110
5.6.6	Modify NE Names in a Batch Manner	111
5.7	Editing a Fiber Connection	113
5.7.1	Modifying the Connection Line Properties	113
5.7.2	Setting the Display Mode of the Connection Line	113
5.8	Browsing the Topology View	114
5.8.1	Checking the Physical Topology View	114
5.8.2	Viewing the Sub-topology View	115
5.8.3	Viewing the Thumbnail	117
5.8.4	Searching Objects	117
5.9	Deleting the Topology	119
5.9.1	Deleting the Global Logical Domain	119
5.9.2	Delete the NE	119
5.9.3	Deleting the Card	120
6	Managing Access NEs	121
6.1	NE Manager GUI	122
6.2	Configuring the Local Service	123
6.3	ONU Query Management	124
6.3.1	Querying ONUs	124
6.3.2	Viewing the ONU List	125

	6.3.3	ONU Query Example	128
6.4		Authorizing ONUs	129
	6.4.1	Configuring the ONU Whitelist.....	129
	6.4.2	Managing ONU Authentication Modes.....	130
	6.4.3	Managing PON Port Authentication Modes.....	132
	6.4.4	Replacing the ONU Logical Identifier.....	133
	6.4.5	Viewing the Authorized ONU Information.....	133
6.5		ONU Registration Management	134
	6.5.1	ONU RMS Error Information Query	135
	6.5.2	Querying the ONU Network Access Interception Logs	135
6.6		Rule Tasks of Enabling the ONU Port	135
	6.6.1	Viewing Rule Tasks.....	136
	6.6.2	Creating a Rule Task.....	136
	6.6.3	Executing Rule Tasks.....	137
6.7		Authorizing Cards	137
6.8		Synchronizing ONUs Manually.....	138
6.9		Obtaining Unauthorized ONUs	139
6.10		Authorizing ONUs Manually	139
6.11		OTDR Link Management	140
6.12		System Maintenance	142
6.13		Upgrading Cards	142
	6.13.1	System Software Upgrade Task	143
	6.13.2	Tasks of Upgrading ONUs in a Batch Manner	145
	6.13.3	Tasks of Upgrading System Cards in a Batch Manner.....	147
	6.13.4	System Software Upgrade Task	150
6.14		Managing Test Tasks	152
	6.14.1	Managing POTS Port Internal / External Line Test Tasks..	152
	6.14.2	Managing VOIP PING Tasks	154
6.15		Managing NE Automatic Discovery Tasks	157
	6.15.1	Viewing NE Automatic Discovery Tasks.....	157
	6.15.2	Creating an NE Automatic Discovery Task.....	158
7		Alarm Management	159
	7.1	Basic Concepts.....	160

7.2	Setting Alarm Related Parameters	164
7.2.1	Managing Alarm Reporting Rules	164
7.2.2	Managing Alarm Filter Rules	166
7.2.3	Setting the Audible Alarms	171
7.2.4	Enabling / Disabling the Audio Alarm.....	172
7.2.5	Setting the Display Modes of New Alarms / Events	172
7.2.6	Setting the Alarm Color	173
7.2.7	Setting Other Items of the Local Alarms.....	174
7.2.8	Setting the Definition of the Alarm History	175
7.2.9	Setting the Alarm Automatic Confirmation Rules.....	175
7.2.10	Converting Events to Alarms	177
7.2.11	Customizing Alarms.....	177
7.3	Managing Alarm / Event Templates	181
7.3.1	Alarm Template.....	181
7.3.2	Event Template.....	186
7.4	Synchronizing Alarms	188
7.4.1	Synchronizing Alarms Manually	188
7.5	Monitoring Network Alarms	189
7.5.1	Viewing current alarms.....	189
7.5.2	Viewing Alarm History	192
7.5.3	Viewing Related Alarms	195
7.5.4	Viewing Alarm Details	195
7.5.5	View alarm logs.	197
7.5.6	Viewing the Alarm Log Statistics	199
7.5.7	Viewing Alarm Statistics.....	201
7.5.8	Querying Reported Events	204
7.5.9	Viewing Reported Alarms.....	206
7.6	Handling Alarms	207
7.6.1	Confirming Alarms	207
7.6.2	Clearing Alarms Manually	208
7.6.3	Confirming and Clearing Alarms.....	209
7.6.4	Locating Alarms.....	209
7.6.5	Shielding Alarms.....	210
7.6.6	Modifying Alarm Levels	211
7.6.7	Editing Alarm Remarks	211

	7.6.8	Exporting the Alarm Information	212
	7.6.9	Editing Alarm Maintenance Experience	212
	7.6.10	Managing Maintenance Experience	213
7.7		Customizing Alarms	214
	7.7.1	Custom Alarm Name.....	214
	7.7.2	Custom Alarm Level.....	215
7.8		Alarm / Event Remote Notification	217
	7.8.1	Setting the Notification Communication Parameters	217
	7.8.2	Setting the Remote Notification Format of the Alarm / Event.....	217
	7.8.3	Setting the Remote Notification Sending Rules of the Alarm / Event.....	218
	7.8.4	Setting the Sending Delay of the Alarm / Event Remote Notification	219
	7.8.5	Sending Alarm / Event Remote Notification	221
7.9		Managing the Alarm / Event Data	221
	7.9.1	Setting the Alarm / Event Overflow Saving.....	222
	7.9.2	Setting the Manual Alarm / Event Saving	224
7.10		Alarm Logs	225
7.11		Managing Alarm Frequency Analysis Rules.....	228
8		Performance Management.....	230
	8.1	Basic Concepts.....	231
	8.2	Managing Performance Query Templates.....	232
	8.2.1	Viewing Performance Templates	232
	8.2.2	Creating a Performance Query Template.....	232
	8.2.3	Modifying a Performance Query Template	234
	8.3	Setting the Performance Collection Time	234
	8.4	Configuring the Performance Classification Switch in a Batch Manner.....	235
	8.5	Managing the Card Performance.....	235
	8.5.1	Viewing the Current Performance.....	236
	8.5.2	Viewing Performance History	237
	8.5.3	Viewing the Performance Comparison.....	239
	8.5.4	Viewing Real-time Performance	240

	8.5.5	View Performance History Trend	241
8.6		Managing Performance Collection.....	242
	8.6.1	Managing Performance Indicator Sets.....	242
	8.6.2	Managing Performance Threshold Sets.....	244
	8.6.3	Managing Performance Collection Tasks.....	247
8.7		Managing Performance Data	249
	8.7.1	Setting the Performance Overflow Saving	250
	8.7.2	Setting Manual Performance Saving	252
	8.7.3	Analysis of PON traffic statistics	253
	8.7.4	Enabling / disabling FTP Report.....	254
	8.7.5	Top Ranking Statistics.....	256
8.8		Managing Statistics Export Task.....	257
	8.8.1	Export Task of Traffic Analysis.....	257
	8.8.2	Export Task of TopN Traffic Ranking.....	259
	8.8.3	Export Task of 15-minute Performance.....	260
	8.8.4	Export Task of Equipment Traffic and 15-minute Performance of Health Degree.....	261
9		Log Management.....	263
	9.1	Log Management Policy.....	264
	9.2	Log Type	265
	9.2.1	System Logs.....	265
	9.2.2	Operation Logs	266
	9.2.3	Security Logs.....	267
	9.2.4	Northbound Interface Command Logs.....	268
	9.3	Log Statistics	270
	9.4	Managing System Logs	272
	9.4.1	Managing System Log Template	272
	9.4.2	Searching System Logs	274
	9.5	Managing Operation Logs.....	275
	9.5.1	Managing Operation Log Templates.....	275
	9.5.2	Querying Operation Logs	277
	9.6	Managing Security Logs.....	280
	9.6.1	Managing Security Log Template	280

	9.6.2	Querying Security Logs.....	282
9.7		Managing Northbound Interface Command Logs.....	284
	9.7.1	Managing TL1 Command Log Templates	284
	9.7.2	Querying TL1 Command Logs	285
	9.7.3	Querying the Web Service Command Log Template	287
	9.7.4	Querying the Web Service Command Logs	289
9.8		Managing Log Data.....	290
	9.8.1	Managing the Log Forwarding Server.....	290
	9.8.2	Setting the Log Overflow Saving	293
	9.8.3	Setting Manual Log Saving	294
10		Resource Management.....	297
	10.1	Managing Resource Statistics Template	299
		10.1.1 Viewing Resource Statistical Templates	299
		10.1.2 Customizing a Resource Statistical Template	301
	10.2	Physical Resource Statistics	302
	10.3	Resource Statistics of Other Types.....	303
	10.4	Exporting Physical Resource Statistics.....	304
	10.5	Exporting Resource Statistics of Other Types	306
	10.6	Example of Resource Statistics.....	307
	10.7	Importing the ODN NSM Information	309
	10.8	Querying Multiple ONUs	310
	10.9	Query Board By Serial Number	312
	10.10	Querying the MDU Phone Number.....	313
	10.11	ONU RMS Error Information Query	314
	10.12	Querying the ONU Network Access Interception Logs	315
	10.13	Importing GIS Data in a Batch Manner	316
	10.14	Gateway Type Config.....	316
	10.15	Unauthorized ONU List	317
	10.16	Modify ONU Names by Importing EXCEL.....	318
11		Data Synchronization and Backup.....	319
	11.1	Managing Data Synchronization Task.....	320

11.1.1	Managing Software / Hardware Version Upgrade Tasks...	320
11.1.2	Managing Configuration Upload Tasks	320
11.2	Backing Up Data.....	324
11.2.1	Managing Software Backup Tasks.....	324
11.2.2	Managing Configuration Export Tasks	326
11.2.3	Managing Card Software Backup Tasks	329
11.2.4	Export Tasks of MAC Address Table.....	332
12	Application Scenarios	336
12.1	Alarm Management	337
12.2	Performance Management.....	340
12.3	Authorization and Domain Division.....	342
12.4	Guaranteeing Device Configuration.....	344
Appendix A	Abbreviations	346

1 Overview

The following introduces the product positioning and GUI of the UNM2000.

- Deployment of the UNM2000 in the TMN
- Manageable Device Types

1.1 Deployment of the UNM2000 in the TMN

The TMN provides hierarchical network architecture and standard network interfaces. It is composed of the business management layer (BML), the network management layer (NML), and the element management layer (EML). This type of composition is called the network management architecture of the TMN.

The UNM2000 locates at the NML and EML in the TMN architecture and manages the devices in the access network, transport network and IP network, as shown in Figure 1-1.

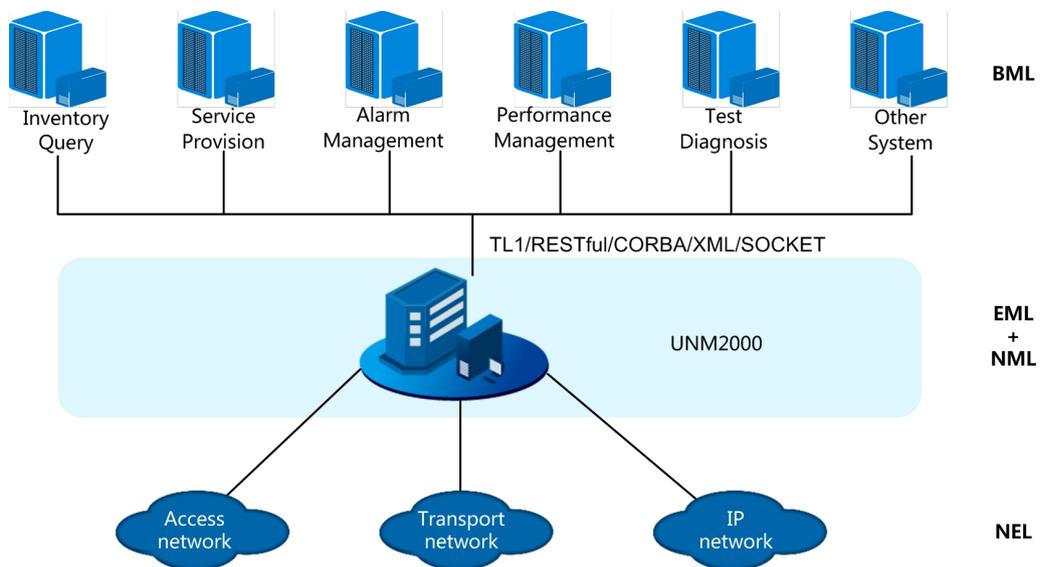


Figure 1-1 Deployment of the UNM2000 in the TMN

1.2 Manageable Device Types

Table 1-1 lists the devices that can be managed by the UNM2000.

Table 1-1 Manageable Devices

Type	Device Model
OLT	AN5116-06B, AN5516-06, AN5116-02, AN5516-04 and AN5516-04B.
ONU	<ul style="list-style-type: none">◆ GPON: AN5506-02-D/F, AN5506-04-B2/D/F1/FA/FAT, AN5506-07A/09A/10A and AN5506-07B/09B/10B.◆ XGPON: AN5646T/Q, AN5656T, AN5221-8N/16N/24N and AN5231-8N/16N/24N.◆ EPON: AN5006-07A/09A/10A and AN5006-07B/09B/10B.◆ 10GEPON: AN5200-07A/09A/10A and AN5200-07B/09B/10B.
MSAN	AN5006-20, AN5006-30, AN5006-15, AN5006-16, AN5220 and AN5516.

2 Basic Operations of the UNM2000

The following introduces the basic operations of the UNM2000, including the following content:

- Login / Logout
- Views the UNM2000 Version
- GUI Introduction
- Menu Description
- Setting UNM2000 System Parameters
- Setting the XFTP Server
- Setting the Default Workspace
- Basic Operations of the UNM2000

2.1 Login / Logout

The following introduces how to log into and log out of the UNM2000 client.

2.1.1 Downloading Client End

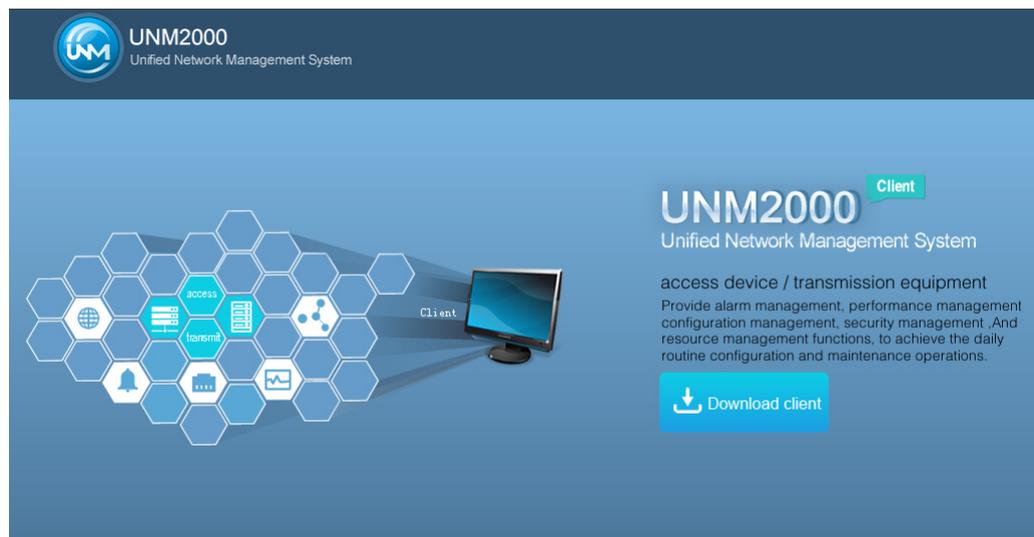
The following introduces how to install the UNM2000 client end.

Prerequisite

- ◆ You have logged in to the system as an administrator.
- ◆ The services of the UNM2000 server are started.
- ◆ The communication between the client and server is normal (You can ping far-end IP address command to check whether the network communication is normal).

Procedure

1. In the address bar of the browser, enter **IP:8080/webstart/** (IP indicates the IP address of the computer when UNM2000 server resides) to open the GUI below.



2. Click  , and click **Save** in the dialog box that appears.
3. In the **Save as** dialog box, click **Save** to download the client end installation file.

2.1.2 Logging into the UNM2000 Client

After logging into the UNM2000 client, you can perform configuration management on the equipment through the GUI of the UNM2000 client.

Prerequisite

- ◆ You have logged in to the system as an administrator.
- ◆ The services of the UNM2000 server are started.
- ◆ The communication between the client and server is normal (You can Ping far-end IP address command to check whether the network communication is normal).
- ◆ The client IP address is included in the access control list (ACL) of the UNM2000. For details about ACL, see [Setting the Access Control List](#).
- ◆ You have been assigned with the valid user account and the password.
- ◆ The UNM2000 client is installed.

Procedure



1. Double-click the  icon on the desktop.
2. In the **Server** field of the **Log into UNM2000** window, enter an IP address or select a desired UNM2000 server IP address from the drop-down list.

The default port for logging into the server is **52001**. If you want to modify the port, refer to the following steps and set **Server** field.

- 1) Click , and click **Add** In the **Server IP Management** dialog box.
- 2) In the highlighted row, enter **IP Address**, **Port Number**, and **Host Name**, and click **OK**.
3. In the **Log into UNM2000** dialog box, enter the valid username and password and click **OK**.



Note:

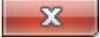
After the UNM2000 is installed, the default login username **admin** and password **admin** are provided. You need to change the password immediately after logging into the UNM2000 to ensure the network system security.

2.1.3 Logging Out of the UNM2000 Client

Prerequisite

The UNM2000 client is running normally.

Procedure

1. In the **UNM2000** window, select **System**→**Exit** or click .
2. Click **Yes** in the displayed **Confirm to Exit from the System**.

2.2 Views the UNM2000 Version

You can view the version information of the UNM2000 through the UNM2000 client.

Prerequisite

You have logged into the UNM2000 client.

Procedure

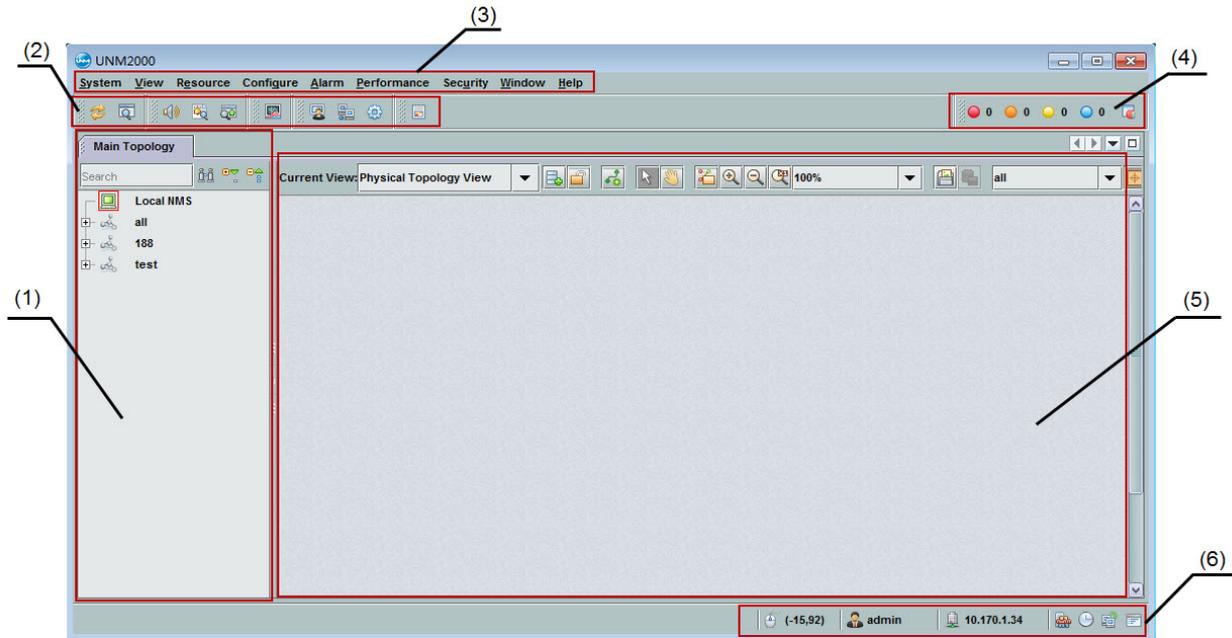
1. Select **Help**→**About UNM2000**.
2. View the UNM2000 version in the displayed window.

2.3 GUI Introduction

Understanding the GUI of the UNM2000 client helps you quickly locate the access methods of various operations and improves the operation efficiency.

2.3.1 GUI

The main GUI of the UNM2000 consists of the object tree pane, toolbar and menu bar, as shown in Figure 2-1.



- | | | |
|-----------------------------|------------------|----------------|
| (1) Object tree pane | (2) Toolbar | (3) Menu bar |
| (4) Alarm statistical panel | (5) Display pane | (6) Status bar |

Figure 2-1 UNM2000 System Main GUI

2.3.2 Shortcut Icons

The following introduces the shortcut icons commonly used in the OTNM2000 GUI.

Shortcut Icons on the Toolbar

Table 2-1 describes the default shortcut icons on the toolbar.

Table 2-1 Default Shortcut Icons in the Toolbar

Category	Symbol	Name	Description
Common functional area		Refresh	Refreshes the current view.
		Search Object	Searches for and locates a desired object.
Alarm		Alarm Prompt Tone Is On	Click the icon to enable / disable the alarm sound prompt.
		The alarm sound prompt is turned off	Click the icon to enable / disable the alarm sound prompt.
Alarm		Current alarm query	Views the current alarms.
		Query Reported Events	Views the reported events.
Performance		Performance history query	Views the performance history.
Others		EMS User Management	Opens the NMS User Management tab to manage the users.
		NE Communication Route Management	Opens the Communication Routing Management tab to manage the NE communication routes.
		Parameter Settings	Opens the Parameter Settings dialog box to set the system parameters.
Help		Legend	Opens the Legend pane to view the system legend.
Alarm Statistics		Critical	Dynamically displays the number of critical alarms; Click this icon to open the Current Alarm - All Objects - Critical tab and view critical alarms.
		Major	Dynamically displays the number of major alarms; Click this icon to open the Current Alarm - All Objects - Major tab and view major alarms.
		Minor	Dynamically displays the number of minor alarms; Click this icon to open the Current Alarm - All Objects - Minor tab and view minor alarms.
		Note	Dynamically displays the number of warning alarms; Click this icon to open the Current Alarm-All Objects - Warning tab and view warning alarms.

Table 2-1 Default Shortcut Icons in the Toolbar (Continued)

Category	Symbol	Name	Description
		Display Alarm Statistics Window	Opens the Alarm Statistics dialog box, which displays the statistics of all current alarms by default.

Other Common Shortcut Icons

Table 2-2 describes other common shortcut icons.

Table 2-2 Other Common Shortcut Icons

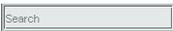
Symbol	Name	Description
	Quick Search in the Browse Tree	Enters a keyword to search the current objects for a desired one. You can click to set the query conditions.
	Advanced Search	Search Object
	Expand	Expands the object tree.
	Collapse	Collapses the object tree.
	Create Custom View	Creates a custom topology view to display only the focused objects.
	Lock the View	Locks the NE icons in the topology view.
	Unlock the View	Unlocks the NE icons in the topology view.
	Create Link	Creates the link between two NEs.
	Click	Moves the NE icons in the topology view when the view the unlocked.
	Move	Moves the topology view.
	Bird-eye view	Displays the aerial view of the topology.
	Zoom In	Zooms in the topology view.
	Zoom Out	Zooms out the topology view.
	Zoom to 100%	Displays the topology view according to its original size.

Table 2-2 Other Common Shortcut Icons (Continued)

Symbol	Name	Description
	-	Sets the display size of the topology view.
	Save picture	Saves the current topology as an image.
	Save	Saves the topology after the modification.
	Topo Layer	Displays different topological layers, such as core layer, convergence layer and access layer.
	Last View	Returns to the view or subnet opened just now.
	Next View	Browses the view or subnet opened before click  .
	Parent View	Returns to the upper level of the current view.
	Select Different View	Quickly selects the view or subnet opened before.
	Scroll Documents Left/Right	Opens the corresponding window towards the left or right when multiple windows are opened.
	Show Opened Documents List	Quickly selects the open a certain window from the list when multiple windows are opened.
	Maximize Window	Maximizes a certain window and hides the other windows when multiple windows are opened.
	Restore Window	Restores the display of multiple windows.

2.3.3 Common Shortcut Keys

Table 2-3 describes the common shortcut keys in the UNM2000.

Table 2-3 Common Shortcut Keys

Shortcut Key	Description
F1	Opens the Help.
F5	Refreshes the current view.
Alt+Shift+Enter	Selects / Cancels the full-screen mode.
Ctrl+E	Opens the Search Object dialog box to search for NEs, logical domains or cards.

Table 2-3 Common Shortcut Keys (Continued)

Shortcut Key	Description
Ctrl+M	Views the current alarms.
Ctrl+H	Views the alarm history.
Ctrl+P	Views the performance history.
Ctrl+G	Opens the Global Template Management tab to manage global templates and configurations.
Alt+S	Opens the System main menu.
Alt+V	Opens the View main menu.
Alt+E	Opens the Resource main menu.
Alt+G	Opens the Configure main menu.
Alt+A	Opens the Alarm main menu.
Alt+P	Opens the Performance main menu.
Alt+U	Opens the Security main menu.
Alt+W	Opens the Window main menu.
Alt+H	Opens the Help main menu.
Ctrl+W	Closes the current window.
Shift+Escape	Maximizes / restores the current window.
Alt+Shift+D	Opens the tab in the current or new window.
Ctrl+Shift+W	Closes all tabs except the Main Topology tab.

2.4 Menu Description

The following introduces all menus in the UNM2000 client through which you can quickly access various operations.

2.4.1 System

Table 2-4 describes the submenus under the **System** main menu.

Table 2-4 Submenus under the **System** Main Menu

Item	Description
Save Data Overflow Saving	When the overflow save task of historical data is set, the UNM2000 will automatically save the EMS log history data, device alarm data and performance data according to the conditions set in the task.

Table 2-4 Submenus under the **System** Main Menu (Continued)

Item		Description
	Save Manually	Saves the EMS log data, device alarm data and performance data manually.
Policy Task Management	Configuration Backup	Sets the data backup attributes to complete the device software backup task and configuration data backup task.
	Upgrade Task	Creates the upgrade task to implement upgrade of the OLT system cards, service cards, TDM cards, voice cards, OLT firmware and ONU software and firmware in a batch manner.
	Data Synchronization	Implements the synchronization of the data on the device and in the UNM2000. The data synchronization tasks include the software / hardware version update tasks, configuration uploading tasks, NE automatic discovery and ONU port enabling rule tasks.
	Test Task	The test task includes the POTS port external / internal line task, VoIP pinging test task and HCU discharge test task.
	Statistics Export Task	Creates the statistics exporting task to export the performance data such as traffic data to the FTP server.
	Preset Task	sets up the configuration script task to download the Telnet commands in a batch manner automatically.
Network Management Tool		Indicates an Web-based application program that provides EMS service process management, resource management, history data management, log management and parameter settings, and configuration import and export functions.
Parameter Settings	Local Settings	Indicates the interface settings, parameter settings, switch settings and other settings of the UNM2000 client.
	User Security Strategy	Sets the user login mode, access control list, account policy and password policy of the UNM2000.
	Alarm Settings	Sets the alarm parameters, including the local setting and the server setting. <ul style="list-style-type: none"> ◆ Local settings: Sets the alarm sound, alarm color and processing mode of reported new alarms. ◆ Server settings: Sets the alarm automatic confirmation rules, remote alarm notification and automatic synchronization mode.
	Performance Settings	Sets the 24-hour performance collection time of the server and performance collection range of the ONU.
	Service Configuration	Sets the global XFTP server and exported file.

Table 2-4 Submenus under the **System** Main Menu (Continued)

Item		Description
	License Setting	Sets the license expiration prompt.
Default Work Section Settings		Sets the UNM2000 workspace directory for storing the temporary resource files needed by the system.
Lock the Terminal		Locks the UNM2000 client manually.
Modify Password		Modifies the password of the current user.
Logout		Logs out of the current UNM2000 client and returns to the user login GUI.
Exiting the System		Exits and closes the UNM2000 client.

2.4.2 View

Table 2-5 describes the submenus under the **View** main menu.

Table 2-5 Submenus under the **View** Main Menu

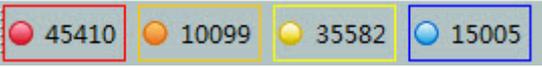
Item		Description
Topo Display	Displays the IP address and type of the NE.	Sets whether to display the NE IP address and type next to the NE icon in the network topology.
	Picture Mode	Sets a picture as the background image of the current topology.
	Map Mode	Sets the map of the local city as the background image of the current topology.
Message Platform		Opens the Message Platform window at the bottom of the main topology, in which you can understand the system information.
Toolbar	Alarm Statistics	Sets whether to display  on the toolbar of the main topology, so as to view the UNM2000 and NE alarms.
	Common Function Area	Sets whether to display  on the toolbar of the main GUI.

Table 2-5 Submenus under the **View** Main Menu (Continued)

Item		Description
	Alarm	Sets whether to display  on the toolbar of the main GUI.
	Performance	Sets whether to display  on the toolbar of the main GUI.
	Others	Sets whether to display  on the toolbar of the main GUI.
	Legend	Sets  on the toolbar of the main GUI. Click this icon and the Legend window appears on the right, displaying the description of the icons.
	Small Toolbar Icons	Sets the display size of shortcut icons.
	Reset Toolbars	Restores the default shortcut keys on the toolbar of the main topology.
	Customize	Adds the commonly used tools onto the toolbar by customizing the toolbar.
Zoom	Zoom In	Zooms in the topology view.
	Zoom Out	Zooms out the topology view.
	Actual Size	Displays the topology view according to its actual size.
	Optimum Size	Displays the topology view according to the window size.
Full Screen		Displays the EMS system in full screen.
Refresh		Refreshes the current view.

2.4.3 Resource

Table 2-6 describes the submenus under the **Resource** main menu.

Table 2-6 Submenus under the **Resource** Main Menu

Item		Description
Open NE Manager		Opens the NE manager, in which you can perform operations based on NEs as well as configure, manage and maintain NEs, cards or ports separately.
Detect Physical Configuration		Detects the card physical configurations of the devices in the network and automatically synchronizes the card physical configurations of the devices to the UNM2000.
Auto NE Discovery		Detects the devices connected to the UNM2000 automatically, creates NE and configures NE data in the topology.
Create Logical Domain		Creates a logical domain for managing NEs. The logical domain is a set of NEs.
Create NE	Create Access NE	Create Access NE
	Create Other NEs	Create Other NEs
Modify NE Names in a Batch Manner		Modifies or replaces the names of logical domains, NEs or ONUs in a batch manner.
Modify ONU Names by Importing EXCEL		Modifies ONU names in a batch manner by importing EXCEL information.
Import ODN NSM Information		Imports the ODN relevant information into the UNM2000, including the IP address and name of the OLT connected to the ODN, PON port of the ONU, ONU name, optical splitter name, port, etc.
Delete NE		Deletes all the data of the selected network or subnet.
Fiber Channel Management		Manages the fiber channels.
Search Object		Searches for the object by the specified search conditions, for example, NE, logical domain or card.
Query ONU		Searches for the ONU by the specified search conditions.
Batch Query ONU		Searches for the ONU by the specified search conditions in a batch manner.
Query MDU Phone Number		Searches for the MDU relevant information by phone number.
Query Board By Serial Number		Queries detailed information of cards through serial number.
ONU RMS Error Information Query		Queries error information of the ONU RMS to know about the fault reason.

Table 2-6 Submenus under the **Resource** Main Menu (Continued)

Item	Description
Querying the ONU Network Access Interception Logs	Through the ONU network interception records, you can check whether multiple ONUs apply access to the network for the same MAC address. This can help the maintenance engineers query the network access failure.
Mark the NE As	Marks the NE with a specified label so that it can be quickly queried.
Label Query	Queries an NE according to the customized NE label.
GIS Batch Import	Imports the NE GIS information in a batch manner.
Gateway Type Config	Sets the NM type information.
Resource Statistics	<p>The resource statistics include physical resource statistics, statistics of other types, physical resource statistics export and statistics export of other types.</p> <ul style="list-style-type: none"> ◆ Physical Resource Statistics: Gathers statistics of NEs, cards, ports and ONUs according to the preset statistical template. ◆ Other Type Statistics: Gathers statistics of ONU users, local end VLANs, NE MGC services and device types according to the preset statistical template. ◆ Physical Resource Statistics Export: Exports the statistics of physical data. If you export statistics directory through the GUI, you can save them as a TXT, EXCEL, CSV, XML, PDF or HTML file. If you export them through the XFTP server, you can only save them as an XML or CSV file. ◆ Statistics Export of Other Types: Exports the statistics of user information or service information. If you export statistics directory through the GUI, you can save them as a TXT, EXCEL, CSV, XML, PDF or HTML file. If you export them through the XFTP server, you can only save them as an XML or CSV file.
Unauthorized ONU List	Queries an unauthorized ONU list in a specific object.

2.4.4 Configuration

The submenus under the **Configure** main menu are described in Table 2-7.

Table 2-7 Submenus under the **Configuration** Main Menu

Item	Description
Global Template Management	The global template management includes the global templates and the global configurations. <ul style="list-style-type: none"> ◆ Global template: Configures the unified template for the NEs of the same model in the administrative domain, such as line template, QoS template, port template, service template and bandwidth template. ◆ Global configuration: Configures the non-template information for the NEs of the same domain in the administrative domain in a centralized manner.
SNMP Parameter Template	Configures and manages the SNMP parameter templates used for communication between the UNM2000 server and NEs.
NE Communication Route Management	Creates management programs so as to manage NEs based on partitions and manage the pre-configured NEs.
Network Access Status Management	Queries, sets and delivers the interconnection status and network access status of the system or the resource management system of the line card.
Tracing Signaling	Traces the signaling frame of the communication between the current IAD and the voice communication card, so as to find the communication faults in a timely manner.
Configuration Synchronization	Compares whether the configuration data in the UNM2000 and the data on the equipment are the same and synchronizes the configuration data in the UNM2000 with the data on the device.
Migrating the PON Configuration	Migrates the PON configuration.

2.4.5 Alarm

Table 2-8 describes the submenus under the **Alarm** main menu.

Table 2-8 Submenus under the **Alarm** Main Menu

Item	Description
Current Alarm	Sets the query conditions to view the current alarms of the entire network or a specified object.
Alarm History	Sets the query conditions to view the alarm history of the entire network or a specified object.

Table 2-8 Submenus under the **Alarm** Main Menu (Continued)

Item		Description
View Report Alarm		Sets the alarm reporting conditions to view the reported alarms of the entire network or a specified object.
Query Reported Event		Sets the event reporting conditions to view the reported events of the entire network or a specified object.
Set- tings	Alarm Report Settings	Sets the alarm reporting rules according to the requirements for network maintenance.
	Event to Alarm Settings	Sets specified events for alarm reporting according to the requirements for network maintenance.
	Shield Rule of North	Sets filter rules for the alarms not reported to the northbound interface according to the requirements for network maintenance.
	Alarm Shield Rule Management	Sets filter rules to filter the alarms not focused according to the requirements for network maintenance.
	Alarm Flashing Shield Rule Management	Sets effective time of filtering rules to filter the alarms not focused in real time according to the requirements for network maintenance.
	Alarm Frequency Analysis Rule	Sets the alarm frequency analysis rule so that the EMS will process alarms according to the rule settings once the specified object meets the preset conditions.
	Alarm Notification	Sets the information of the alarm receiver to make sure important alarms are notified to the device maintainer in a timely manner.
	Custom Alarm Level	Customize the alarm levels.
	Alarm Maintenance Experience	Enters the experience information of alarm maintenance.
Alarm Query Template		Quickly completes the settings of alarm browsing and alarm attributes to simplify the user setting operations.
Event Query Template		Sets the event reporting rules according to the requirements for network maintenance.
Shield Project Alarms		Sets alarm filtering fields to automatically filter all the reported alarms and alarm clearance information during the project construction.
Custom Alarm Name		Customizes alarm names.
Alarm Log	Query Alarm Log	Queries alarms according to the query conditions.
	History Alarm Log Statistics	Gathers statistics of historical alarms according to the specified statistical conditions.

Table 2-8 Submenus under the **Alarm** Main Menu (Continued)

Item	Description
Current Alarm Log Statistics	Gathers statistics of current alarms according to the specified statistical conditions.

2.4.6 Performance

The submenus under the **Performance** main menu are described in Table 2-9.

Table 2-9 Submenus under the **Performance** Main Menu

Item	Description
Performance History	Sets the query conditions to view the performance history of the entire network or a specified object.
View Performance History Trend	Sets the statistical template of performance history to view the performance history charts so as to understand the performance data change trend of the specified object and the running status of the network.
Collection Task Management	Sets the indicator, threshold, task and time for the performance connection.
PAS Collection Task Management	Sets the indicator, threshold, task and time for the performance connection of the transport domain.
Performance Classification Switch Config	Queries or configures the performance classification switch for NEs in a batch manner.
Performance Query Template	Save the common performance query conditions as a template.
Pm FTP Switch Management	Configure the FTP performance reporting switch.
Analysis of PON traffic statistics	Query the traffic analysis data of the PON port.
Top rank statistics	Query the traffic ranking of the PON port and the health ranking of the device.

2.4.7 Security

Table 2-10 describes the submenus under the **Security** main menu.

Table 2-10 Submenus under the **Security** Main Menu

Item	Description
EMS User Management	Manages the UNM2000 users, user groups and operation sets, including the security attribute settings and authority allocation.
Device User Management	Manages the device users, including adding, deleting, modifying, enabling and disabling the device users.
Monitor User Session	Sets the operations of monitoring user sessions and user activity information.
Search the System Logs	Sets the filter conditions to query the system logs.
Query Operation Logs	Sets the filter conditions to query the operations logs.
Query Security Logs	Sets the filter conditions to query the security logs.
Query Device Syslog	Sets the filter conditions to query the device operations logs.
Query Northbound Interface Command Logs	Sets the filter conditions to query the northbound command logs.
Statistical System Logs	Sets the filter conditions to gather statistics of system logs.
Statistical Operation Logs	Sets the filter conditions to gather statistics of operation logs.
Statistical Security Logs	Sets the filter conditions to gather statistics of security logs.
Statistical Northbound Interface Command Logs	Sets the filter conditions to gather statistics of northbound command logs.
Log Forwarding Server Management	Forwards the UNM2000 logs to other servers.

2.4.8 Window

Table 2-11 describes the submenus under the **Window** main menu.

Table 2-11 Submenus under the **Window** Main Menu

Item	Description
Close Window	Closes all the opened windows except the main topology.
Maximize Window	Maximizes the current window.
Undock Window	Cascades all the opened windows.
Close All Windows	Closes all the opened windows except the main topology.
Close Other Windows	Closes all the opened windows except the main topology and current window.
Window	Displays the description of each window.

2.4.9 Help

Table 2-12 describes submenus under the **Help** main menu.

Table 2-12 Submenus under the **Help** Main Menu

Item	Description
Help	Displays on-line help of the UNM2000.
Legend	Opens the Legend pane to view the system legend.
License Management	Displays the UNM2000 license information, including server ID and operations for updating the license.
About UNM2000	Displays the UNM2000 version, registration information and installed components.

2.5 Setting UNM2000 System Parameters

The UNM2000 system parameters include the browse tree display mode, time mode, topology display, ping parameters, Telnet proxy server, GUI display, font settings, personalized switch settings, default page opening settings and NE manager settings. The following introduces how to set and use these parameters.

2.5.1 Setting the Display of the Browse Tree

The **Viewing Tree Setting** dialog box is used for setting the display of the main topology. You can set the icon size, border pixels, height as well as the space between the border and the text.

Background Information

This setting will take effect immediately for the client end. After logging into the server from the current client end, all the users can view the setting result.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**Interface Setting**→**Viewing Tree Setting** in the left pane to open the **Viewing Tree Setting** dialog box.

3. Set various parameters as required. Users can preview the display style via the instance text during setting.
4. Click **Apply** after the settings are completed, and the settings will take effect immediately.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the default values.

2.5.2 Setting the Time Mode

Set the time mode of the client end. The UNM2000 displays the time in the configured time mode (UTC or local time).

Background Information

This setting will take effect immediately for the client end. After logging into the server from the current client end, all the users can view the setting result.



Note:

It is recommended that the client time should be consistent with that of the server to avoid reporting errors of data at both ends.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**Other Setting**→**Time Mode** in the left pane to open the **Time Mode** dialog box.
3. Set the time display mode of the client end as required. Then click **Apply** to apply the settings.

2.5.3 Setting the Topology Display

The UNM2000 allows you to set the background image display of the main topology. You can set the display style as required.

Background Information

This setting will take effect immediately for the client end. After logging into the server from the current client end, all the users can view the setting result.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**Interface Setting**→**Topology Setting** in the left pane to open the **Topology Setting** dialog box.
3. Set the background display mode of the main topology.

- ▶ Select **Image Mode** and then click **Apply**→**OK** to set the background of the main topology to image mode.

In the image mode, right-click in the blank area of the physical topology view and select **Set Background Image** or **Use the Default Background Image** from the shortcut menu to set the background image of the physical topology view.

- ▶ Select **Map Mode** to set the background of the main topology to map mode.
 - a) In the **gis map url** text box, enter the address of the network map or the map package in the local EMS.
 - b) Click **Apply**→**OK**.

**Caution:**

The address entered in the **dis map url** text box should meet the following requirements:

- ◆ For the network map, the address must be the URL of the GIS online map database.
 - ◆ For the map package in the local EMS, the address should be that of the map folder downloaded to the local EMS.
-

Other Operations

- ◆ Expand / collapse all logical domains.
Right-click in the blank area of the physical topology view and select **Expand All Logic Domains** or **Collapse All Logic Domains**.
- ◆ Hide nodes.
Right-click the NE in the physical topology view and select **Hidden Node** from the shortcut menu. The NE will not appear in the physical topology view.
- ◆ Manage the hidden nodes.
Right-click in the blank area of the physical topology view and select **Manage the Hidden Nodes** to open the **Hide Node Management** dialog box. Then select the nodes to be displayed and click **OK**. The corresponding nodes are displayed in the physical topology view.
- ◆ Lock, move, zoom in or zoom out the physical topology view via the shortcut icons at the top of the main topology.

2.5.4 Setting Ping Parameters

You can set the UNM2000 to continuously ping the NE or transfer the ping via the server so as to confirm whether the communication between the UNM2000 and the NE is normal.

Background Information

- ◆ When **Consecutive Ping** is not selected, the EMS will execute the Ping command at most four times.
- ◆ When the client cannot ping the NEs, you can select **Forward Ping Packet via the Server** to determine whether the communication between the EMS and NEs are normal.
- ◆ After the Ping parameters of the client are set, the settings take effect immediately.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**Para Setting**→**Ping Parameter Config** in the left pane to open the **Ping Parameter Config** dialog box.
3. Set the Ping parameters as required and click **Apply** to validate the settings.
 - ▶ If **Consecutive Ping** is selected, the EMS will send the Ping commands consecutively to the object after you right-click an object and select **Ping**.
 - ▶ If **Forward Ping Packet via the Server** is selected, the Ping commands will be forwarded by the server.

2.5.5 Setting the Telnet / SSH Proxy Server

After setting the parameters related to the Telnet / SSH proxy server, you can use the proxy server to access the device.

Background Information

The settings of the Telnet Proxy Server take effect immediately.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**Param Setting**→**Telnet/SSH Proxy Server** to open the dialog box.
3. Select **Enable Telnet/SSH Proxy Server**, set the information of the proxy server according to the actual situation and click **Apply**. The settings will take effect immediately.

2.5.6 Setting the Font

You can set the font, size and style of the UNM2000 GUI by **Font Setting**.

Background Information

This setting will take effect immediately for the client end. After logging into the server from the current client end, all the users can view the setting result.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**Interface Setting**→**Font Setting** in the left pane to open the dialog box.
3. Set various parameters as required. You can preview the font during setting.
4. Click **Apply** after the settings are completed, and the settings will be valid.

Other Operations

Click **Restore the system default font** to restore the parameters to the default values.

2.5.7 Setting the Default Opening Page for NE Manager

You can customize the default opening page of the NE manager as desired.

Background Information

This setting will take effect immediately for the client end. After logging into the server from the current client end, all the users can view the setting result.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**Switch Setting**→**Default Page Open Setting** in the left pane to open the **Default Page Open Setting** dialog box.
3. Set the default opening page of the NE manager.
4. Click **Apply** after the settings are completed, and the settings will be valid.

Other Operations

Click **Restore Default Configurations** to restore to the default system configuration.

2.5.8 Setting the Personalization Switch

You can set the personalization switch to top the vendor information in the ONU list.

Background Information

This setting will take effect immediately for the client end. After logging into the server from the current client end, all the users can view the setting result.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**Switch Settings**→**Personal Style Setting** in the left pane to open the **Personal Style Setting** dialog box.
3. Select **ONU vendor info show setting** and click **Apply** to take effect immediately.

Other Operations

Click **Restore Default Configurations** to restore to the default configuration.

2.5.9 Setting the GUI Display

You can set the maximum number of tables rows displayed on the GUI, the display mode of the alarm name, performance name as well as whether to lock the GUI automatically.

Background Information

This setting will take effect immediately for the client end. After logging into the server from the current client end, all the users can view the setting result.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select Local SettingsInterface SettingDisplay in the left pane to open the dialog box.
3. Set the parameters according to your needs and then click **Apply**. The settings will take effect immediately.

2.5.10 Setting the NE Manager

The UNM2000 client end supports setting the opened NE manager quantity and supports enabling NE manager closing prompt to facilitate the utilization.

Background Information

This setting will take effect immediately for the client end. After logging into the server from the current client end, all the users can view the setting result.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.

2. Select Local SettingsInterface SettingSet up NmFrame Open in the left pane to open the **Set up NmFrame Open** dialog box.
3. Click **Apply** after the settings are completed, and the settings will be valid.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the default values.

2.6 Setting the XFTP Server

You can set the XFTP server and related parameters to implement the data transmission between the UNM2000 client and the server end.

Background Information

The XFTP server settings are the foundation for implementing the functions of multiple modules, including policy task module, data history save module, log forwarding module and statistical information export module. The functions of the modules implemented via setting the XFTP server are shown in the following table.

Module Name	Implemented Function	Related Function
Policy Task	Implements the task customization via the XFTP server.	Includes the software backup task, configuration export task, system software upgrade task, ONU batch upgrade task and service card batch upgrade.
Resource Export	Exports the resource statistics onto the preset XFTP server.	Includes the NE resource statistics, card resource statistics, port resource statistics, ONU resource statistics, ONU port resource statistics, MDU port resource statistics, local VLAN statistics, ONU user statistics, NE MGC service statistics, ONU MGC service statistics, device type statistics, PON device capability statistics, PON traffic statistics, MAC address of the PON port and MAC address(es) of a single or networkwide OLTs.
Save Data	Releases the database space and saves the data onto the XFTP server.	Includes the operation log save, TL1 log save, system log save, alarm history save, performance history save and event overflow save.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Service Configuration**→**XFTP Server Setting** in the left pane to view the preset XFTP server.

XFTP Server Setting

Set Global XFTP Server

Host Name	Host IP	Protocol Type	Username	Password	Port Num...	Path
10.251.80.3	IPv4;10.251.80.3	FTP	admin	*****	21	/
Config	IPv4;10.251.80.8	FTP	cfgftp	*****	21	/
Default	IPv4;10.251.80.8	FTP	fiberhome	*****	21	/
Resource	IPv4;10.251.80.8	FTP	rscftp	*****	21	/
Test	IPv4;10.251.80.4	FTP	fnftp	*****	21	/
Upgrade	IPv4;10.251.80.8	FTP	ugdftp	*****	21	/

Total 6 entries

3. Click **Add** to add a blank row in the window. Then click each field and set the parameters of the XFTP server.
4. After completing the settings, click **Apply**. The added XFTP server appears in the window.

Other Operations

For the XFTP server already set, if it is no longer used or if you want to test it before use, do as follows:

- ◆ Select the XFTP server not needed and click **Delete** to delete it.
- ◆ Select the desired XFTP server and click **Test XFTP** to test whether the XFTP server can be connected normally.

2.7 Setting the Default Workspace

When using the UNM2000 for the first time, you need to set up a workspace directory for storing the temporary resource files required by the system.

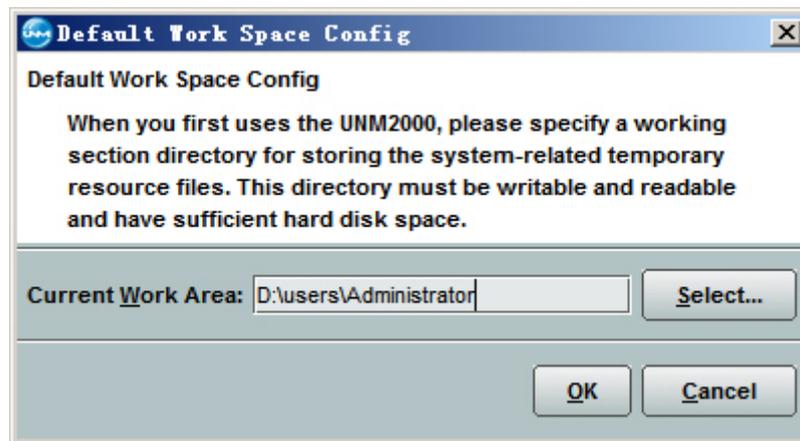


Note:

This directory must be readable and writable with a hard disk space greater than 512M.

Procedure

1. Select **System**→**Default Work Section Settings** from the main menu to open the **Default Work Section Settings** dialog box.



2. Click **Select** to select the folder where the workspace locates and then click **Open**.
3. Click **OK** to complete the settings.

2.8 Basic Operations of the UNM2000

The following introduces basic operations of the UNM2000 client for users to quickly know how to operate the EMS.

2.8.1 Updating the License

The UNM2000 License file is used for controlling the functions and management capability of the UNM2000. Without the License file, you cannot log into the UNM2000 client. The following introduces how to update the UNM2000 license.

Prerequisite

- ◆ Log into the UNM2000 as an administrator.
- ◆ The UNM2000 License file has been obtained.

Procedure

1. Back up the original License.
Create a **backup** folder in the **D:\unm2000\platform\etc\license** directory and copy the original license file **unm2000_license.lic** to this folder.
2. Select **Help**→**License Management** from the main menu.
3. In the displayed **License Information** dialog box, click **Update the License**.
4. In the **Open** dialog box, select a corresponding license file and click **Open**.
5. In the **license Comparison** dialog box, check the control items of the original and new license files and then click **Confirm to Update License**.
6. Click **OK** in the **Message** alert box.
7. Click **Close** in the **License Information** dialog box.

2.8.2 Modifying the User Password

To ensure the access security of the UNM2000, it is recommended to modify your password regularly.

Procedure

1. Select **System**→**Modify Password** from the main menu.
2. In the displayed **Modify Password** dialog box, enter **Old Password**, **New Password** and **Confirm Password**.



Note:

The new password must comply with the set password policies. For setting the password policies, see [Setting the Password Policy](#).

3. Click **OK**.

2.8.3 Locking the Terminal

If the UNM2000 client is idle, you can lock the client upon leaving to prevent unauthorized operations. The operation is only applicable to the user who performed the operation.

Prerequisite

You have logged into the UNM2000.

Procedure

1. Follow the steps below to lock the client.
 - ▶ Lock the terminal manually.

Select **System**→**Lock the Terminal** to open the **The window is locked** dialog box.
 - ▶ Locking the terminal automatically.

Enable the automatic terminal lock according to [Setting the GUI Display](#). If no operation is performed after a set time period, the terminal will be locked automatically.

2.8.4 Logging Out Users

Different EMS users have different operation authority. You can log out from the EMS and then log in as another user to perform different operations.

Procedure

1. Select **System**→**Logout** from the main menu.
2. Click **OK** in the displayed alert box.
3. In the displayed **UNM2000 Login** dialog box, enter the corresponding username and password, and click **Login**.



2.8.5 Viewing the Message Platform

You can view the message platform to understand the information prompting the influence on the UNM2000 running the operation return information.

Procedure

1. Select **View**→**Message Platform** from the main menu to open the **Message Platform** pane.
2. View the prompts or returned message of the operations in the **Message Platform** pane at the lower part of the window.

2.8.6 Managing the Toolbar

You can set the tools to be displayed in the toolbar and the shortcut button of each tool, so as to improve the operation efficiency.

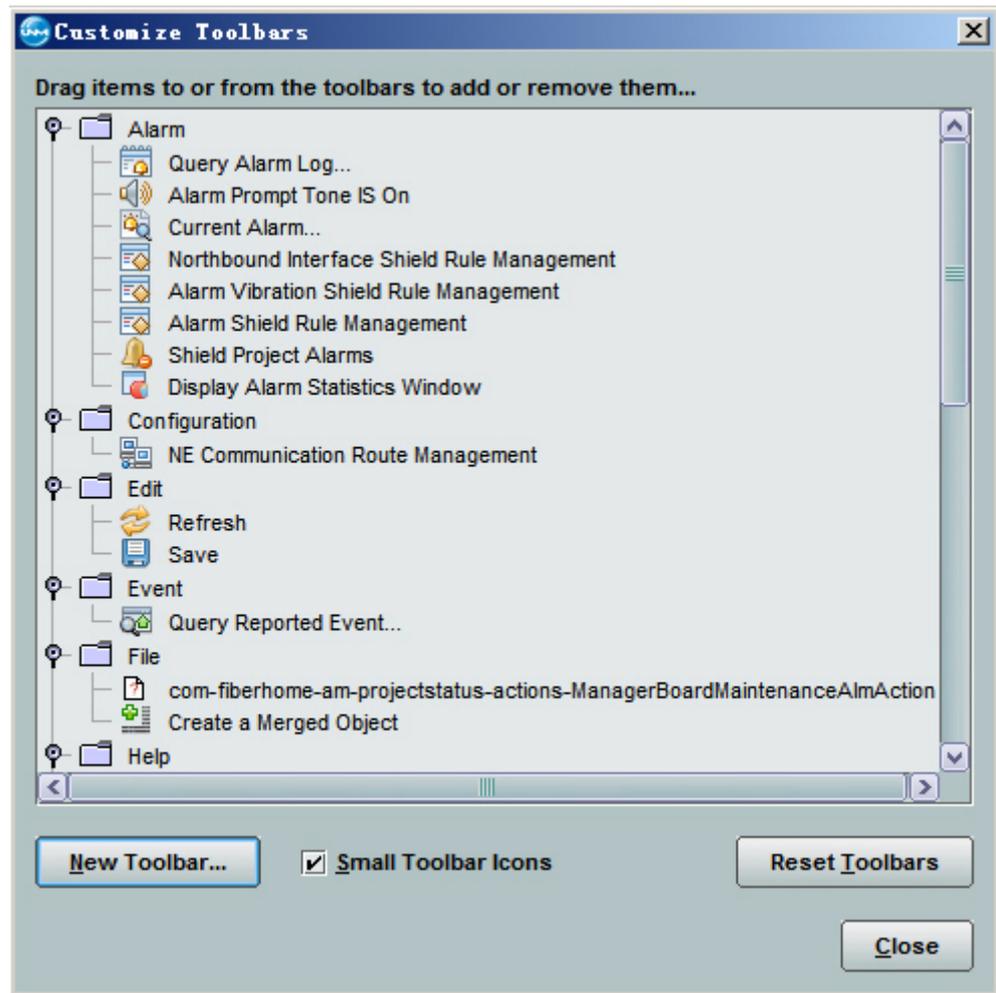
Procedure

1. Select **View**→**Toolbars** from the main menu.
2. In the **Toolbar** box, click the functional blocks to be displayed in the main topology GUI.

3. The ✓ symbol will be shown on the right side of the selected functional block. The selected functional blocks will also be shown in the toolbar in the main view.

Other Operations

1. Select **Customize** to open the **Customize Toolbar** dialog box.



2. Click **New Toolbar**, enter the new functional block name in the **New Toolbar** dialog box, and click **OK**.
3. Drag the items in the available tool area in or out of the toolbar to add or delete the corresponding shortcut icon as required.
4. After completing the setting, click **Close**.

The example below illustrates creating the **Topology** functional block in the toolbar, and drag the **Create Customized View** shortcut icon into the **Topology** functional block in the **Customize Toolbar** dialog box.



2.8.7 Customizing Views

In case of too many devices in the main topology, the focused object is not easy to locate and view. However, you can create a custom view to only display your focused objects.

Background Information

- ◆ Each user can create up to five custom views.
- ◆ Users can only see the custom views created by themselves.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. On the toolbar of the **Current Topology** or **Current View** tab, click .
2. In the **Create custom views** dialog box that appears, fill in the view name and the remarks.
3. Select **Node Member**→**Select**. In the **Select Object** dialog box, select the NEs to be displayed in the custom view, and then click **OK**.
4. Select **Link Member**→**Select**. In the **Select Object** dialog box, select the NE links to be displayed in the custom view, and then click **OK**.
5. Click **OK** in the **Create Custom View** dialog box.
6. In the UNM2000 alert box that appears, click **Yes** to switch to the custom view.

3 Security Management

The security management is used to prevent unauthorized login to the public network to guarantee the network data security. The security management includes the security policy management, user management and authority and domain division management of the UNM2000.

- User Security Concepts
- User Security Policy Management
- Managing UNM2000 Users
- Managing User Sessions
- Authorization and Domain Division

3.1 User Security Concepts

The security management of the UNM2000 users mainly includes authority management, password policy, account policy, access user management and user monitoring. The concepts involved in the security management of the UNM2000 users are described as follows:

Managed Entities

- ◆ **Object Set:** Indicates a set of managed objects. Dividing the managed objects into object sets, facilitating the allocation of authority for managing NEs.

The object set can be created through the logical domain. It includes the physical objects and EMS pre-authorized OLTs, with the smallest granularity being NEs.

- ◆ **Object Set:** Indicates a set of operations. You can divide the client operations into different operation sets for convenient management of user authority. Different operations have different influence on the system. You can divide the operations that may cause the same influence on the system into an operation set. When being assigned with the authority of an operation set, the user can perform all the operations included in the operation set.



Note:

Default operation sets are provided in the UNM2000. When the default operation sets cannot meet the requirements for authority assignment. You can create operation sets as needed.

- ◆ **User Group:** Indicates a set of UNM2000 users of the same management authority. The UNM2000 supports creating user groups to manage the users of the same authority in a same group. The users in a same group have the same authority and can perform the operations included in the operation set associated with the user group.

The default user groups of the UNM2000 include the Administrators group, the security management group, inspector group, the operator group and the maintainer group.

- ▶ Administrators: The Administrators group cannot be created nor deleted. The Administrators group has the administrative domains of all objects in the entire network and all the operation authority except the security management authority. Its administrative domains and operation authority cannot be modified.
- ▶ Security Admin Group: This group cannot be created nor deleted. The Security Admin Group has the administrative domains of all objects in the entire network and the authority related to security management authority.
- ▶ Inspector group: This group has the default authority of **Inspector Operation Sets**. The users in this group can only query and gather statistics, having no authority to perform the creation and configuration operations.
- ▶ Operator group: This group has the default authority of **Operator Operation Set**. Apart from the basic authority of the inspector group, the users in this group can perform the creation, modification and deletion operations in the UNM2000, but having no authority related to security management.
- ▶ Maintainer group: This group has the default authority of **Operator Operation Set**. Apart from the authority of the inspector group and the operator group, the users in this group can perform the configuration operations that may influence the running of the UNM2000 and the NEs, such as searching for service path, deleting service configuration, etc.
- ◆ User: Indicates the UNM2000 client end users. The username and password of the user uniquely determines the corresponding UNM2000 operation and management authority. When a user is added into a user group, the user is assigned with the operation authority associated with the user group.
 - ▶ One user can be added into multiple user groups simultaneously, and therefore the final authority of the user are the user's original authority coupled with the authority of the user groups to which the user belongs. There are two ways to assign authority to users:
 - Adding a user into a specific user group so that the user has the authority assigned to the user group.
 - Bind the user with the object set and the operation set.

- ▶ The UNM2000 provides a default user named admin, which is the system administrator. The admin user belongs to the **Administrators** and **Security Admin Group** groups by default. You cannot modify the authority of admin or add it to other user groups either.

Authorization and Domain Division

When the managed objects and users are of a large scale, the uniform management of authorization and domain division by a certain type of users will be both time and effort consuming. Therefore, it is necessary to divide the managed objects into several sub-domains. Each sub-domain can perform authorization and domain division management without interfering each other.

The authority and domain division function of the EMS is implemented by dividing the object sets and operation sets. With the authority division management function, you can divide the EMS authority into different functional domains, and with the domain division management function, you can divide NE units into different network domains. Assigning the UNM2000 users with the authority combination of different functional domains and network domains effectively controls user management authority.

Application of the authorization and domain division management: Divide the user groups into ordinary user group and administrative user group. Creating a user group is like creating a sub-domain. In this sub-domain, the users are authorized with the operation authority within this sub-domain and can create the object set, operation set, user group, users based on such domain authority. They are visible to other users within the sub-domain, but invisible to users outside the sub-domain.



Note:

The network management system provides an embedded user named admin, who is authorized with all authority and can manage all object sets, operation sets, user groups and users.

Account Policy and Password Policy

The UNM2000 user security can be implemented by setting the account policy and password policy.

- ◆ Account policy: Defines the minimum length, account login and unlocking settings of the user account. Using the account policy can enhance the security of the user account.
- ◆ Password policy: Defines the complexity, updating period and length limit of the password.

3.2 User Security Policy Management

The security policies, such as access control, password and lockout management and online user monitoring effectively enhance the access security of the UNM2000 and prevent unauthorized operations.

The user security policies are the access control rules defined for managing users. The security policy planning and configuration should be completed upon initial installation. You can adjust the security policies according to your management requirement.

The user security policy management includes the following:

- ◆ Setting the User Login Mode
- ◆ Setting the Access Control List
- ◆ Setting the Account Policy
- ◆ Setting the Password Policy

3.2.1 Setting the User Login Mode

The UNM2000 supports the single-user login mode and multi-user login mode. Typically, the UNM2000 runs in the multi-user mode. When maintaining the UNM2000 server (for example, adjusting the user group, administrative domain or operation authority of a user), you can set the UNM2000 to the single-user login mode to avoid operation interference caused by other users.

Background Information

- ◆ Single-user mode: In this mode, only one admin user can log into the UNM2000 via the client end, and all other online users will be forced to exit.

- ◆ Multiple-user mode: In this mode, multiple users are allowed to log in simultaneously. This mode is used for monitoring the network routinely.



Caution:

When the UNM2000 is switched to the single-user mode, only one admin user can log into the UNM2000 via the client end, and all other online users will be forced to exit. To ensure that other users use the UNM2000 normally, switch the UNM2000 to the multi-user login mode after completing the maintenance in single-user mode.

Prerequisite

Log in as an **admin** user.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **User Security Strategy**→**User Login Mode** in the left pane to open the **User Login Mode** dialog box.
3. Set the login mode as required. Then click **Apply** and the settings will be valid.

3.2.2 Setting the Access Control List

By setting the access control list, you can have the UNM2000 users log in to the client from the specified IP address or network segment to ensure network security.

Background Information

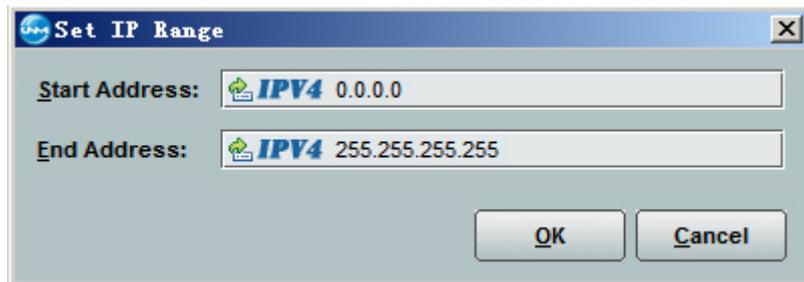
The access control list set by a user is only applicable to the user.

Prerequisite

You have logged into the OTNM2000 as a user belonging to **Security Admin Group**.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. In the left pane, select **User Security Strategy**→**Access Control List** to open the **Access Control List** dialog box.
3. Click **Add** to open the **Set IP Range** dialog box.



4. Set **Start Address** and **End Address** and click **OK**. The added IP range will be displayed in the access control list.



Note:

Click  to switch between IPV4 and IPV6.

5. Click **Apply**, and the settings will take effect.

3.2.3 Setting the Account Policy

The account policy includes locking / unlocking users, non-logged-in user policy, and the minimum length of the username. Setting the account policy can ensure the security of the account and the network.

Prerequisite

You have logged in as a member of the **Security Administrator** group.

Background Information

- ◆ The account policy must be configured upon initial installation of the UNM2000 and can be adjusted accordingly during maintenance.

- ◆ The new account policy has no effect on the accounts already set.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **User Security Strategy**→**Account Policy** in the left pane to open the dialog box.
3. Set the parameters and then click **Apply** to apply the settings.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the default values.

3.2.4 Setting the Password Policy

Setting the complexity of the password and modifying the password regularly can improve the access security of the UNM2000. The password policy, set by the security administrator, is applicable to all users.

Prerequisite

You have logged in as a member of the **Security Administrator Group**.

Background Information

- ◆ The password policy must be configured upon initial phase of the site building and can be adjusted accordingly during maintenance.
- ◆ The new password policy has no effect on the passwords already set.
- ◆ The password policy includes the complexity, updating period and length limit.
- ◆ The new password policy will be applicable to all users of the UNM2000.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.

2. Select **User Security Strategy** → **Password Policy** in the left pane to open the dialog box.
3. Set the information in **Common Policy** and **Advanced Policy**, and then click **Apply**. The settings will take effect immediately.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the default values.

3.3 Managing UNM2000 Users

The following introduces how to create, modify and delete the UNM2000 users, and how to assign the authority for the users.

3.3.1 Operation Set Management

The operation set is the set of operations of the same type. Through the operation set management, users can assign and manage the operations on the equipment uniformly.

- ◆ In the default operation sets provided by the UNM2000, the application operation complete set and the object operation complete set cannot be deleted.
- ◆ The operation sets include two types: **NM application** and **Network device**.
- ◆ When a certain user or user group is bound with an operation set, this user or user group will have the authority of the operations in this set.
- ◆ Only the users in the security administrator group and the sub-domain security administrator group can manage the operation sets.

3.3.1.1 Viewing Operation Sets

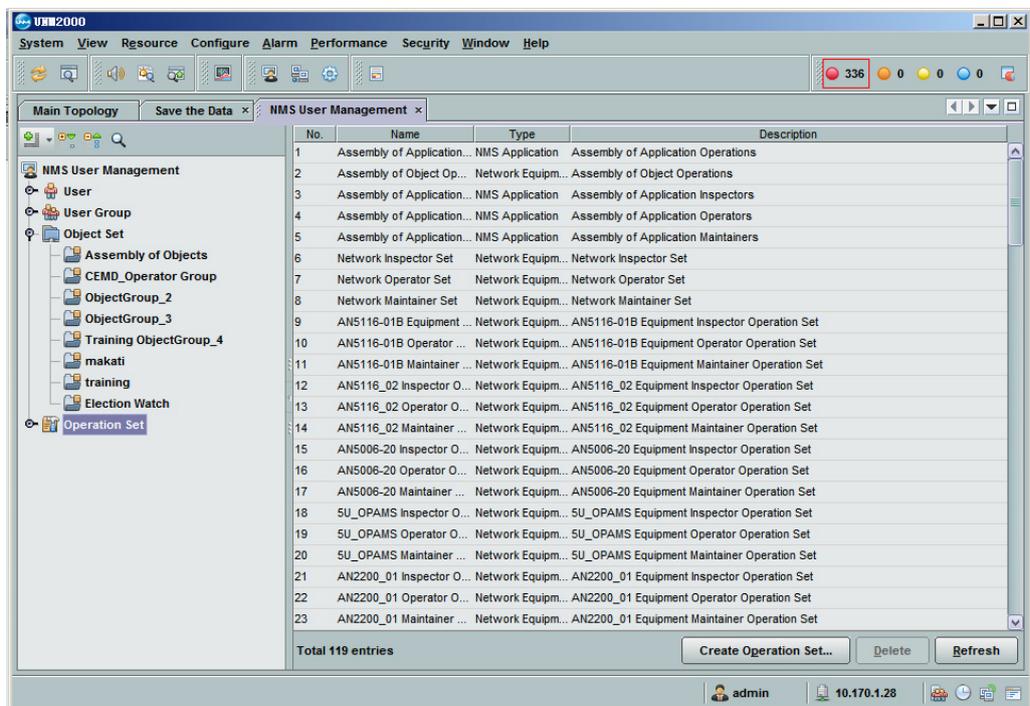
The security administrator can view specific operations included in an operation set to check whether the authority in the operation set meet the requirements.

Prerequisite

You have logged into the OTNM2000 as a user belonging to **Security Management Group**.

Procedure

1. Select **Security**→**NMS User Management** from the main menu to display the **NMS User Management** window.
2. Select **Operation Set** or click  before **Operation Set** in the left pane. Then view the existing operation sets in the right pane or the expanded list of **Operation Set** in the left pane.



3. Double-click the operation set entry in the right pane to view details in the **Basic Information**, **Member** and **Service For** tabs of the operation set.

Other Operations

- ◆ In the right pane, click the button at the lower part of the corresponding entry, or right-click the entry, and select operations such as **Delete**, **Refresh**, **Copy Cell**, **Print** or **Export**.

- ◆ Select a desired operation set in the left pane, modify the corresponding information in the right pane as needed and click **Apply**.



Note:

You can only modify the descriptions in the application operation complete set and the object operation complete set.

3.3.1.2 Creating Operation Groups

The operation set is the set of operations of the same type. Through the operation set management, users can assign and manage the operations on the equipment uniformly. You can create operation groups when the existing operation groups cannot meet your requirements.

Prerequisite

You have logged into the UNM2000 as a user belonging to **Security Administrator** group.

Procedure

1. Select **Security** → **NMS User Management** from the main menu to display the **NMS User Management** window.
2. Select one of the following access methods to display the **Create Operation Set** dialog box.

No.	Access Method
1	Click NMS User Management in the left pane and click Create Operation Set in the right pane.
2	Click NMS User Management in the left pane, right-click in the right pane and select Create Operation Set from the shortcut menu.
3	Select Operation Set in the left pane and click Create Operation Set in the right pane.
4	Click Operation Set in the left pane, right-click in the right pane and select Create Operation Set from the shortcut menu.
5	Right-click Operation Set in the left pane and select Create Operation Set from the shortcut menu.

3. In the **Create Operation Set** dialog box, set the parameters in the **Basic Information** and **Member** tabs.



Note:

Click **Copy Members from the Operation Set**, and select the operation set in the **Select the Operation Set** dialog box, so as to copy the members of the corresponding operation set. This can improve the setting efficiency.

4. After completing the settings, click **OK**.

Subsequent Operation

Click the added object set to view its relevant information in the right pane.

3.3.2 Object Set Management

The object set is the set of managed objects of a certain type. Via the object set management, users can manage the equipment objects uniformly.

- ◆ The default object set provided by the UNM2000 is the complete set of the objects, including all manageable objects. You cannot delete the default object set, but can only modify its descriptions.
- ◆ When a certain user or user group is bound with an object set, this user or user group will have the authority of the objects in this set.
- ◆ Only the users in the security administrator group and the sub-domain security administrator group can manage the object sets.

3.3.2.1 Viewing Object Sets

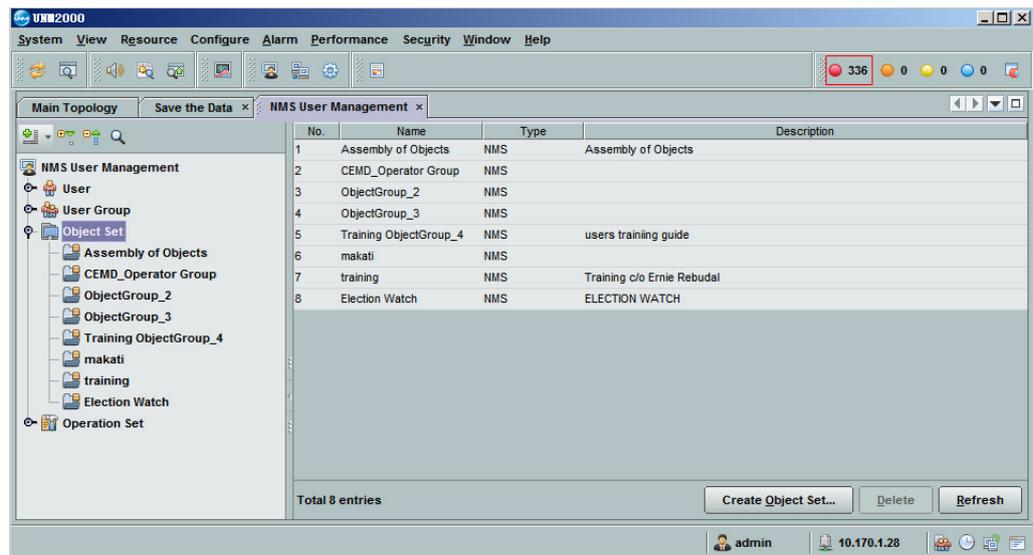
The security administrator can view the objects included in the object set to check whether the objects in the object set meet the requirements.

Prerequisite

You have logged into the UNM2000 as a user belonging to **Security Administrator** group.

Procedure

1. Select **Security**→**NMS User Management** from the main menu to display the **NMS User Management** window.
2. Click **Object Set** in the left pane or click  before **Object Set** in the left pane. Then view the existing object sets in the right pane or the expanded list of **Object Set** in the left pane.



3. Double-click the object set entry in the right pane to view details in the **Basic Information**, **Member** and **Service For** tabs of the object set.

Other Operations

- ◆ In the right pane, click the button at the lower part of the corresponding entry, or right-click the entry, and select operations such as **Delete**, **Refresh**, **Copy Cell**, **Print** or **Export**.
- ◆ Select a desired object set in the left pane, modify the corresponding information in the right pane as needed and click **Apply**.



Note:

You can only modify the descriptions in the application operation complete set and the object operation complete set.

3.3.2.2 Creating an Object Set

When the current object set cannot meet the requirements, you can create a new object set.

Prerequisite

You have logged into the UNM2000 as a user belonging to **Security Administrator** group.

Procedure

1. Select **Security**→**NMS User Management** from the main menu to display the **NMS User Management** window.
2. Select one of the following access methods to open the **Create Object Set** dialog box.

No.	Access Method
1	Click NMS User Management in the left pane and click Create Object Set in the right pane.
2	Click NMS User Management in the left pane, right-click in the right pane and select Create Object Set from the shortcut menu.
3	Select Object Set in the left pane and click Create Object Set in the right pane.
4	Select Object Set in the left pane, right-click the right pane and select Create Object Set from the shortcut menu.
5	Right-click Object Set in the left pane and select Create Object Set from the shortcut menu.

3. In the **Create Object Set** dialog box, set the parameters in the **Basic Information** and **Member** tabs.



Note:

Click **Copy member form object set**, and select the object set in the **Select object set** dialog box, so as to copy the members of the corresponding object set. This can improve the setting efficiency.

4. After completing the settings, click **OK**.

Subsequent Operation

Click an added object set to view the information related to the object set in the right pane.

3.3.3 Managing User Groups

The user group is the set of the network management users with the same management authority. For the users to be granted with the same authority, you can add them into the same user group and authorize the user group to make every user in the user group have the same authority, quickly allocating the authority to users.

- ◆ The default user groups of the UNM2000 include the Administrators group, the security administrator group, the operator group, the maintainer group, and the monitor group.
- ◆ When a user is bound with a user group, this user owns the authority assigned to the user group.
- ◆ Only the users in **Security Admin Group** and **Domain Security Admin Group** can manage user groups.



Caution:

You cannot delete the Administrators group and the security administrator group, but can only modify their descriptions.

3.3.3.1 Viewing User Groups

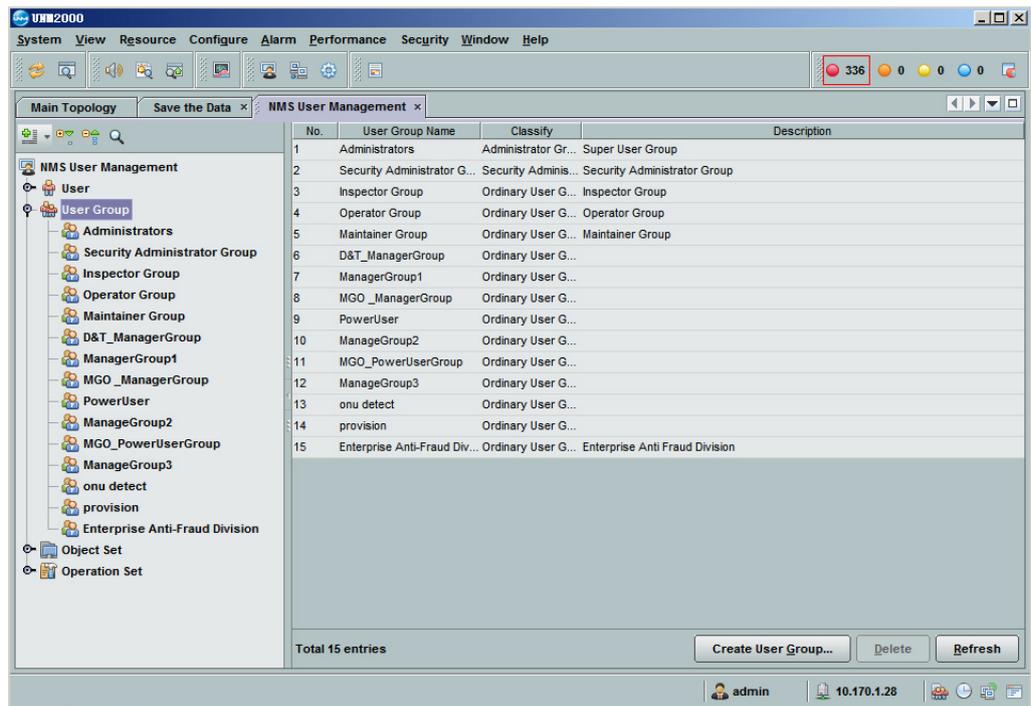
The security administrator can view the administrative domains of the user groups to check which objects are managed by the user group.

Prerequisite

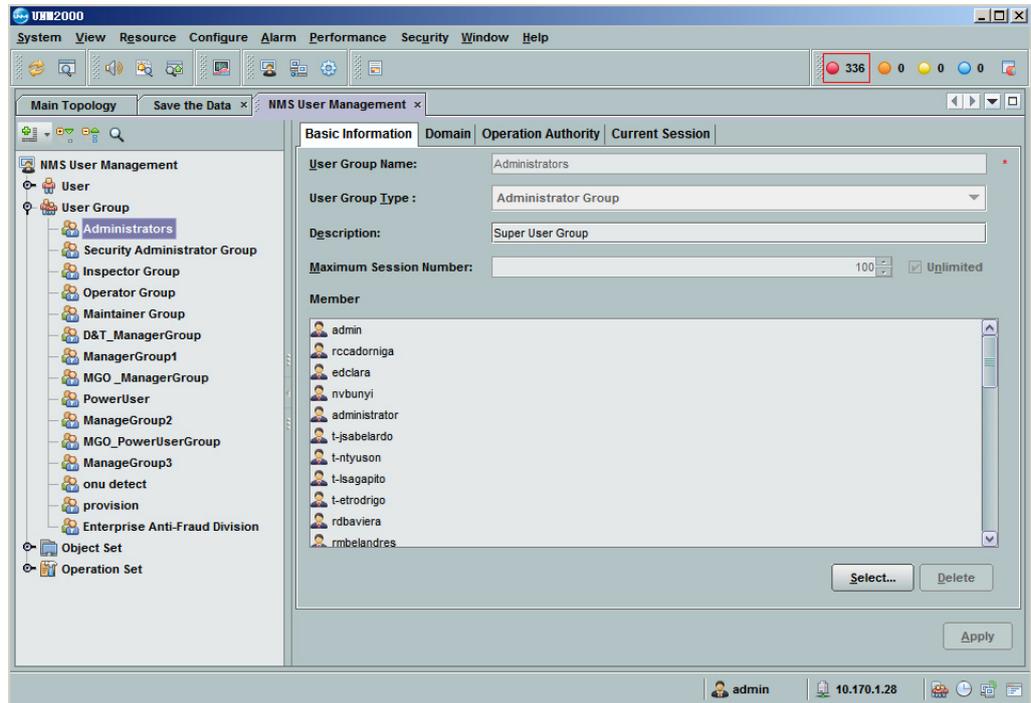
You have the authority of **Security Admin Group**.

Procedure

1. Select **Security**→**NMS User Management** from the main menu to display the **NMS User Management** window.
2. Click **User Group** in the left pane or click **+** before **User Group**, and you can view the existing user groups in the right pane or the drop-down menu of User Group.



3. Click the user group entry to view the details of the user group.



Note:

The **Current Session** tab displays the sessions of the online users in the user group.

Other Operations

- ◆ In the right pane, click the button at the lower part of the corresponding entry, or right-click the entry, and select operations such as **Delete**, **Refresh**, **Copy Cell**, **Print** or **Export**.
- ◆ Select the corresponding user group in the left pane, and modify the user group information in the right pane through **Find** or **Select**.

3.3.3.2 Creating User Groups

When default user groups in the UNM2000 do not meet the requirements for user authorization, you can create user groups according to the management features of the users, which is convenient for assigning authority for users.

Prerequisite

You have logged into the UNM2000 as a user belonging to **Security Administrator** group.

Procedure

1. Select **Security**→**NMS User Management** from the main menu to display the **NMS User Management** window.
2. Select one of the following access methods to open the **Create User Group** dialog box.

No.	Access Method
1	Click NMS User Management in the left pane and click Create User Group in the right pane.
2	Click NMS User Management in the left pane, right-click in the right pane, and select Create User Group in the shortcut menu.
3	Select User Group in the left pane, and click Create User Group .
4	Click User Group in the left pane, right-click in the right pane and select Create User Group from the shortcut menu.
5	Right-click User Group in the left pane, and select Create User Group from the shortcut menu.

3. Table 3-1 shows how to set the user group parameters in the **Create User Group** dialog box.

Table 3-1 The User Group Settings

Parameter		Description
Basic Information	User Group Name	Compulsory. Sets the user group name.
	User Group Type	<p>Sets the user group type to Sub Domain Security Administrator Group or Ordinary User Group.</p> <ul style="list-style-type: none"> ◆ Domain Security Admin Group: The Domain Security Admin Group, with its management domain assigned by the security administrator, only has the Security Management authority, which cannot be modified. ◆ Ordinary User Group: The administrative domain and operation authority of the users in this group are assigned by the security administrator or sub domain security administrator.

Table 3-1 The User Group Settings (Continued)

Parameter		Description
	Description	The brief description of the user group, used to identify different user groups.
	Maximum Session Number	Sets the maximum number of sessions for users in the user group. It can be used to limit the number of sessions logged in by users in one user group in one time interval. Value range: 0 to 100, Unlimited.
	Member	Sets the members of the user group via the Select and Delete buttons.
Domain		Sets the management domain of the user group. The objects of the management domain are arranged in parallel in the tree topology of the devices, the global logical domains, and the object groups. The valid management domain is the sum of the selected devices, global logical domains, and object groups.
Operation Authority		Sets the operation authority of the user group. The objects of the operation authority are classified into the network management application objects, all objects in the management system, and network devices. The network management application authority includes the operation groups of the network management application types and the network management operation list.

**Note:**

Click **Copy Authority Settings from the User Group**, set the user group in the Select User Group dialog box, and directly copy the management domain authority and operation authority of the corresponding user group. This can improve the setting efficiency.

4. Click **OK**.

Subsequent Operation

Click an added user group to view the information related to the user group in the right pane.

3.3.4 Managing Users

The user refers to the person who uses the UNM2000. Users need to log into the UNM2000 via the corresponding user account. The UNM2000 provides a default superuser named admin.



Caution:

The authority of admin cannot be modified and the admin user cannot be added to other user group.

3.3.4.1 Viewing Users

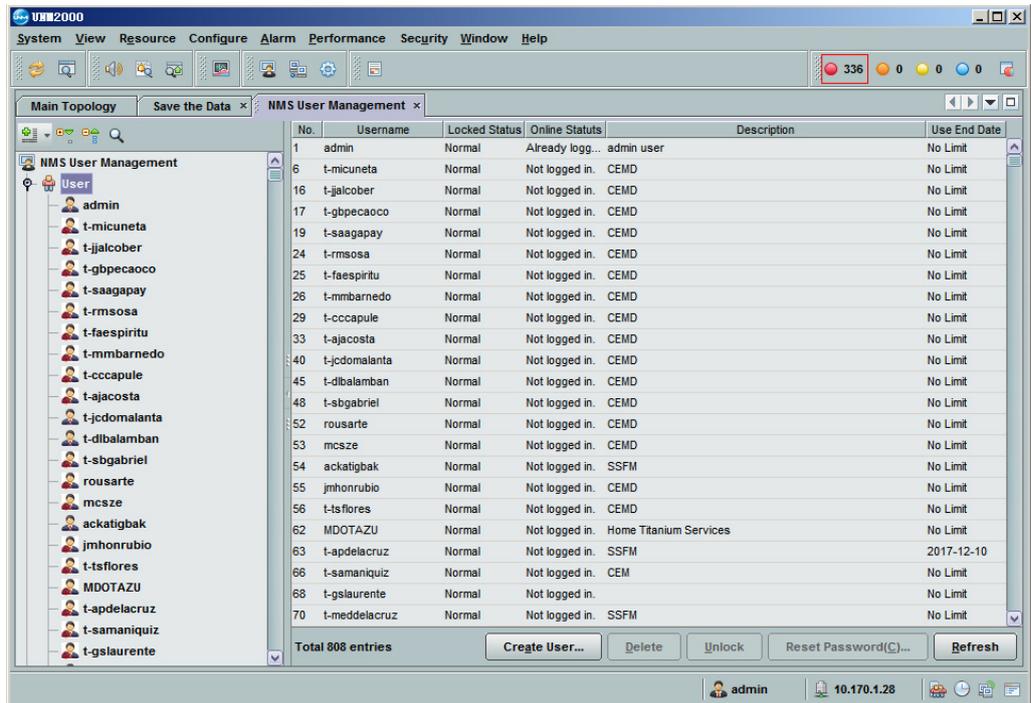
You can query the number and additional information of the UNM2000 users for convenient user management.

Prerequisite

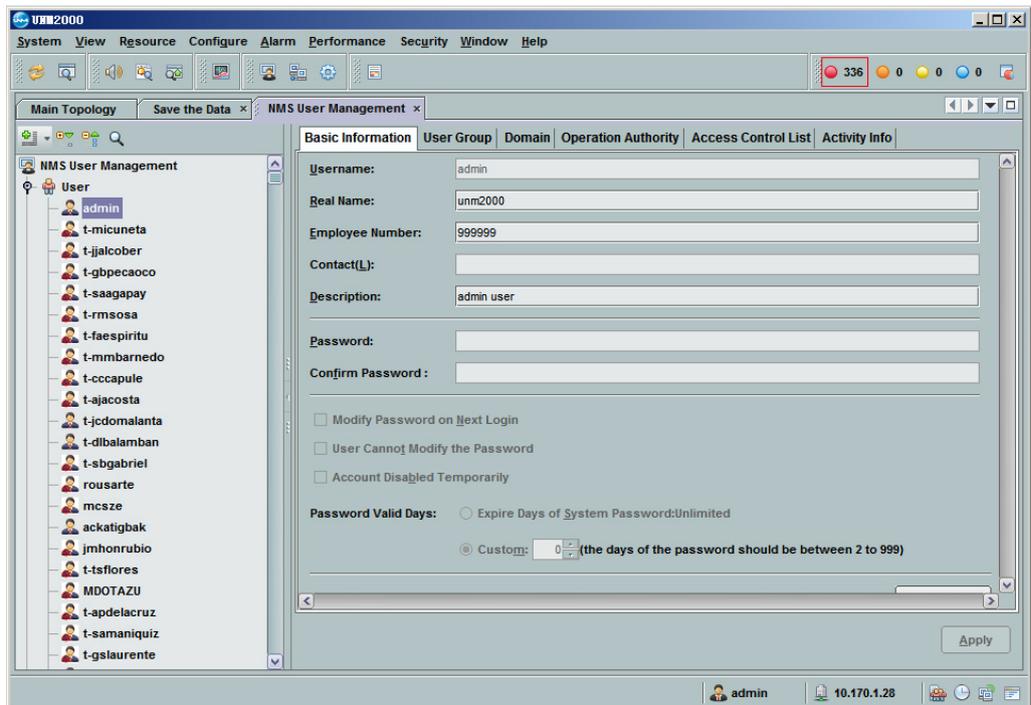
You have the authority of **Security Admin Group** or higher authority.

Procedure

1. Select **Security** → **NMS User Management** from the main menu to display the **NMS User Management** window.
2. Click **User** or  before User in the left pane, and then view the existing users in the right pane or the expanded list of User in the left pane.



3. Click a user entry and view the details of the user in the right pane.



Other Operations

- ◆ In the right pane, click the button below the corresponding entry, or right-click the entry, and select operations such as **Delete**, **Unlock**, **Reset password**, **Copy**, **Refresh**, **Print**, **Copy Cell**, or **Export**.
- ◆ In the right pane, modify the information in the **Basic Information** and **Access Control List** and then click **Apply** to apply the changes.

3.3.4.2 Creating Users

Create the UNM2000 user accounts and assign them with corresponding authority so as to allocate the accounts to users of different responsibilities.

Background Information

The UNM2000 provides a default user named admin. You cannot modify the authority of **admin** or add it to other user groups, either.

Prerequisite

You have the authority of **Security Admin Group** or higher authority.

Procedure

1. Select **Security**→**NMS User Management** from the main menu to display the **NMS User Management** window.
2. Select one of the following access methods to display the **Create User** dialog box.

No.	Access Method
1	Click NMS User Management in the left pane and click Create User in the right pane.
2	Click NMS User Management in the left pane, right-click in the right pane, and select Create User in the shortcut menu.
3	Click User in the left pane and then click the Create User button in the right pane.
4	Click User in the left pane, right-click in the right pane and select Create User from the shortcut menu.
5	Right-click User in the left pane and select Create User from the shortcut menu.

3. Table 3-2 shows how to set the user parameters in the **Create user** dialog box.

Table 3-2 User Settings

Parameter		Description
Basic Information	Username	Compulsory. Sets the user account, which must comply with the account policies. For the settings of the account policies, see Setting the Account Policy .
	Real Name	Sets the actual name of the user.
	Employee Number	Sets the employee ID of the user.
	Contact	Sets the contact information of the user for convenient management.
	Description	Description information of the user, for distinguishing users.
	Password	Required. Sets the user password, which must comply with the password policies. For the settings of the password policies, see Setting the Password Policy .
	Confirm Password	Required. Types the password again.
	Modify Password on Next Login	If this item is selected, when the corresponding user logs in again, he or she will be requested to modify the password.
	User Cannot Modify the Password	If this item is selected, the corresponding user cannot modify the password via the client end.
	Account Disabled Temporarily	If this item is selected, the corresponding user cannot log in.
Basic Information (Advanced)	Password Valid Days	Sets the password valid days. <ul style="list-style-type: none"> ◆ Select "Expire Days of System Password:Unlimited", and the password will never be expired. ◆ Select Custom to set the number of days. Value range: 2 to 999.
	Maximum Online Number	Sets the maximum online number of current users.
	Exit after waiting for a period (minutes) of:	Sets the waiting time for users to exit automatically.
	Unlogged User Policy	Sets the policy for user accounts which do not log in for a long time.

Table 3-2 User Settings (Continued)

Parameter		Description
	Login Time Range	Sets the time range for user's login.
User Group		Sets the user group to which this user belongs.
Domain		Sets the management domain of the user. The objects of the management domain are arranged in parallel in the tree topology of the devices, the global logical domains, and the object groups. The valid management domain is the sum of the selected devices, global logical domains, and object groups.
Operation Authority		Sets the operation authority of the user. The objects of the operation authority are classified according to the network management application objects, all objects in the management system, and network devices. The network management application authority includes the operation groups of the network management application types and the network management operation list.
Access Control List		Sets the access control list of the user. <ul style="list-style-type: none"> ◆ Select Use all access control list in the system, and the ACLs set by the system will be used in the range of IP addresses logged in by the user account. For setting the ACLs of the system, see Setting the Access Control List. ◆ Select Use the following assigned ACL to set the range of IP addresses logged in by the user account.



Note:

Click **Copy Privilege from Users**, set the user in the **Select User** dialog box, and directly copy the management domain and operation authority of the corresponding user to improve the setting efficiency.

4. Click **OK**.

Subsequent Operation

Click the added user in the left pane to view the information related to the user in the right pane.

3.3.4.3 Unlocking Users

When the number of login attempts exceeds the limit set in the account management policy at the client, the user will be locked. The user can be unlocked via the following ways:

- ◆ The admin user resets the password of the user and you can login again.
- ◆ The users belonging to the **Administrators** group unlock the user.

Background Information

- ◆ Only the users in **Security Admin Group** and **Domain Security Admin Group** can unlock users.
- ◆ The UNM2000 supports manual unlocking and automatic unlocking of the locked user.

Prerequisite

The UNM2000 client end is locked.

Procedure

- ◆ Unlock the user manually.
 - 1) Select **Security**→**NMS User Management** from the main menu to display the **NMS User Management** window.
 - 2) Click  before the **User** node to expand the user node.
 - 3) Right-click the locked user, and select **Unlock** from the shortcut menu.
- ◆ Unlock the user automatically.

Set the automatic unlocking time according to [Setting the Account Policy](#). The locked user can log in only after the set automatic unlocking time expires.

3.3.4.4 Resetting the User Password

In case you forget your password, your password expires, or you are disallowed to log into the UNM2000, you need to reset the password. The following instructs the users in the security administrator group to reset the passwords of other users.

Background Information

The users in the Security Admin Group and the Domain Security Admin Group can reset the passwords of all the users except the admin user. The password of the admin user can only be modified by the admin user at the UNM2000 client end.

Procedure

1. Select **Security**→**NMS User Management** from the main menu to display the **NMS User Management** window.
2. Click  before the **User** node to expand the user node.
3. Right-click the corresponding user, and select **Reset Password** from the shortcut menu.
4. In the **Reset Password** dialog box, set **New Password** and **Confirm Password**, and then click **OK**.



Note:

- ◆ The new password must comply with the set password policies. For setting the password policies, see [Setting the Password Policy](#).
 - ◆ If **Modify Password on Next Login** is selected, the user must modify the password upon next login.
-

3.4 Managing User Sessions

The users belonging to the **Security Admin Group** or **Inspector Group** can monitor user sessions. You can understand the information of the current online users in the system via monitoring the user sessions. The following introduces the operations of monitoring the user sessions and activities.

3.4.1 Monitoring the User Session

By monitoring user sessions, you can view the information of the online users.

Background Information

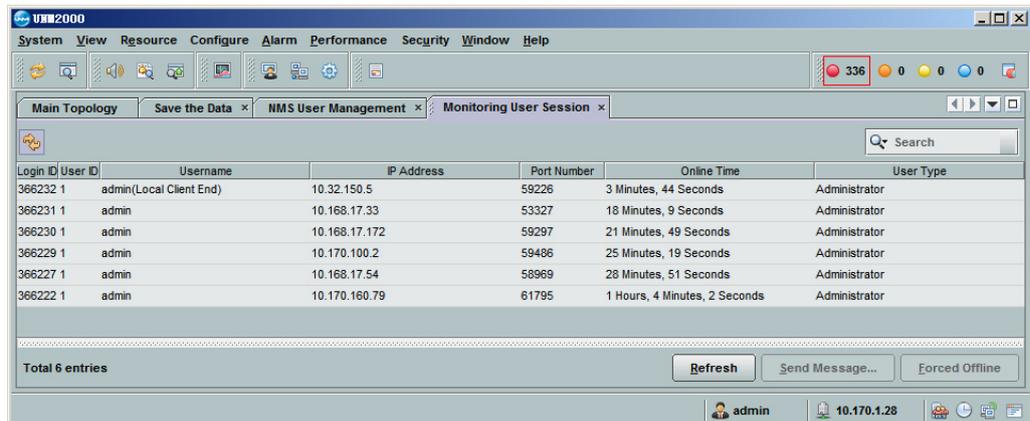
- ◆ Session: The connection set up between the client end and the server.
- ◆ When the user login mode is set to **Multi-User Mode**, one user account can log in multiple client ends at the same time. You can specify the maximum number of concurrent online users using a same account. For details, see [Creating Users](#).
- ◆ The object of forced exiting and sending messages is the user session. For example, if the user account “user” logs in the same UNM2000 server via client ends A and B, sessions a and b will be generated respectively. When the account “user” generating session a is forced to exit, the account “user” generating session b is not influenced.

Prerequisite

You have logged in as a member of the **Security Administrator** group.

Procedure

1. In the main menu, select **Security**→**Monitor User Session**.
2. In the **Monitoring User Session** tab, view the information of the online user.



The screenshot shows the UNM2000 interface with the 'Monitoring User Session' tab selected. The table displays the following data:

Login ID	User ID	Username	IP Address	Port Number	Online Time	User Type
366232	1	admin(Local Client End)	10.32.150.5	59226	3 Minutes, 44 Seconds	Administrator
366231	1	admin	10.168.17.33	53327	18 Minutes, 9 Seconds	Administrator
366230	1	admin	10.168.17.172	59297	21 Minutes, 49 Seconds	Administrator
366229	1	admin	10.170.100.2	59486	25 Minutes, 19 Seconds	Administrator
366227	1	admin	10.168.17.54	58969	28 Minutes, 51 Seconds	Administrator
366222	1	admin	10.170.160.79	61795	1 Hours, 4 Minutes, 2 Seconds	Administrator

At the bottom of the table, it indicates 'Total 6 entries'. Below the table are buttons for 'Refresh', 'Send Message...', and 'Forced Offline'. The user interface also shows the user 'admin' and IP address '10.170.1.28' at the bottom right.

Other Operations

Right-click in the **Monitor User Session** tab and click **Refresh**, **Copy Cell**, **Print** or **Export**.

3.4.2 Logging Out Users

By monitoring user sessions, you can view the information of the online users and log out the users who may influence the system security as needed, so as to ensure the system security.

Background Information

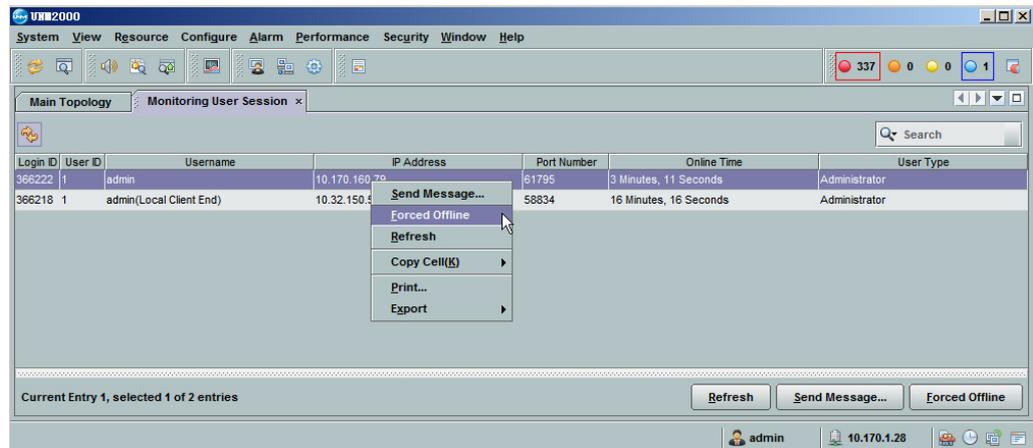
- ◆ Session: The connection set up between the client end and the server.
- ◆ When the user login mode is set to **Multi-User Mode**, one user account can log in multiple client ends at the same time. You can specify the maximum number of concurrent online users using a same account. For details, see [Creating Users](#).
- ◆ The object of forced exiting and sending messages is the user session. For example, if the user account “user” logs in the same UNM2000 server via client ends A and B, sessions a and b will be generated respectively. When the account “user” generating session a is forced to exit, the account “user” generating session b is not influenced.
- ◆ The superuser **admin** can force all users except for itself to exit, and the users in the security administrator can only force the common users to exit.

Prerequisite

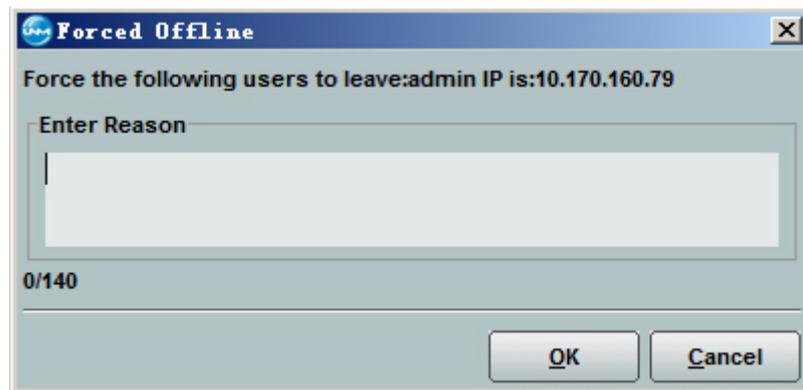
You have logged in as a member of the **Security Administrator** group.

Procedure

1. In the main menu, select **Security**→**Monitor User Session**.
2. In the **Monitoring User Session** tab, view the information of the online user.
3. Right-click the corresponding user session, and select **Forced Offline** from the shortcut menu.



4. Type the reasons in the **Forced Offline** dialog box, and click **OK**.



3.4.3 Sending Messages to Online Users

Sending messages to online users implements the convenient communication between users.

Background Information

- ◆ Session: The connection set up between the client end and the server.
- ◆ When the user login mode is set to **Multi-User Mode**, one user account can log in multiple client ends at the same time. You can specify the maximum number of concurrent online users using a same account. For details, see [Creating Users](#).

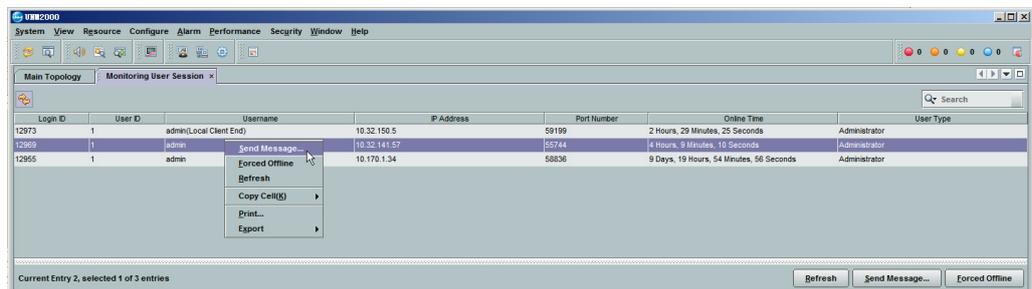
- ◆ The object of forced exiting and sending messages is the user session. For example, if the user account “user” logs in the same UNM2000 server via client ends A and B, sessions a and b will be generated respectively. When the account “user” generating session a is forced to exit, the account “user” generating session b is not influenced.
- ◆ The UNM2000 does not support the user of the current session sending messages to himself or herself.

Prerequisite

You have logged in as a member of the **Security Administrator** group.

Procedure

1. In the main menu, select **Security**→**Monitor User Session**.
2. In the **Monitoring User Session** tab, view the information of the online user.
3. Right-click the corresponding user session, and select **Send Message** from the shortcut menu.



4. Type the message contents in the **Send Message** dialog box, and then click **OK**.

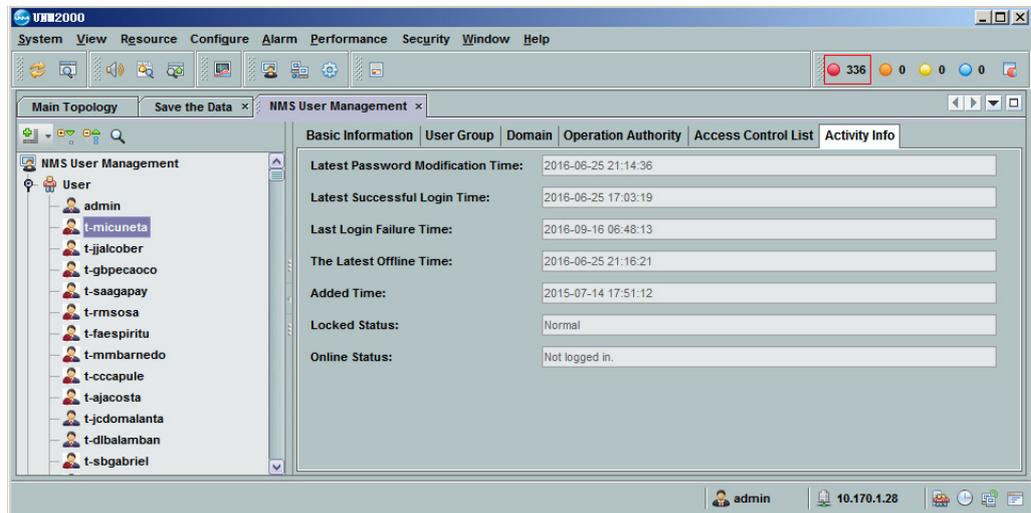
3.4.4 Monitoring User Activities

You can monitor the user action information, so as to prevent illegal operations of users.

Procedure

1. Select **Security**→**NMS User Management** from the main menu to display the **NMS User Management** window.

2. Click  before the **User** node to expand the user node.
3. Click the corresponding user and click **Activity Info** in the right pane to view the activity information of the user.



Note:

When an operation influences the UNM2000, you can perform operations on the corresponding user accordingly. For example, log out the user in the **Monitor User Session** window.

3.5 Authorization and Domain Division

The following takes assigning authority for users in two areas as example to introduce how to create user accounts and assign authority.

Scenario Description

The devices in Area A and Area B are managed by UNM2000 for uniform supervision. The device in Area A is monitored, operated and maintained by working staff in Area A and the device in Area B is monitored, operated and maintained by working staff in Area B. Therefore, the working staff in Area A and Area B should be allocated with user accounts and authority respectively.

Procedure

1. Create object sets.

Create object set A and object set B according to the area division. Add the devices of Area A and Area B to the members of object set A and object set B.

For creating object sets, see [Creating an Object Set](#).

2. Create operation sets.

Adopt the default operation sets according to the users' responsibilities.

- ▶ The working staff responsible for monitoring: the application supervisor set and the network supervisor set.
- ▶ The working staff responsible for operation: the application operator set and the network operator set.
- ▶ The working staff responsible for maintenance: the application maintainer set and the network maintainer set.

For creating operation sets, see [Creating Operation Groups](#).

3. Create user groups.

According to the users' responsibilities, it is required to create six user groups, as shown in Table 3-3.

Table 3-3 Creating User Groups

User Group Name	User Group Type	Management Domain	Operation Authority
Inspector Group A	Common user group	Object Group A	Application supervisor set and network supervisor set
Operator Group A	Common user group	Object Group A	Application operator set and network operator set
Maintainer Group A	Common user group	Object Group A	Application maintainer set and network maintainer set
Inspector Group B	Common user group	Object Group B	Application supervisor set and network supervisor set
Operator Group B	Common user group	Object Group B	Application operator set and network operator set
Maintainer Group B	Common user group	Object Group B	Application maintainer set and network maintainer set

For details of creating user groups, see [Creating User Groups](#).

4. Create users.

- ▶ Create the user's basic information. Set the username and password. For security, select **Modify Password on Next Login** or set the valid days of the password.
- ▶ Set the login time ranges according to the working shifts of the staff.
- ▶ Set the users' user groups. If six user groups A, B, C, D, E, and F are to be created, as shown in Table 3-4. After being assigned with a user group, the user will be authorized with the management domain and operational authority of the user group.

Table 3-4 Creating Users

User	User Group
A	Inspector Group A
B	Operator Group A
C	Maintainer Group A
D	Inspector Group B
E	Operator Group B
F	Maintainer Group B

- ▶ Set the access control list to restrict users' login IP address to the specified ones.

For details of creating user groups, see [Creating Users](#).

After completing the above configurations, provide the user accounts for the corresponding staff.

4 Configuration Management

The configuration management means the operations to configure the information of the network and the system equipment, and is the most significant management function of the UNM2000.

- NE Communication Route Management
- SNMP Parameter Template
- ONU Capability Set Template
- Managing Global Templates
- Managing Global Configurations
- Tracing Signaling
- Configuration Synchronization
- Network Access Management
- Pinging NEs
- Telnet NE
- The Tracert Function of the UNM2000 Server
- Migrating the PON Configuration

4.1 NE Communication Route Management

By using the NE communication management function, you can set the Manager server IP address and the receiver address of Trap. The following introduces how to manage NE communication routes.



Note:

You can configure multiple EMS server addresses when using distributed deployment mode of EMS servers.

4.1.1 NE Management Program

The NE management program is used to set the communication protocol between the UNM2000 and the device. Only when the NE management program is correctly configured can normal communication between the UNM2000 and the device be ensured so as to manage devices through the UNM2000.

4.1.1.1 Creating the Management Program

Correct configuration of the NE management program is the prerequisite to ensure normal communication between the UNM2000 and the NEs.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Configure**→**NE Communication Route Management** from the main menu to open the **NE Communication Route Management** tab.



Note:

- ◆ The **anm_manager-1507393536(127.0.0.1)** is the default management program. If no management program and no partition are configured during the creation of the NE, the default management program will be selected for the NE.
 - ◆ It is supported only one NE communication routing management in the singleton mode and no need to add.
-

2. Right-click **NE Communication Route Management**, and select **Create Management Program** from the shortcut menu. Configure various parameters of the management program, and click **OK**.

4.1.1.2 Deleting / Modifying a Management Program

In case of network resource adjustment and that changes are made to the management program that the NE belongs to, you can delete the management program and then create one or directly modify the management program to meet your requirement.



Note:

Deleting the default management program is not supported.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Configure**→**NE Communication Route Management** from the main menu to open the **NE Communication Route Management** tab.
2. Delete a management program:



Note:

Deleting the default management program is not supported.

- 1) In the left pane of the **Communication Routing Management** tab, right-click the management program and select **Delete the Manager** from the shortcut menu.
- 2) Click **OK** in the dialog box that appears to complete deleting the management program.
3. Modify a management program:
 - 1) In the left pane of the **Communication Routing Management** tab, right-click the management program and select **Manager Property** from the shortcut menu.
 - 2) Modify the parameters as needed in the **Manager Properties** dialog box that appears, and then click **OK**.
 - 3) Click **Yes** to save the settings.

Other Operations

1. In the left pane of the **Communication Routing Management** tab, click  → **Pass-through before the management program**. The right pane displays the pass-through NE list under the current management program.
2. Right-click an NE and select the corresponding operation from the shortcut menu: **Cancel Manager Management**, **Copy NE**, **Delete NE**, **modify NE Attribute**, etc.



Note:

Copy NE is used to copy the NE of the same type. After copying an NE, users only need to modify the different parameters (such as the IP address), so that they can create NEs rapidly.

4.1.1.3 Pre-configuration

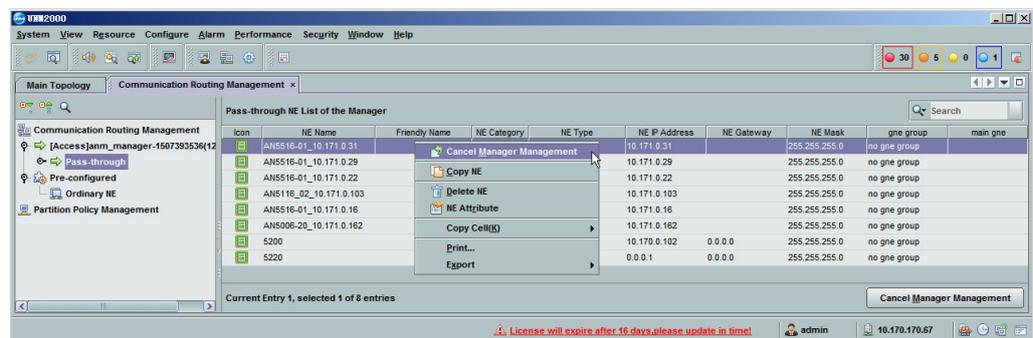
The NEs in the **Pre-configured** communication NE list are those without management program.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Configure**→**NE Communication Route Management** to open the **Communication Routing Management** tab.
2. In the left pane of the **Communication Routing Management** tab, click **Pass-through** before the management program.
3. Click a certain NE in the **Pass-through NE List of the Manager** in the right pane and select **Cancel Manager Management** from the shortcut menu. This NE is moved to **Pre-configured** NE list.



Subsequent Operation

1. Right-click a certain NE in the pre-configured common NE list and select **Select Management Object** from the shortcut menu, or click a certain NE in the pre-configured common NE list and click the **Select Management Object** button to select a management program for the NE again.
2. Click **OK**. The NE is moved to the pass-through NE list.

4.1.2 Partition Policy Management

The partition policy can be used to divide the NEs in a same management program according to the start IP address and end IP address of the partition. The NEs will be assigned to the corresponding management program for management according to the partition policy automatically after adding.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Configure**→**NE Communication Route Management** from the main menu to open the **NE Communication Route Management** tab.
2. Right-click **Partition Policy Management** in the left pane and select **Create a Partition** from the shortcut menu. In the displayed dialog box, set the parameters and click **OK**.



Note:

- ◆ **Manager Name:** Indicates the name of the created management program.
 - ◆ After the partition is created
 - ▶ If the management program has not been configured upon NE creation, the UNM2000 will assign the corresponding management program according to the partition to which the NE's IP address belongs.
 - ▶ If the management program has been configured upon NE creation, although inconsistent with the management program of the partition to which the NE's IP address belongs, this management program is still preferred.
-

Other Operations

Right-click the created partition and select **Create a Partition**, **Modify Partition** or **Delete the Partition** from the shortcut menu to perform the corresponding operation.

4.2 SNMP Parameter Template

To ensure the communication between the EMS and the NE, it is necessary to configure the SNMP parameters of NEs at the UNM2000.

You can directly configure the SNMP parameters of NEs at the UNM2000 side, create NEs manually, or automatically apply the SNMP parameters by using the applicable SNMP parameter template upon NE automatic discovery.

4.2.1 Creating and Using the SNMP Parameter Template

You can manage the SNMP parameter templates used for the communication between the UNM2000 and the NEs.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Background Information

The SNMP parameter template named **default** is the default template and cannot be deleted. If no SNMP parameter template is set for an access NE during the creation, the NE will use the default SNMP parameter template **default**.

Procedure

1. Select **Configure**→**SNMP Parameter Template** from the main menu to open the **SNMP Parameter Template Management** tab.
2. Click **Create** to open the **SNMP Parameter Template** dialog box, set various parameters and click **Create**.
3. Right-click the specific template and select **Bind NE** from the shortcut menu to open the **Select Bound NE** dialog box. Select the NE to be bound and click **OK**.

4. After the NE is bound, the information on the NE bound with the SNMP parameter template will be displayed in the **Binding NE Information** pane.

Other Operations

Modify the SNMP parameter template bound with the NE.

1. In the main topology window, right-click the NE and select **Attribute**. The **Attribute Page** dialog box appears on the right.
2. In the **Basic Information** dialog box, click the SNMP parameter template and select a new template from the drop-down box to modify the SNMP parameter template bound with the NE.

4.2.2 Modifying / Deleting an SNMP Parameter Template

You can manage the SNMP parameter templates used for the communication between the UNM2000 and the NEs.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Background Information

The SNMP parameter template named **default** is the default template and cannot be deleted.

Procedure

1. Select **Configure**→**SNMP Parameter Template** from the main menu to open the **SNMP Parameter Template Management** tab.
2. In the upper pane of the **SNMP Parameter Template Management** dialog box, select the desired SNMP parameter template.
 - ▶ Modify the parameter settings in the **SNMP Parameter Template** pane at the lower part and then click **Modify**.
 - ▶ Click **Delete** to delete the SNMP parameter template.



Note:

The SNMP parameter template bound with an NE cannot be deleted.

4.3 ONU Capability Set Template

The current method of adapting to the NE by adding the ONU type code cannot meet the ever-increasing requirements for adaptation of new terminal types.

With the ONU capability set template, you can configure the parameters such as ONU port quantity, port type and resource type. The UNM2000 can deliver it to the device to support the new type of ONU in real time, which quickly meet the adaptation requirements without upgrading the device.

4.3.1 Adding an ONU Capability Set Template

You can create an ONU capability set template, configure the parameters such as ONU port quantity, port type and resource type and then deliver it to the device to quickly adapt to the new ONU.

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The ONU capability set template is enabled.

Procedure

1. Select **Configure**→**ONU Capability Set Template** from the main menu to open the **ONU Capability Set Template** tab.
2. Click  or right-click in the blank area of the **ONU Capability Set Template** and select **Create Model**.
3. In the displayed **Create a ONU Capability Set Template** dialog box, set various parameters and click **OK**.

Other Operations

Binding an ONU capability set template

1. In the **ONU Capability Set Template** window, right-click the specified template. Select **Bind NE** from the shortcut menu to open the **Select Bound NE** dialog box.
2. Select the NE to be bound and click **OK**. After the NE is bound, the information of the bound NE will be displayed in the **Binding NE Information** pane on the right.



Note:

The ONU capability set template bound with an NE cannot be deleted.

4.3.2 Modifying an ONU Capability Set Template

When the ONU capability set template cannot meet the user requirement, you can modify the template as needed.

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The ONU capability set template is enabled.

Procedure

1. Select **Configure**→**ONU Capability Set Template** from the main menu to open the **ONU Capability Set Template** tab.
2. Select an ONU capability set template and click  or right-click to select **Modify Model**.

Other Operations

Deleting the ONU capability set template

1. In the **ONU Capability Set Template** window, select an ONU capability set template and click  or right-click to select **Delete Template**.



Note:

The ONU capability set template bound with an NE cannot be deleted.

4.4 Managing Global Templates

A template is a set of attributes with specific values. For example, if a template is referenced to configure the resources, such as ADSL or G.SHDSL port, the parameter values of the attributes preset in the template will be automatically adopted by the resource.

You can use a template to configure multiple NEs of the same model in the administrative domain of the entire network by using the global profile, so as to improve the project start-up efficiency.

4.4.1 Viewing the Global Template

You can configure multiple NEs of the same model in the administrative domain of the entire network in a batch manner by using the global profile, so as to improve the project start-up efficiency.

Prerequisite

You have the authority of **Operator Group** or higher authority.



Note:

The following uses the **ADSL Line Template** of the AN5006–20 as an example. You can follow the same procedures to view other templates with the only difference in the access method.

Procedure

1. Select **Configure**→**Global Template Manager** from the main menu to open the **Global Template Management** tab.

2. Select **Global Profile**→**ADSL Line Profile** under the AN5006-20 to open the **Line Profile** tab.
3. Click the template entry in the **ADSL Line Profile** tab to view the NE bound with the template.

Other Operations

In the **ADSL Line Profile** dialog box, right-click the template entry and select **Add**, **Delete**, **Batch Modify**, **Compare Templates**, **Bind to System Card / Port**, etc.

4.4.2 Adding a Global Template

When the existing global templates do not meet the requirements or new global templates are needed, follow the steps below to add global templates.

Prerequisite

You have the authority of **Operator Group** or higher authority.



Note:

The following uses the **Packets Rate Control Profile** of the AN5116–06B as an example. You can follow the same procedures to bind other templates with the only difference in the access method.

Procedure

1. Select **Configure**→**Global Template Manager** from the main menu to open the **Global Template Management** tab.
2. Select **Global Profile**→**Packets Rate Control Profile** under the AN5116-06B to open the **Packets Rate Control Profile** tab.
3. Click  to open the **Enter the number of rows to add** dialog box, enter the number of templates to be added and click **OK**.
4. Complete the parameter settings of the packet rate control template(s) in the right pane and click . The system automatically generates the **Global Template ID**.

4.4.3 Modifying a Global Template

When the existing global templates do not meet your requirements, you can create global templates by following operations.

Background Information

- ◆ You can only modify the parameter settings of the template with the template name unchanged after a global template is saved.
- ◆ The UNM2000 will automatically update the modified parameter settings of the template.

If the template is bound with a device, the device will be issued automatically after the parameter settings of the template is saved.

Prerequisite

You have the authority of **Operator Group** or higher authority.

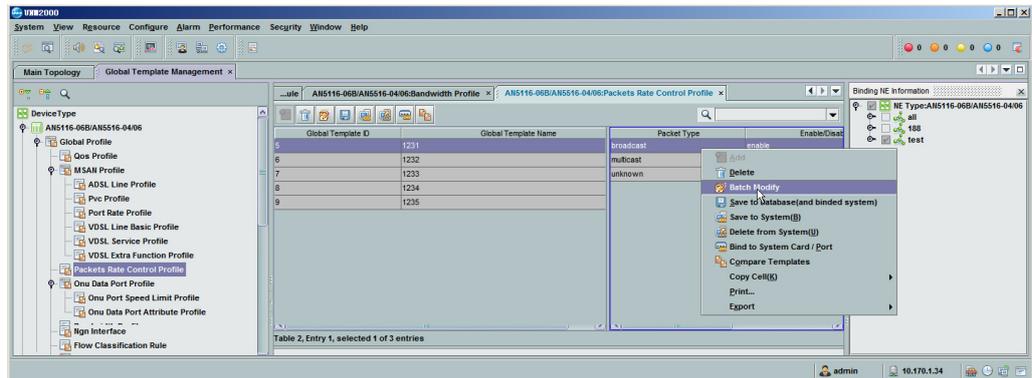


Note:

The following uses the **Packets Rate Control Profile** of the AN5116-06B as an example. You can follow the same procedures to bind other templates with the only difference in the access method.

Procedure

1. Select **Configure**→**Global Template Manager** from the main menu to open the **Global Template Management** tab.
2. Click **Device Type**→**AN5116-06B**→**Global Profile**→**Packets Rate Control Profile** under the **Global Template Management** tab to open the **Packets Rate Control Profile** tab.
3. On the **Packets Rate Control Profile** tab, right-click the desired template and select **Batch Modify** to open the **Batch Modify** dialog box.



4. Modify the parameter settings in the **Batch Modify** dialog box and click **Apply** → **OK** at the lower part to save the changes.

4.4.4 Binding / Unbinding a Global Template

You can bind a global template with a device so that the parameter settings of the device are consistent with those set in the global template in the UNM2000.

Prerequisite

You have the authority of **Operator Group** or higher authority.



Note:

The following uses the **Packets Rate Control Profile** of the AN5116–06B as an example. You can follow the same procedures to bind other templates with the only difference in the access method.

Procedure

1. Select **Configure** → **Global Template Manager** from the main menu to open the **Global Template Management** tab.
2. Double-click **Global Profile** → **Packets Rate Control Profile** under the AN5116-06B to open the **Packets Rate Control Profile** tab.
3. Select a template and click , or right-click it and select **Save to System** to open the **Select Object** dialog box. Select a desired system and click **OK**.

4. Bind a card / port (for the template to be bound with a card / port).
 - 1) Select a template and click , or right-click it and select **Bind to System Card / Port** to open the **First Select NE** dialog box. Select a desired NE and click **Next**.
 - 2) The **Please Select ONU Port** dialog box appears. Select a desired port and click **Next**. After the binding is completed, the corresponding binding information appears in the **Binding NE Information** pane.
5. Unbind a template.
 - 1) In the **Packets Rate Control Profile** dialog box, click .
 - 2) In the displayed **Select Object** dialog box, select the device information and click **OK** to unbind the template from the device.

Other Operations

Select the shortcut menu or click the button on the toolbar to perform the corresponding operation on the template, such as **Delete**, **Batch Modify**, **Delete from System** and **Compare Templates**.

4.4.5 Deleting a Global Template

When a global template is no longer needed, you can delete it.

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The template to be deleted is not bound with any device; otherwise, see [Binding / Unbinding a Global Template](#) to unbind the template from the device.



Note:

The following uses the ADSL Line Template as an example. You can follow the same procedures to delete other templates with the only difference in the access method.

Procedure

1. Select **Configure**→**Global Template Manager** from the main menu to open the **Global Template Management** tab.
2. Select **ADSL Line Profile** in the left pane to open the **ADSL Line Profile** tab.
3. Click  to open the **Configure the Selection Range** dialog box, select the corresponding range according to the quantity of templates to be deleted and then click **OK**.

4.5 Managing Global Configurations

The global configuration is a set of attributes with specific values. You can use the global configuration to configure NEs of multiple types (non-template) in the administrative domain of the entire network, so as to improve the project start-up efficiency.

4.5.1 Viewing Global Configurations

You can configure NE devices of multiple types (non-template) within a global network management domain uniformly, so as to enhance the project provisioning efficiency.

Prerequisite

You have the authority of **Operator Group** or higher authority.



Note:

The following uses the **Voip Service Vlan** under **Voice Service Config** of the AN5006–30 as an example. You can follow the same procedures to view other templates with the only difference in the access method.

Procedure

1. Select **Configure**→**Global Template Manager** from the main menu to open the **Global Template Management** tab.

2. In the left pane, select **Global Config**→**Voice Service Config**→**Voip Service Vlan** to open the Voip Service Vlan tab and view the existing voice VLAN configuration data.

4.5.2 Adding the Global Configuration

When the existing global configurations do not meet the requirements or new global configurations are needed, follow the steps below to add the global configuration.

Prerequisite

You have the authority of **Operator Group** or higher authority.



Note:

The following uses the **IGMP Mode** under **Service Config** of the AN5116-06B as an example. You can follow the same procedures to perform the operation on other global configurations with the only difference in the access method.

Procedure

1. Select **Configure**→**Global Template Manager** from the main menu to open the **Global Template Management** tab.
2. In the left pane, select **Global Config**→**Service Config**→**IGMP Mode** to open the **IGMP Mode** tab.
3. Click  to open the **Enter the number of rows to add** dialog box, enter the number of entries to be added and click **OK**.
4. In the multicast mode dialog box, complete the parameter settings and click . The system generates the **Global Configuration ID** automatically.

4.5.3 Modifying the Global Configuration

When the existing global configurations do not meet your requirements, you can modify the global configurations according to your needs.

Prerequisite

You have the authority of **Operator Group** or higher authority.



Note:

The following uses the **IGMP Mode** under **Service Config** of the AN5116-06B as an example. You can follow the same procedures to perform the operation on other global configurations with the only difference in the access method.

Procedure

1. Select **Configure**→**Global Template Manager** from the main menu to open the **Global Template Management** tab.
2. In the left pane, select **Global Config**→**Service Config**→**IGMP Mode** to open the **IGMP Mode** tab.
3. In the **IGMP Mode** tab, right-click the desired configuration entry and select **Batch Modify** to open the **Batch Modify** dialog box.
4. Modify the parameter settings in the **Batch Modify** dialog box and click **Apply** →**OK** at the lower part to save the changes.

4.5.4 Issuing the Global Configuration to Device

The following introduces how to issue the global configuration to device and make the device parameter consistent with the global configuration parameter.

Prerequisite

You have the authority of **Operator Group** or higher authority.



Note:

The following uses the **ARP Proxy Switch** under **Service Config** of the AN5116-06B as an example. You can follow the same procedures to perform the operation on other global configurations with the only difference in the access method.

Procedure

1. Select **Configure**→**Global Template Manager** from the main menu to open the **Global Template Management** tab.
2. in the left pane, select **Global Config**→**Service Config**→**ARP Proxy Switch** to open the **ARP Proxy Switch** tab.
3. Select the configuration and click  or right-click the **Save to Database** from the shortcut menu to open the **Configure the Selection Range** dialog box. Select range and click **OK**.
4. Select the configuration and click  or right-click the **Save to Database** from the shortcut menu to open the **Configure the Selection Range** dialog box. Select range and click **OK**.

4.5.5 Deleting a Global Configuration Template

When a global template is no longer needed, you can delete it.

Prerequisite

You have the authority of **Operator Group** or higher authority.



Note:

The following uses the **Voip Service Vlan** under **Voice Service Config** of the AN5006–30 as an example. You can follow the same procedures to delete other templates with the only difference in the access method.

Procedure

1. Select **Configure**→**Global Template Manager** from the main menu to open the **Global Template Management** tab.
2. In the left pane, select **Global Config**→**Voice Service Config**→**Voip Service Vlan** to open the **Voip Service Vlan** tab.
3. Select the global config needed to be deleted, click  to delete the object.

4.6 Tracing Signaling

Tracing the signaling is used to trace the signaling frame of the communication between the current IAD and the voice communication card, so as to find the communication faults in a timely manner.

Background Information

This function is only supported by the FTTH-type and FTTB-type ONUs that support voice service.

Prerequisite

Set the **Signaling Trace Reporting Enable Status** of the signaling-traced object to **Enable** in the **SNMP TRAP Receiver IP (NE Manager**→**Local Service Config)**.

Procedure

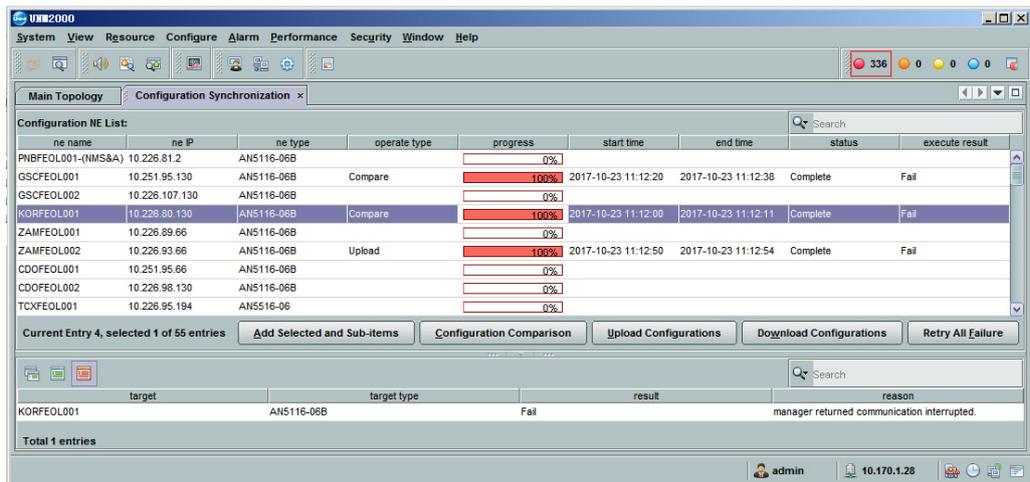
1. In the main menu, select **Configure**→**Signaling Tracing** to open the **Select Signaling Tracing Object** dialog box.
2. Select the signaling tracing object in the pane and click **OK**. Add one row in the right pane. Then set **IP address**, **Four-layer source port number**, and **4 Layer Destination Port Number**.
3. Click **OK** to open the **Signal Trace** tab.
4. Click **Start** to perform tracing signaling.

4.7 Configuration Synchronization

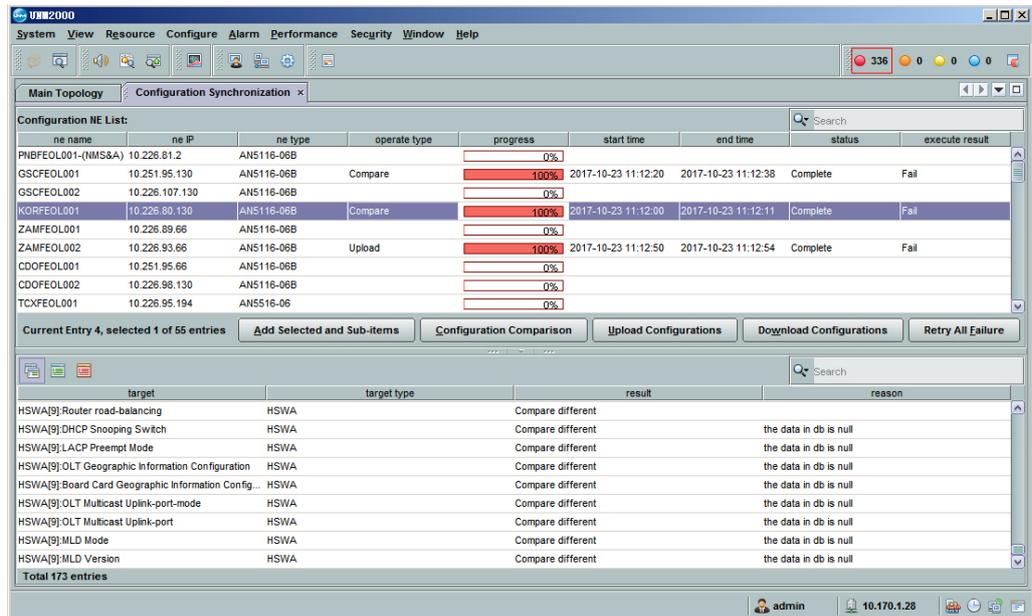
The configuration synchronization function implements the comparison between the configuration data in the UNM2000 and that on the device. If any difference is detected, the corresponding data will be downloaded or uploaded to ensure consistency of the configuration.

Procedure

1. Select **Configure**→**Configuration Synchronization** from the UNM2000 main menu to display the **Configuration Synchronization** tab.
2. Click **Add Selected and Sub-items** to open the **add ne** dialog box, select the objects to be compared and select **OK**. The **Configuration Synchronization** tab displays the added NE whose configuration is to be synchronized.



3. Select the objects to be compared in the configuration synchronization NE list, and click **Configuration Comparison** to compare the configuration.
4. View the comparison result in the lower part of the **Configuration Comparison** tab.



Subsequent Operation

When the comparison results are different, you can click **Config Upload** or **Config Download** to upload or download the configuration according to Table 4-1.

Table 4-1 Configuration Uploading / Downloading

Button	Description
Config upload	Uploads the configuration data of the equipment to the network management database.
Config download	Downloads the configuration data from the network management database to the equipment.

4.8 Network Access Management

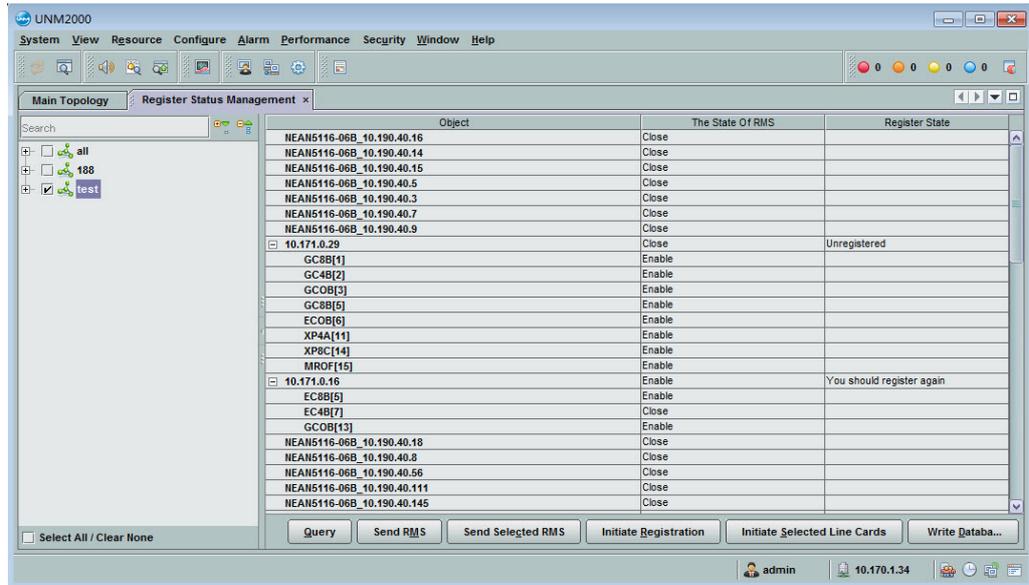
The network access management helps you analyze and observe the resource interconnection status and network access status of the system and the line card.

Prerequisite

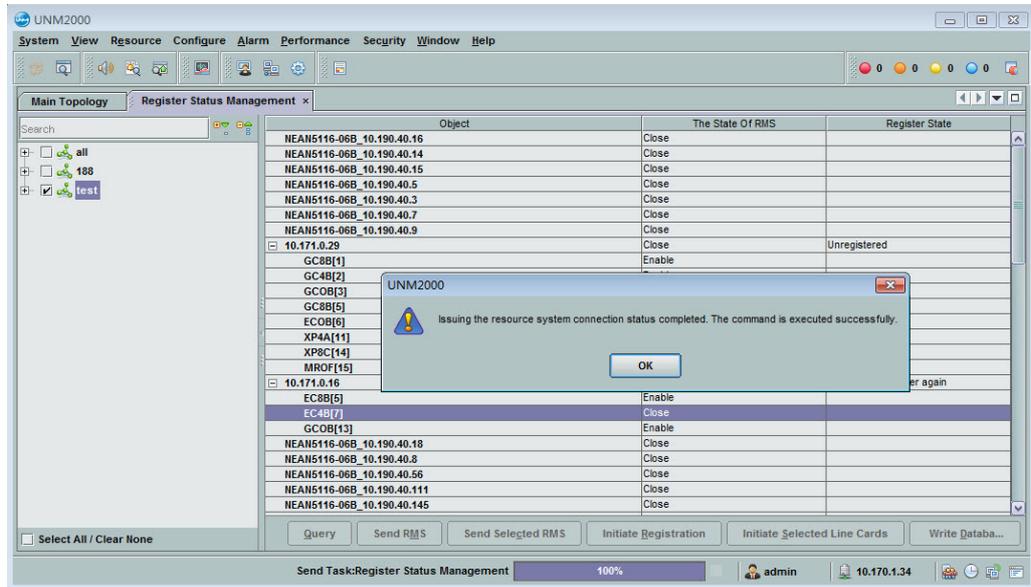
You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **Configure**→**Network Access Status Management** to open the **Register Status Management** tab.
2. Select the desired object in the object tree and select the **Query Status** button to query the resource management system interconnection status and registration status of the object.



3. Select the system / card to be registered in the object tree, and click the **Send RMS Connection Status** or **Send the Selected Line Card RMS Connection Status** button to enable the interconnection with the resource management system.
4. Select the system / card to be registered and click the **Initiate Registration** or **Initiate Registration of the Selected Line Cards** button. After the registration succeeds, the status is as shown in the following figure.



- Click the **Write DB** or **Read DB** button to write the configuration into the database or read the configuration from the database.

4.9 Pinging NEs

The Ping operation is used to check whether the communication between NEs and the EMS is normal.

Procedure

- Right-click the object in the main topology object tree and select **Ping** from the shortcut menu. In the displayed **Command Tool** dialog box, view the Ping operation result.

4.10 Telnet NE

When the UNM2000 client cannot access the device directly, it can access the device via Telnet or access the Telnet proxy server to perform operations via CLI. For setting the Telnet proxy server, see [Setting the Telnet / SSH Proxy Server](#).

Procedure

1. Right-click the object in the main topology object tree and select **Telnet** from the shortcut menu.
2. In the displayed **Command Tool** dialog box, enter the username and password to log into the CLI and perform operations via the CLI.

4.11 The Tracert Function of the UNM2000 Server

The UNM2000 supports performing the Tracert operation from the UNM2000 server to the specified IP address.

Background Information

The Tracert (tracing the route) function is used to test the gateway that the data packet passes from the source host to the destination. It mainly checks whether the network connection is reachable and analyzes the failure occurrence location in the network. The Tracert command uses the IP Time to Live (TTL) field and the ICMP error message to determine the route from a host to another host in the network.

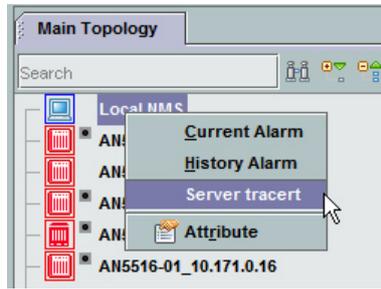
The command is Tracert on Windows OS and it is Traceroute on UNIX OS.

Prerequisite

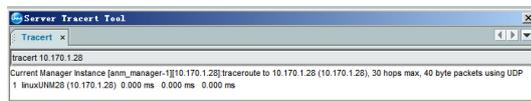
- ◆ The authority of the Tracert function is configured in the authority and domain division management. Only if have the corresponding authority can you perform the Tracert function.
- ◆ At present, it only needs to support sending the Tracert packet to the IP address in the IPv4 format, and it does not need to support sending the Tracert packet to the IP address in the IPv6 format and the host domain name.

Procedure

1. In the **Main Topology** pane of the UNM2000 main topology, right-click **Local NMS** and select **Server tracert**.



2. In the **Server Tracert Tool** command dialog box, enter the specified IP address and press Enter. The Tracert result appears in the command window.



4.12 Migrating the PON Configuration

The UNM2000 supports PON configuration migration as well as the PON port configuration migration.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Configure**→**PON Configuration Migration** from the main menu to open the **Operation Instructions** alert box.
2. Click **OK** to open the **PON Configuration Migration** dialog box.
3. Set the parameters, such as source OLT and destination OLT.
4. Click **Execute**.
5. Click **Yes** in the alert box that appears.

5 Topology Management

The topology management is used to create and manage the topology architecture of the entire network, so as to present the network connection status and operating status of the equipment. You can view the topology objects and real-time alarm prompts in the topology view.

- Topology Creation Flow
- Creating a Global Logical Domain
- Creating NEs
- Adding Cards
- Creating a Link
- Editing an NE
- Editing a Fiber Connection
- Browsing the Topology View
- Deleting the Topology

5.1 Topology Creation Flow

The creation flow of the network topology describes the creation procedures of the subnet, NEs, cards and links as well as the relationship among the operation tasks. The creation flow of the network topology is as shown in Figure 5-1.

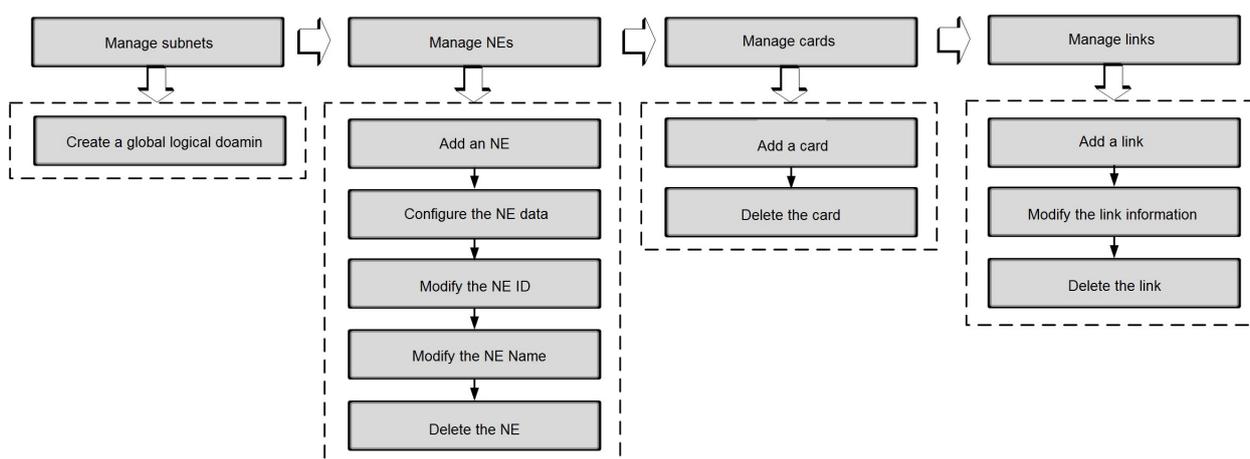


Figure 5-1 Flow for Creating the Network Topology

In the creation flowchart, the horizontal procedures indicate the four phases of the network topology creation: creating the subnet, creating the NE, creating the card and creating the link; the vertical procedures indicate the operation tasks included in each phase.

The creation flow of the network topology is as shown in Table 5-1.

Table 5-1 Description of the Network Topology Creation Flow

Procedure	Operation	Description
Manage the subnet	Create a global logical domain	For convenient management, the topological objects in the same area or of the similar attributes can be placed and displayed at the same topological layer.
Manage the NE	Create the NE	To manage the physical devices through the UNM2000, you need to create the corresponding NEs in the UNM2000. Creating NEs includes creating the access NE and virtual NE, and discovering the NE automatically.
	Configure the NE data	The NEs are not configured after being created. Before managing the NEs via the UNM2000, you need to configure the NE data first.
	Modify the NE ID	The NE ID is the unique identifier of the NE. During the network planning, each NE must be assigned an unique ID. In case of NE ID conflicts, the route conflicts will occur and consequently some NEs cannot be managed. To adjust the original planning and modify the NE ID during debugging or capacity expansion, you can modify it through the UNM2000.

Table 5-1 Description of the Network Topology Creation Flow (Continued)

Procedure	Operation	Description
	Modify the NE name	You can modify the NE name as needed at any time. Modifying the NE name does not influence the running of the NE.
	Delete the NE	If an inappropriate NE is created, you can delete it in the UNM2000. Deleting the NE will cause loss of all information related to the NE in the UNM2000; however, it will not influence the running of the device.
Manage the card	Add the card	During manual configuration of NE data, if a physical card is added after configuring the NE data, you need to add the card on the NE panel.
	Delete the card	In case of network configuration change or modifying the card configuration the NE is required, you can delete the card from the NE panel.
Manage the link	Create the link	You can create links, cables as well as virtual fibers on the UNM2000.
	Modify the fiber connection information	You can modify the name, attenuation, length and type of the fiber according the connection status and physical features of the fiber.
	Delete the fiber	To delete an NE or modify the fiber connection between NEs during network adjustment, you need to delete the fiber connection between the NEs.

5.2 Creating a Global Logical Domain

For convenient management of NEs, you can customize logical domains and place the NEs in the same area or of the same attribute into a same logic domain. The domain is a set of various NEs, and sub logical domains can be created under it. For example, you can create a logical domain named Site A, and then create sub logical domains Area 1, Area 2, etc. under Site A.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Resource**→**Create Logical Domain** to open the **Create Global Logical Domain** dialog box.
2. In the **Create Global Logical Domain** dialog box, set various parameters, in which the logical domain name is required and other parameters are optional .

3. After configuring the parameters, click **OK**. The created logical domain appears in the main topology.

Other Operations

Right-click the logical domain and select the shortcut menus to perform the corresponding operations.

5.3 Creating NEs

To manage the physical devices through the UNM2000, you need to create the corresponding NEs in the UNM2000. There are two ways to create the NEs: Manual creation and automatic discovery. For creating the network topology architecture, manual creation of NEs in a batch manner is recommended. For network capacity expansion, automatic discovery of NEs is recommended.

5.3.1 Create Access NE

Only when the access NE is created can the access devices be managed via the UNM2000.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main topology, right-click to select **Create NE** → **Create Access NE**, or select **Resource** → **Create NE** → **Create Access NE** from the main menu to open the **Create Access NE** dialog box.
2. Set the parameters according to Table 5-2.

Table 5-2 Settings of Creating the Access NE

Parameter	Description	Comment
NE Type	NE type.	Required.
Default Shelf Type	After the NE type is selected, the corresponding subrack (shelf) type will be determined by the system.	
NE Name	The name of the NE for identification.	

Table 5-2 Settings of Creating the Access NE (Continued)

Parameter	Description	Comment
IP address of the NE	The IP address of the NE.	Optional
NE Mask	The mask of the NE.	
NE Gateway	The IP address of the gateway NE.	
Alias Name	The alias of the NE. If this item is configured, the main topology will display the alias; If this item is not configured, the main topology will display the NE name.	
NE SN	The NE attribute information used for identifying the NE.	
Manufacturer Name		
Remark		
Username		
Password		
Longitude	The longitude and latitude of the physical area to which the device locates, convenient for locating.	
Latitude		
Topo Level	The topological level to which the NE belongs.	
Manager	The management program to which the NE belongs. If this item is not configured, this NE belongs to the management program of its partition; if this item is not configured and no partition exists, this NE belongs to the default management program.	-
SNMP Parameter Template	The template used for the communication between the UNM2000 server and various NEs. Generally, the default template is selected.	-

- After configuring the parameters, click **OK**. The created access NE appears in the logical domain or main topology.

5.3.2 Automatic Discovery of NEs

The UNM2000 supports the NE automatic discovery function. You can set the desired IP segment, in which the NEs will be discovered automatically and created in the UNM2000. Meanwhile, the configuration data will be uploaded, adding the NEs to the UNM2000 for management.

5.3.2.1 Viewing NE Automatic Discovery Tasks

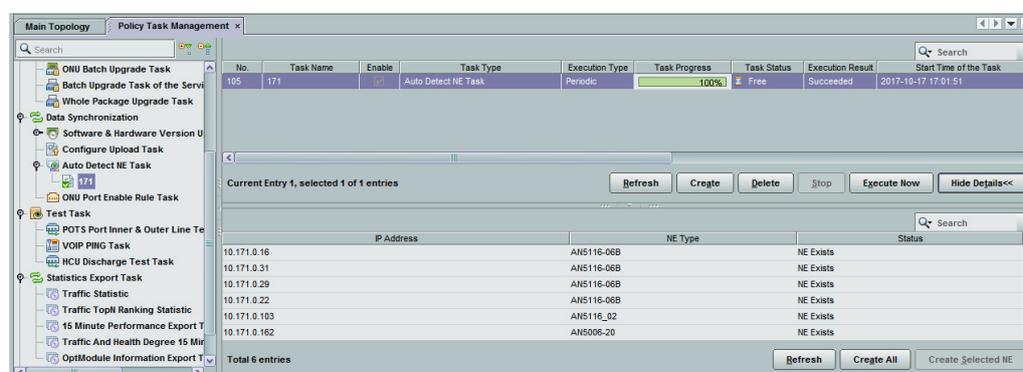
You can view the created NE automatic discovery task to automatically discover the NE information such as IP address, type and status.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

- Follow the access method below to open the **Policy Task Management** tab, to view the existing NE automatic discovery tasks.
 - Select **Resource**→**Auto Detect NE Task** from the main menu.
 - Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window. Select **Data Synchronization**→**Auto Detect NE Task** from the left pane.
- Click the created NE automatic discovery task in the left pane to view the NE IP address, NE type and status.



5.3.2.2 Creating an NE Automatic Discovery Task

You can set the system to discover the NEs inside the appointed IP address range as required and create the discovered NE automatically.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Follow the access method below to open the **Policy Task Management** tab.
 - ▶ Select **Resource**→**Auto Detect NE Task** from the main menu.
 - ▶ Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window. Select **Data Synchronization**→**Auto Detect NE Task** from the left pane.
2. Click the **Create** button at the bottom of the tab, or right-click **Auto Detect NE Task** in the left pane to open dialog box.
3. Set the parameters in the **Basic information** and **Extend information** tabs as required, and click **OK**. The new task appears in the task list.



Note:

- ◆ Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.
 - ◆ In the **Extend information** tab, click **Import IP Address** to import the IP addresses in a batch manner.
-

5.3.2.3 Automatic Discovery of NEs

You can set the system to discover the NEs inside the appointed IP address range as required and create the discovered NE automatically.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Follow the access method below to open the **Policy Task Management** tab, to view the existing NE automatic discovery tasks.
 - ▶ Select **Resource**→**Auto Detect NE Task** from the main menu.

- ▶ Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window. Select **Data Synchronization**→**Auto Detect NE Task** from the left pane.
2. Right-click a corresponding task and select **Execute Now**, or select the task and click **Execute Now** at the lower right corner of the tab to execute the NE auto discovery task.

5.4 Adding Cards

After configuring the NE data, you need to add cards in the NEs. You can manually add cards or have the cards added automatically.

5.4.1 Adding Cards Automatically

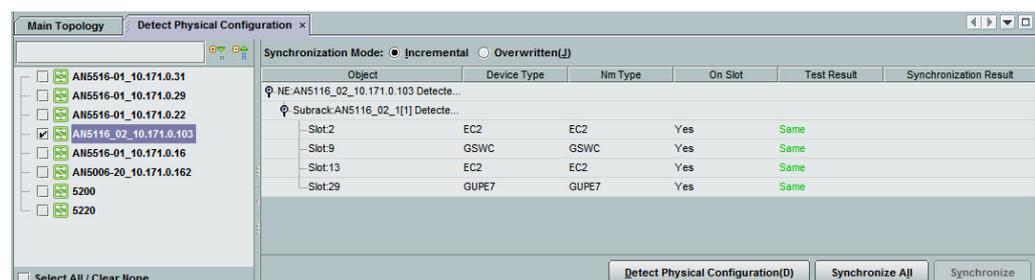
The physical configuration detection function enables you to implement the automatic discovery of physical cards, which then can be synchronized to the UNM2000 automatically using the synchronization operation.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Resource**→**Detect Physical Configuration** from the main menu to open the **Detect Physical Configuration** tab.
2. Select the system to be detected in the object tree pane, and click **Detect Physical Configuration (D)** at the lower part of the tab to execute the detection command. Then you can view the information of the detected cards and ports.



3. Select the synchronization mode according to Table 5-3, and click the **Synchronize All** button to synchronize the configuration of detected cards to the UNM2000.

Table 5-3 Synchronization Mode

Synchronization Mode	Meaning
Incremental	Only synchronizes the added cards in the physical configuration (against the current configuration in the UNM2000).
Cover type	Overrides the current configuration in the UNM2000 with the newest physical card configurations.

5.4.2 Adding Cards Manually

You can add cards manually or pre-configure the cards as required.

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The NE has been created.

Procedure

1. Right-click a desired NE in the main topology and select **Open NE Manager** from the shortcut menu to open the **NE Manager** window.
2. Add the card.
 - ▶ Adding all cards
 - a) Right-click the subrack in the device tree and select **Add All Cards** from the shortcut menu.
 - b) In the displayed dialog box, click **Yes**. The UNM2000 adds all the cards to the recommended locations respectively.
 - c) Right-click the card and select **Delete Card / Replace Card** from the shortcut menu to adjust the inserted cards according to the quantity and location of actual cards of the project.
 - ▶ Adding a single card

Right-click the slot of the card in the subrack view and select **Add Card** → **Add XXX Card** from the shortcut menu according to the actual cards and card location in the project.

Subsequent Operation

6.7 describes how to authorize the added cards and deliver the configuration to the devices.

5.5 Creating a Link

Since there are no physical connections between the OLT devices, you can create connections between any two NEs in the UNM2000 for convenient topology management.

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The NE data and card data have been configured.

Procedure

1. Right-click in the blank area of the physical topology view, and select **Create Virtual Link** from the shortcut menu to open the **Create the Virtual Connection** dialog box.
2. Table 5-4 shows how to set the parameters.

Table 5-4 Description of Parameters in the Create the Virtual Connection Dialog Box

Parameter	Description
Name	The name of the virtual connection.
Source End NE	The source NE of the virtual connection.
Sink NE	The destination NE of the connection.
Remark	The remark information of the fiber used for creating the connection.
Media Type	The media type of the fiber, including G625, G653, G654 and G655. The default type is G625.
Link Cost	The line cost of the fiber.
Designed Attenuation	The attenuation of the fiber.

Table 5-4 Description of Parameters in the Create the Virtual Connection Dialog Box
(Continued)

Parameter	Description
Length	The length of the fiber.
Link Number	The connection numbering of the fiber.
Associated Link Number	The associated connection numbering of the fiber.
Direction	Includes the following four types: <ul style="list-style-type: none"> ◆ Forward: The connection line has an arrow from the source NE to the sink NE. ◆ Bidirectional: The connection line has bidirectional arrows.
Control Point Format	Includes folding line and curve.
Width	The width of the connection line.
Color	The color of the connection.
Link Type	The line type of the connection. Options are solid line and dashed line.

3. After the setting is completed, click **OK**. The connection line appears between the source and sink NEs.

5.6 Editing an NE

After configuring the NE basic data, you can set the NE attribute (NE name, NE IP address, etc.) and NE icon according to the management requirement.

5.6.1 Setting NE Attributes

After creating NEs, you can modify the NE attributes (NE name, NE IP address, etc.) according to the network running status and management requirement.

- ◆ Modifying the NE name does not influence the running of the NE.
- ◆ Inappropriate IP address settings may cause anomalous communication between the UNM2000 and the NE or between NEs. This type of failures can be eliminated by modifying the NE IP address.

- ◆ When the active management IP (NE IP address) is interrupted, the service will be automatically switched to the standby management IP address, and the system displays the communication anomaly alarm of the active management channel and filters the system communication interruption alarm.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the **Object Tree** or **Physical Topology View** menu, right-click the desired NE and select **Attribute** from the shortcut menu to open the **Attribute Page** pane.
2. Modify the NE attributes as needed.
3. Click  to apply the settings.

5.6.2 Editing Icons

You can modify the size and pattern of the NE icon according to your preference.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the **Physical Topology View**, right-click the NE whose icon is to be edited and select **Edit the Icon** from the shortcut menu to open the **Edit Icon** dialog box.
2. Modify the size and pattern of the NE icon and preview the icon at the lower part of the dialog box.
3. After the completion of the editing icon, click **OK** and the NE icon turns into the pattern you preferred.

5.6.3 Setting the Displayed Content of the Icon

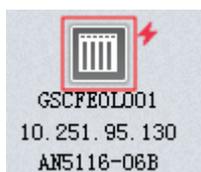
You can set whether to display the NE IP address and type in the NE icon, facilitating NE query in the topograph.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **View**→**Topology View**→**Show NE IP** or **View**→**Topology View**→**Show NE Type**. These sub-menu options will be selected and the NE icon will display its IP address and type.



5.6.4 Tagging the NE

You can make special tags on the NEs to distinguish NEs of difference levels of attention.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select the NE to be marked in the object tree pane of the **Main Topology**.
2. Select **Resource**→**Mark the NE As** from the main menu.
3. In the **Identifier NE** dialog box, enter the tag content and click **OK**.

5.6.5 Querying a Label

The following introduces how to query marked objects.

Procedure

1. Select **Resource**→**Label Query** to open the **Label Query** tab, which displays all the objects marked with labels by default.
2. Do as follows:
 - ▶ **Reset Query:** Click **Reset Query** to open the **Reset Query** dialog box and then set the flag name and applicable object to search for the object with a specific flag.
 - ▶ **Refresh:** Click **Refresh** to refresh the objects in the tab.
 - ▶ **Locate to Object:** Select the desired object and click **Locate to Object** to locate the object in the **Main Topology** tab.
 - ▶ **Delete the Flag:** Select the object and click **Delete the Flag** to delete the flag of the object.

5.6.6 Modify NE Names in a Batch Manner

When the network is of large scale, you can modify the names of the logical domains, NEs and ONUs into easy-to-identify names in a batch manner.

Prerequisite

You have the authority of **Operator Group** or higher authority.

1. Select **Resource**→**Modify NE Names in a Batch Manner** from the main menu to open the **Modify NE Names in a Batch Manner** tab.
2. select **NE** in the left pane of the **Modify NE Names in a Batch Manner** tab to modify the NE names in a batch manner.
 - 1) Click **Set Object Query Conditions** to open the **Set Object Query Condition** dialog box. Then query and modify the object, and click **OK**.
 - 2) Select any of the following three ways to modify NE names in a batch manner.
 - Modify the NE names in a batch manner by importing an Excel file.
 - i) Click **Excel Import** to open the **Import Data** dialog box. Select **Download Template** to download the Excel file template.

- ii) In the downloaded Excel template table, enter the **Logical Address** and **Current Name** of the desired NEs and then enter the **Preview Name** (name displayed after being modified) of the NEs according to the requirements.
- iii) In the **Import Data** dialog box, select **View File** to upload the Excel table edited and then click **OK**.
- Set the modification rules to modify the NE names in a batch manner.
 - i) Select the desired NEs and click **Batch Modify** to open the **Batch Modify** dialog box.
 - ii) Set the batch modification rule in the **Batch Modify** dialog box according to Table 5-5, and then click **OK**.

Table 5-5 Settings in the **Batch Modify** Dialog box

Parameter		Description
Description		The descriptive information of the batch modification rule.
Settings	Prefix characters	The prefix characters of the object to be modified, not involved in incremental value.
	Starting value	The starting value of the object to be modified.
	Suffix characters	The suffix characters of the object to be modified, not involved in incremental value.
	Incremental value	The incremental value of the object to be modified.

- iii) In the **Confirm information** alert box, click **Yes** to confirm the modification.
- iv) In the **Modify NE Names in a Batch Manner** tab, check the new names under the **Preview Name** column. After the confirmation, click **Save**.
- Set the replacement rules to modify the NE names in a batch manner.
 - i) Select the desired NEs and click **Replace in a Batch Manner** to open the **Replace in a Batch Manner** dialog box.
 - ii) Enter the original NE names and new NE names in the **Search Characters** and **Replace with** and textboxes and then click **OK**.
 - iii) In the **Confirm information** alert box, click **Yes** to confirm the replacement.

- iv) In the **Modify NE Names in a Batch Manner** tab, check the new names under the **Preview Name** column. After the confirmation, click **Save**.



Note:

In the left pane of the **Modify NE Names in a Batch Manner** tab, click **Logical Domain** or **ONU** to modify the names of logical domains or ONUs according to Step 2.

5.7 Editing a Fiber Connection

This section introduces how to modify the connection line properties and how to expand / collapse the connection line.

5.7.1 Modifying the Connection Line Properties

You can modify the properties of the connection line between NEs, such as direction, type and width.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Right-click the connection line between NEs and select **Connection Properties** from the shortcut menu to open the **Link Attribute** dialog box.
2. Modify the connection line direction, control point format, width and color as needed.
3. After modification, click **OK**.

5.7.2 Setting the Display Mode of the Connection Line

When there are multiple connection lines between the NEs, you can collapse or expand the lines.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Right-click the connection line between the NEs and set the display mode.
 - ▶ Collapse the connection lines: After Collapse line is selected from the shortcut menu, the collapsed line is added with a + symbol, and the connection line names are hidden.
 - ▶ Expand the lines: After the Expand line is selected from the shortcut menu, the connection lines are expanded, each of which is displayed with its name.

5.8 Browsing the Topology View

In the physical topology view, you can browse the NE topology monitored by the UNM2000 and relevant information.

5.8.1 Checking the Physical Topology View

In the physical topology view, you can check the NE topology monitored by the UNM2000 and relevant information.

Procedure

1. Click the **Main Topology** tab and select **Physical Topology View** from the **Current View** drop-down list.
2. The **Current View** window displays the information of the devices in the topology.

Subsequent Operation

Perform the following operations via the shortcut menus:

- ◆ Set the topology background image.

In the image mode, right-click in the blank area of the physical topology view and select **Set Background Image** or **Use the Default Background Image** from the shortcut menu to set the background image of the physical topology view.

- ◆ Expand / collapse all logical domains.

Right-click in the blank area of the physical topology view and select **Expand All Logic Domains** or **Collapse All Logic Domains**.

- ◆ Hide nodes.

Right-click the NE in the physical topology view and select **Hidden Node** from the shortcut menu. The NE will not appear in the physical topology view.

- ◆ Manage the hidden nodes.

Right-click in the blank area of the physical topology view and select **Manage the Hidden Nodes** to open the **Hide Node Management** dialog box. Then select the nodes to be displayed and click **OK**. The corresponding nodes are displayed in the physical topology view.

- ◆ According to Table 2-2, you can lock, move, zoom in or zoom out the physical topology view by clicking the shortcut icons on the top of the view.

5.8.2 Viewing the Sub-topology View

By checking the sub-topology view, you can view the topology relationship between various physical units of the NE, including the subrack, cards, and ports.

Procedure

1. Right-click the NE in the object tree pane or the physical topology and select **View Topology** to open the **Sub-topology View** tab of the corresponding NE.
2. The **Sub-topology View** tab displays all the information of the NE, including the subrack, card and the connection of the port.

Subsequent Operation

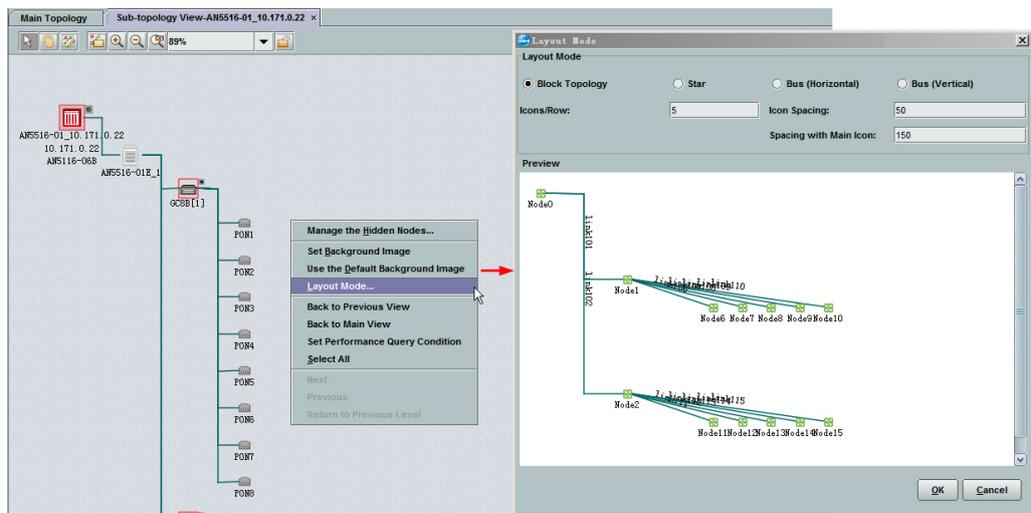
You can perform the following operations in the sub-topology view via the shortcut menus.

◆ Set the background image.

Right-click the blank area in the Sub-topology View tab, and select **Set Background Image** or **Use the Default Background Image** to set the background image of the sub-topology view.

◆ Set the layout style.

- 1) Right-click the blank area in the **Sub-topology View** tab, and select **Layout Mode** to open the **Layout Mode** dialog box.



- 2) Adjust the layout style as required, and preview the adjustment results in the **Preview** pane.

- 3) Click **OK**.

◆ Hide node.

Right-click the node in the sub-topology view, and select **Hidden Node**; then the selected node will not be displayed in the sub-topology view.

◆ Manage the hidden nodes.

Right-click in the blank area of the sub-topology view and select **Manage the Hidden Nodes** to open the **Hide Node Management** dialog box. Then select the nodes to be displayed and click **OK**. Then the corresponding nodes will be displayed in the sub-topology view.

◆ Edit icons.

Right-click the node in the sub-topology view, and select **Edit the Icon**, in the **Edit Icon** dialog box, set the size and style of the node icon, and click **OK**.

- ◆ Table 2-2 describes how to lock, move, zoom in, and zoom out the sub-topology view via the shortcut icons at the top part of sub-topology view.

- ◆ Add splitter

Right-click the PON object in the sub-topology view, and select **Add Splitter**. In the **Add Optical Splitter** dialog box, set parameter of the splitter and then click **OK**.

5.8.3 Viewing the Thumbnail

The **Bird-eye View** displays the thumbnail of the topology. In case the topology window displays only part of the view, you can browse the full view, understand the topology architecture as well as locate the display area of the topology view via **Bird-eye View**.

Procedure

1. On the toolbar above the topology view, click  to open the **Bird-eye View**, which displays the thumbnail of the corresponding topology.



Note:

In the **Bird-eye View** window, only the area within the purplish red frame is displayed. Drag this area to locate the display zone of the topology.

5.8.4 Searching Objects

You can search for and locate the object quickly via the object search functions.

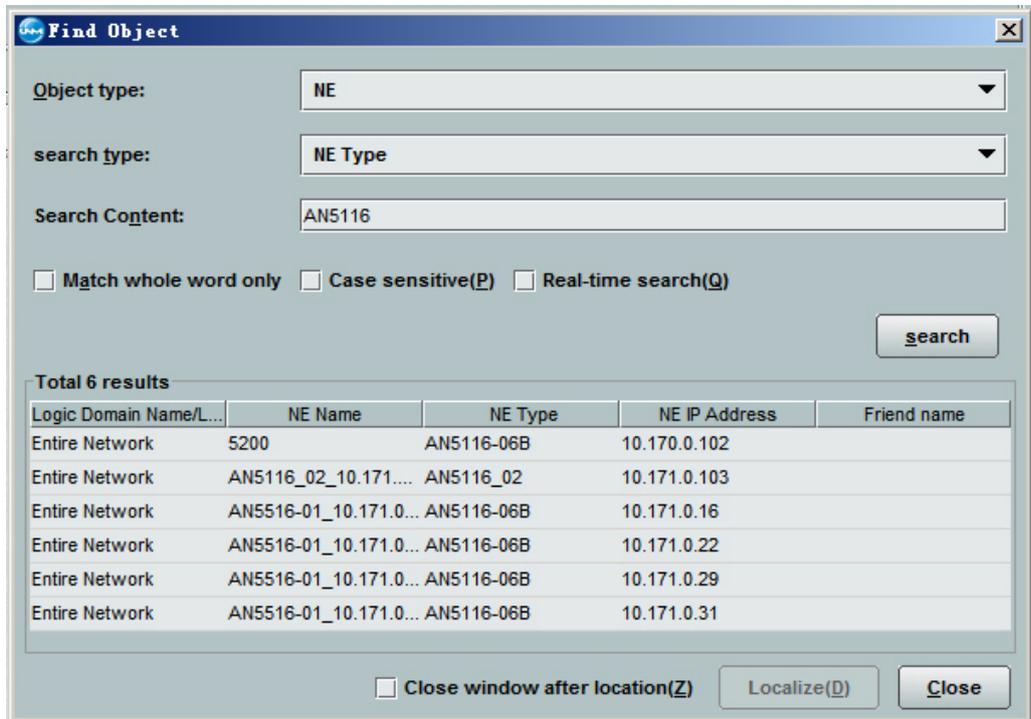
Background Information

The objects include NEs, logical domains and cards.

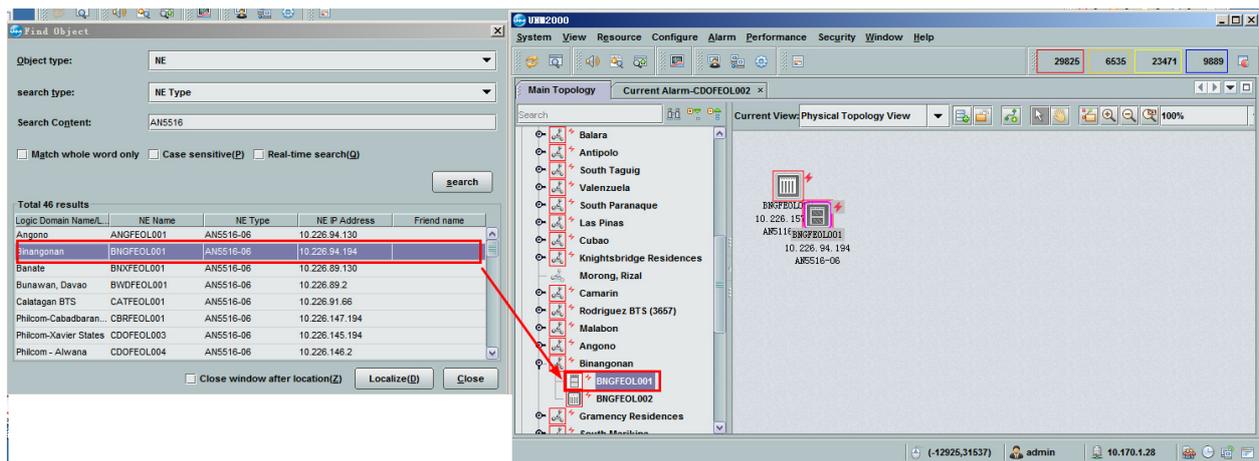
Procedure

1. Select **Resource**→**Search Object** from the main menu.

- In the displayed **Advanced Search** dialog box, set the object type, search type and search content, and then click **Search**.



- Select the desired object in the search result and click **Localize**. The **Main Topology** tab will automatically go to the area that the NE locates in and mark the target object.



5.9 Deleting the Topology

Typically, you need to delete the objects in the network topology before adjusting the topology.

5.9.1 Deleting the Global Logical Domain

When adjusting the network topology, you can delete the subnet logical domain that is no longer needed from the topology view. After a logical domain is deleted, the objects in this logical domain will be moved to its upper-level logical domain.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Right-click in the logical domain of the main topology window and select **Delete** from the shortcut menu.
2. In the displayed dialog box, click **Yes** to apply.

5.9.2 Delete the NE

In case an inappropriate NE is created or changes are made to an NE during network adjustment, you can delete the NE in the UNM2000. Deleting the NE will cause loss of all information related to the NE in the UNM2000; however, it will not influence the running of the device.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Right-click the desired NE and select **Delete** from the shortcut menu.
2. Click **Yes** in the dialog box that appears.



Caution:

Deleting an NE will delete all the related connections simultaneously.

5.9.3 Deleting the Card

In case of network configuration change or modifying the card configuration of the NE is required, you can delete the card from the NE.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Right-click the desired NE in the main topology and select **Open NE Manager** from the shortcut menu to open the **NE Manager** window.
2. Delete the card.
 - ▶ Delete all cards.
 - a) Right-click the subrack in the device tree and select **Delete All Cards** from the shortcut menu.
 - b) In the displayed dialog box, click **Yes** to apply.
 - ▶ Delete a single card
 - a) Right-click the desired card in the device tree and select **Delete Card** from the shortcut menu.
 - b) In the displayed dialog box, click **Yes** to apply.

Subsequent Operation

6.7 describes how to authorize cards and delivery configuration to device.

6 Managing Access NEs

The following introduces how to manage the access NEs using the UNM2000.

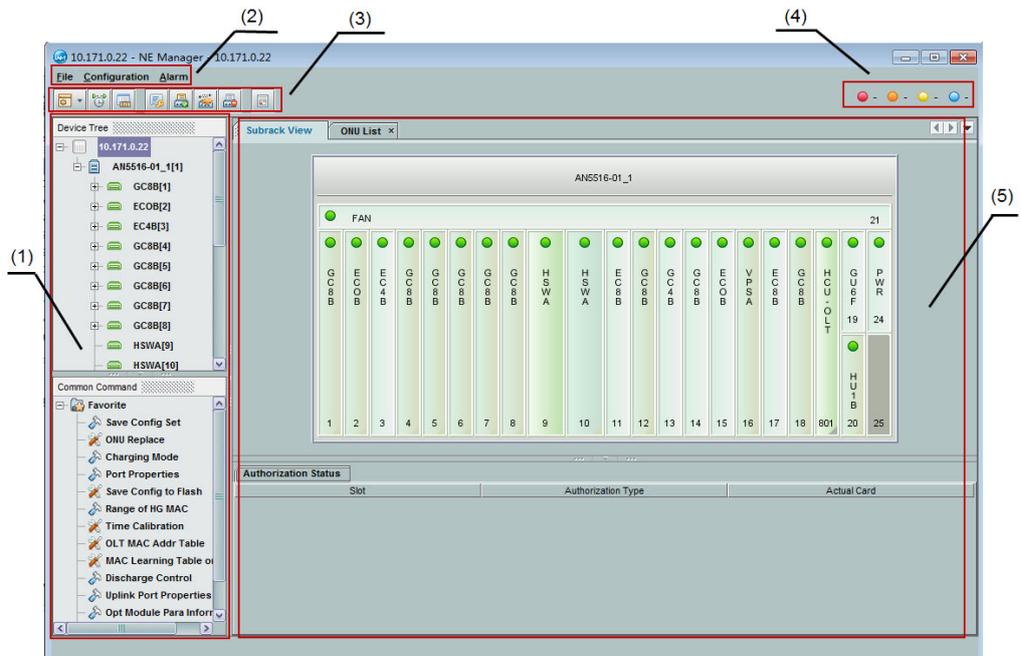
- NE Manager GUI
- Configuring the Local Service
- ONU Query Management
- Authorizing ONUs
- ONU Registration Management
- Rule Tasks of Enabling the ONU Port
- Authorizing Cards
- Synchronizing ONUs Manually
- Obtaining Unauthorized ONUs
- Authorizing ONUs Manually
- OTDR Link Management
- System Maintenance
- Upgrading Cards
- Managing Test Tasks
- Managing NE Automatic Discovery Tasks

6.1 NE Manager GUI

The NE Manager GUI is the main GUI for managing the devices. You can perform operations based on NEs as well as configure, manage and maintain the NEs, cards or ports separately. You can select the corresponding operation object and the corresponding function in the main menu of the NE manager to search for and use the related configuration items of the function.

Access Method

Right-click the object in the object tree of the main topology and select **Open NE Manager** from the shortcut menu to access the **NE Manager GUI**, as shown in Figure 6-1.



- (1) Device tree / Operational tree pane
- (2) Main menu
- (3) Toolbar
- (4) Alarm statistical panel
- (5) Display pane

Figure 6-1 NE Manager GUI

6.2 Configuring the Local Service

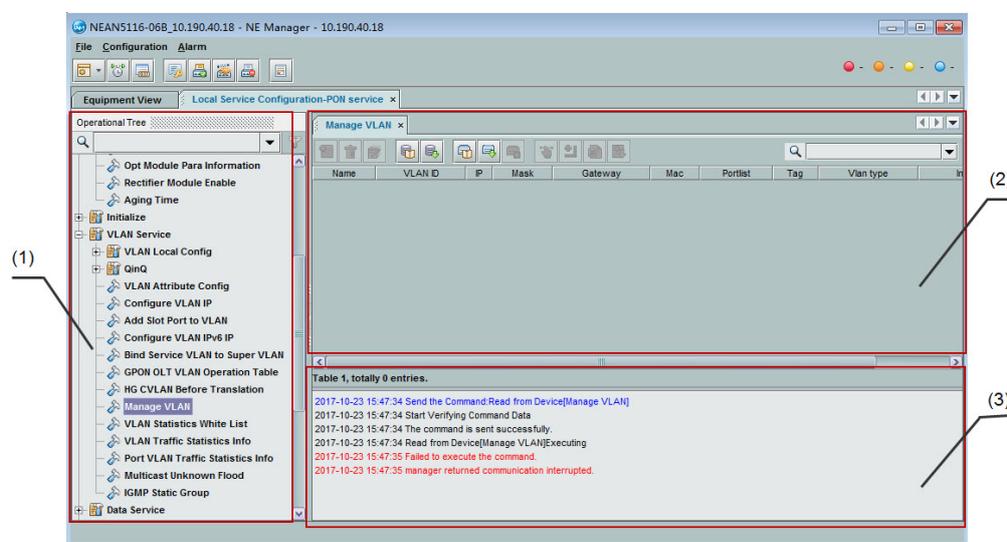
The following introduces the access method and GUI layout of the **Local Service Configuration** function in the NE Manager.

Access Method

1. Click an NE in the **Main Topology** of the UNM2000.
2. Click **Resource**→**Open NE Manager** from the UNM2000 main menu.
3. In the **NE Manager** main menu, select **Configuration**→**Local Service Configuration**→**PON service**.

GUI Introduction

The **Local Service Config** window contains the **Operational Tree**, **Service Configuration Tab** and **Operation Information Displayed Pane**, as shown in Figure 6-2.



(1) Operational tree pane

(2) Service configuration
pane

(3) Operation information
pane

Figure 6-2 Local Service Configuration GUI

6.3 ONU Query Management

By querying the system, slot number, PON port number and logical ID of the ONU, you can quickly acquaint yourself with the distribution of the ONU.

6.3.1 Querying ONUs

With the ONU query function, you can find the desired ONU quickly and view the system, slot number, PON port number and logical ID of the ONU.

The UNM2000 supports querying ONUs by different ONU attributes. It supports both fuzzy match and complete match. The ONU query conditions fall into two parts:

- ◆ General query conditions: Include the logical domain, device type, ONU PON type, device name, friendly name, logical ID, physical ID, OLT IP address, management IP address, and voice service and data service of the ONU.
- ◆ Advanced query conditions: Include slot No., ONU No., ONU password, logical SN password, optical splitter No., optical splitter port No., ONU label, ONU user information and ONU service class.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **Resource**→**Query ONU** from the main menu.
2. Set the query conditions in the **Set ONU Query Conditions** dialog box.
3. After completing the settings, click **OK**. The **Query ONU** tab displays the ONUs meeting the query conditions.

Device Name	Device Type	System	Slot Number	PON Number	ONU Number	Physical Address	ONU Password	Logical ID	Logic SN Password	Alias Name	ONU Serv.	ONU PON
PON[1]-ANS5006-01-A[1]	ANS5006-01-A	ANS5516-01_10.171.0.22	11	1	1	12-13-14-15-16-17						
PON[2]-ANS5006-01-A[1]	ANS5006-01-A	ANS5516-01_10.171.0.22	11	2	1	21-31-41-51-61-71						
PON[3]-ANS5006-07B[1]	ANS5006-07B	ANS5516-01_10.171.0.22	11	3	1	54-46-71-07-49-e0						
PON[1]-ANS5006-04F[1]	ANS5006-04F	ANS5516-01_10.171.0.22	3	1	1	33-11-11-11-11-11						
PON[2]-ANS5006-04P[2]	ANS5006-04P	ANS5516-01_10.171.0.22	3	2	2	77-72-22-22-22-22						
PON[1]-ANS5006-07B[1]	ANS5006-07B	ANS1116_02_10.171.0.103	2	1	1							
PON[1]-ANS5006-20[2]	ANS5006-20	ANS1116_02_10.171.0.103	2	1	2							
PON[1]-ANS5006-07B[2]	ANS5006-07B	ANS1116_02_10.171.0.103	2	1	23			OBLFTTH100966071	321			
PON[1]-ANS5006-20[3]	ANS5006-20	ANS1116_02_10.171.0.103	2	1	33			OBLFTTH100966077	123			
PON[1]-ANS5006-07B[4]	ANS5006-07B	ANS1116_02_10.171.0.103	2	1	44							
PON[1]-ANS5006-07B[5]	ANS5006-07B	ANS1116_02_10.171.0.103	2	1	55			OBLFTTH100966055	123			
PON[4]-ANS5006-04-F[1]	ANS5006-04-F	ANS5516-01_10.171.0.22	13	4	1	FHTT10980840						
PON[1]-ANS5006-01-A[1]	ANS5006-01-A	ANS5516-01_10.171.0.16	5	1	1	00-00-00-00-00-0f						
PON[1]-ANS5006-04-F[1]	ANS5006-04-F	ANS5516-01_10.171.0.31	7	1	1	FHTT00000149						
PON[1]-HG260[2]	HG260	ANS5516-01_10.171.0.31	7	1	2	000000000055						
PON[1]-ANS5006-20[3]	ANS5006-20	ANS5516-01_10.171.0.31	7	1	3	000000000054						
PON[1]-ANS5006-04-F[1]	ANS5006-04-F	ANS5516-01_10.171.0.31	7	1	4	000000000053						

- In the **Query ONU** tab, select one or more entries and click **Service Configuration** at the lower-right corner to go to the **NE Manager** window. Then you can query the service configuration information of the ONU device.

Subsequent Operation

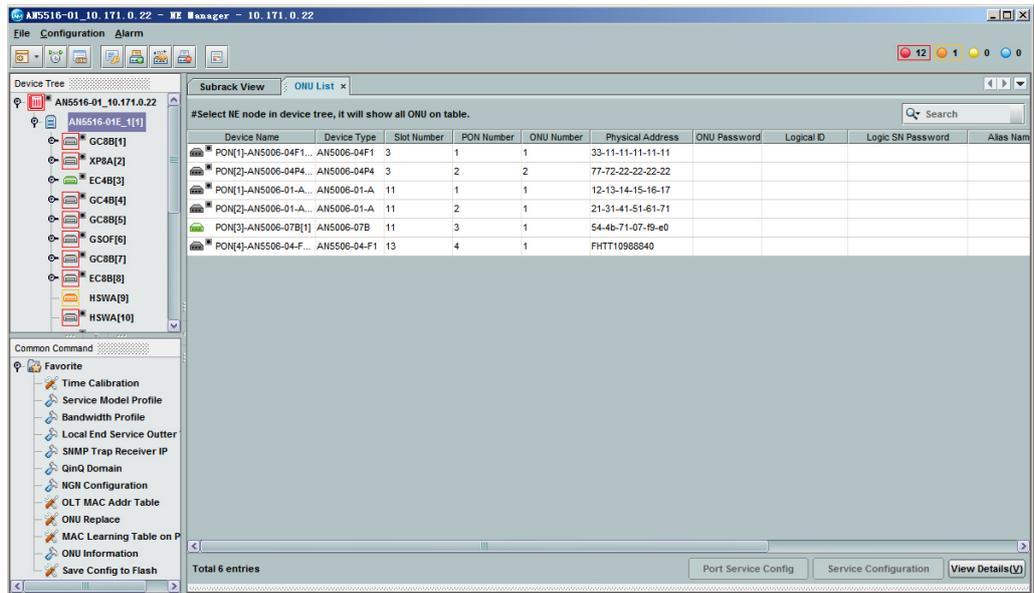
Right-click an ONU, select **Service Configuration**, **Locate to ONU List** or **Service Configuration** from the shortcut menu.

6.3.2 Viewing the ONU List

You can view the ONU details and configure the ONUs.

Procedure

- In the main menu of the NE Manager GUI, select **Configuration**→**ONU List** to open the **ONU List** tab.



2. You can perform the following operations as required.

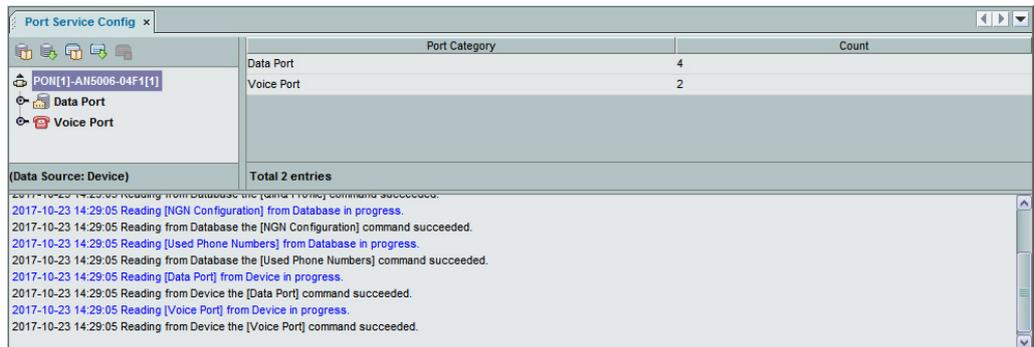


Note:

The following uses **Port Service Config**, **Service Configuration** and **View Details** as an example to introduces how to perform the operations.

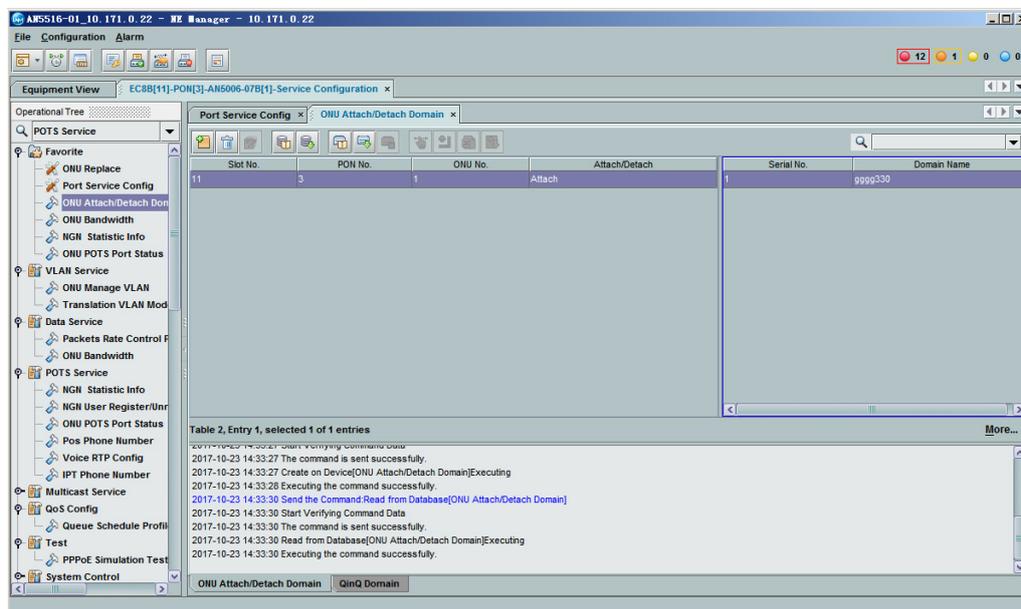
► Port service configuration

In the **ONU List** tab, select a port and click **Port Service Config** to view the port type of the ONU service and the number of ports of different types.



► Service Configuration

In the **ONU List** tab, select a port and click **Service Configuration** to access the designated ONU service configuration tab and perform the service configuration of the ONU.

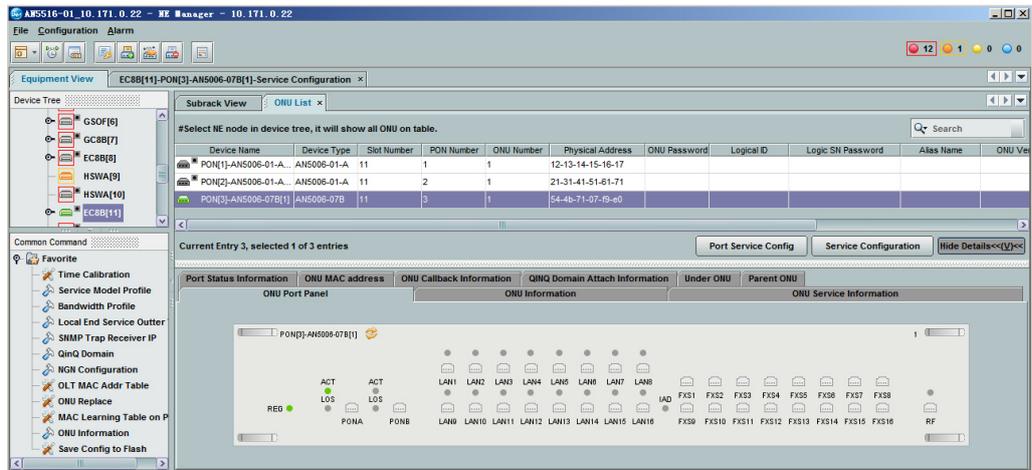


Note:

Right-click the designated configuration option in the **Operational Tree** and select **Favorite** from the shortcut menu to save this option in the favorite folder, so that the user can find it quickly next time. Select **Cancel Favorite** to remove this option from the favorite folder.

► View details

Click **View Details** to view the detailed information of the specified ONU, including **ONU Port Panel**, **ONU Information**, **ONU Service Information**, **Port Status Information**, **ONU MAC address**, **ONU Callback Information**, **QINQ Domain Attach Information**, **Under ONU** and **Parent ONU**.



6.3.3 ONU Query Example

With the ONU query function, you can find the desired ONU quickly and view the system, slot number, PON port number and logical ID of the ONU.

Background

The UNM2000 supports querying ONUs by different ONU attributes. It supports both fuzzy match and complete match. The ONU query conditions fall into two parts:

- ◆ General query conditions: Include the logical domain, type, name, logical ID, physical ID, OLT IP address, voice service and data service of the ONU.
- ◆ Advanced query conditions: Include slot No., ONU No., ONU password, logical SN password, optical splitter No., optical splitter port No., ONU label and ONU user information.

The following introduces how to perform the ONU query via setting different query conditions:

Querying the ONU Object by MAC Address

1. Select **Resource**→**Query ONU** from the main menu.
2. Enter the MAC address of the ONU in the **Physical Address** field.
3. Click **OK**. The **Query ONU** tab displays the ONUs matching the MAC address.

Querying the ONU by ONU Data Service

1. Select **Resource**→**Query ONU** from the main menu.
2. Enter the IP address of the OLT in the **OLT IP** field.
3. Set **Service Condition** to **Data** and specify the values of **CVLAN ID** and **SVLAN ID**.
4. Click **OK**. The **Query ONU** tab displays the ONUs matching the set conditions.

Querying the ONU by ONU Location

1. Select **Resource**→**Query ONU** from the main menu.
2. Select the logical domain where the desired ONU resides from the drop-down list on the right of **Logical Domain**.
3. Click the **Advanced** tab in the **Set ONU Query Conditions** dialog box.
4. Specify **Slot Number** and **ONU Number** in the **Advanced** tab.
5. Click **OK**. The **Query ONU** tab displays the ONUs matching the set conditions.

6.4 Authorizing ONUs

You can perform ONU authorization related operations, including configuring the authentication mode of the PON port or the ONU, authorizing the ONU, replacing the ONU logical identifier and viewing authorized ONU list.

6.4.1 Configuring the ONU Whitelist

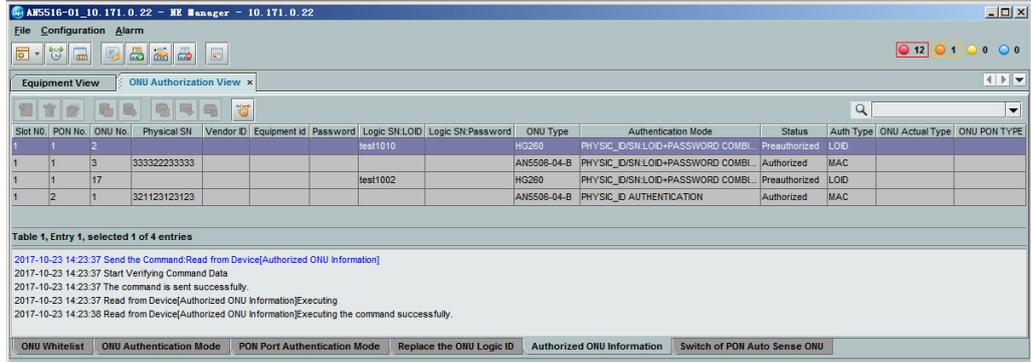
You can query the information of the authorized ONUS and pre-authorize the unauthorized ONUs. The ONUs in the white list can be authorized and service-provisioned, while the ONUs not in the whitelist cannot be authorized or services cannot be provisioned.

Prerequisite

- ◆ You have the authority of **Maintainer Group** or higher authority.
- ◆ The settings of the PON port authorization type of the OLT device have been completed.

Procedure

1. Select **Configuration**→**ONU Authentication**→**ONU Whitelist** in the main menu of the NE manager to open the **ONU Authorization View** tab, displaying the information of the authorized ONUs.



2. Modify the ONU whitelist information: Select an entry, double-click **Slot No.**, **PON No.**, **ONU Type** and **ONU No.** and select the corresponding value from the drop-down list.

Pre-authorizing the ONU

1. Click  in the ONU Authorization View window. In the displayed dialog box, enter the number of ONUs to be pre-authorized and click **OK**.
2. Set the parameters for these ONUs to be pre-authorized according to the PON port authentication mode.
3. Click  in the ONU Authorization View window to deliver the pre-authorization information to the devices.

6.4.2 Managing ONU Authentication Modes

View and modify the authentication mode of the ONU connected to a single PON port, card or device.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **Configuration**→**ONU Authentication**→**ONU Authentication Mode** in the main menu of the NE manager GUI.
2. Select the object in the **Switch Objects (ONU Authentication Mode)** dialog box that appears, click **OK**.
3. To modify the authentication mode of an ONU, double-click the **Authentication Mode** of this ONU and select the desired authentication mode from the drop-down list. Table 6-1 describes the authentication modes.

Table 6-1 Description of the ONU Authentication Modes

Authentication Mode	Description
Physical address authentication	Authenticates the ONU based on its MAC address.
Logical SN authentication: enable the ONU MAC automatic replacement function under the logical SN authentication mode	Turn on this switch to set the ONU that is already authenticated based on its SN to be authenticated based on its MAC address.
Logical SN authentication: disable the ONU MAC automatic replacement function under the logical SN authentication mode	Turn on this switch, and the ONU can be authenticated only based on its SN. It cannot be authenticated based on its MAC address.
GPON password authentication: enable the ONU MAC automatic replacement function under the GPON password authentication mode	Turn on this switch to set the ONU that is already authenticated based on GPON password to be authenticated based on its MAC address.
GPON password authentication: disable the ONU MAC automatic replacement function under the GPON password authentication mode	Turn on this switch, and the ONU can be authenticated only based on GPON password. It cannot be authenticated based on its MAC address.

4. After completing the settings, click  to deliver the configuration to device.

6.4.3 Managing PON Port Authentication Modes

You can view and modify the authentication mode of each PON port. After the authentication mode of the PON port is set, the ONUs under this PON port will be authenticated adopting the set authentication mode.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the NE manager window, select **Configuration** → **ONU Authentication** → **PON Port Authentication Mode** to open the **ONU Authorization View** tab and view all the PON port authentication modes.
2. To modify the authentication mode of a PON port, double-click the **Authentication Mode** of this PON port and select the desired authentication mode from the drop-down list. Table 6-2 describes the authentication modes.

Table 6-2 Description of PON Port Authentication Modes

Authentication Mode	Description
PHYSIC_ID AUTHENTICATION	Authenticates based on the MAC address of the ONU.
PHYSIC_ID +PASSWORD AUTHENTICATION	Authenticates based on the MAC address and password of the ONU.
PASSWORD AUTHENTICATION	Authenticates based on the password of the ONU.
SN:LOID+PASSWORD AUTHENTICATION	Authenticates based on the SN or password of the ONU.
PHYSIC_ID/SN:LOID +PASSWORD COMBINED AUTHENTICATION	Authenticates based on the MAC address, SN or password of the ONU.
NO AUTHENTICATION	No authentication is required for the ONU.
SN:LOID AUTHENTICATION	Authenticates based on the SN of the ONU.

Table 6-2 Description of PON Port Authentication Modes (Continued)

Authentication Mode	Description
PHYSIC_ID/SN:LOID COMBINED AUTHENTICATION	Authenticates based on the MAC address or SN of the ONU.
PHYSIC_ID/PHYSIC PASSWORD COMBINED AUTHENTICATION	Authenticates based on the MAC address or password of the ONU.
Note 1: The ONU password and SN have been set before delivery. You can obtain them by viewing the label attached to the ONU device.	

- After completing the settings, click  to deliver the configuration to device.

6.4.4 Replacing the ONU Logical Identifier

When an ONU using the authentication based on logical ID is faulty, you can replace it with an ONU of the same type. The logical ID of the new ONU is still the logical ID of the faulty ONU. The services on the original ONU will be downloaded to the new ONU, and service configuration is not required.

Procedure

- Select **Configuration** → **ONU Authentication** → **Replace the ONU Logic ID** in the main menu of the NE manager to open the **ONU Authorization View** tab.
- Click  and enter the number of rows to be added in the dialog box that appears. Then click **OK**.
- Set the parameters accordingly.
- After completing the settings, click  to deliver the configuration to device.

6.4.5 Viewing the Authorized ONU Information

You can view the authorized ONU information.

Procedure

1. In the NE manager window, select **Configuration**→**ONU Authentication**→**Authorized ONU Information** from the main menu to display the **Switch Object (Authorized ONU Information)** dialog box.
2. Select the card or port and click **OK** to view the information of the authorized ONU connected to the card or port. The statuses displayed in the Status column in the **ONU Authorization View** tab are described in Table 6-3.

Table 6-3 ONU Authorization Status

Status	Meaning
Authorized	The ONU is connected and the authorization information is sent to the ONU.
Preauthorized	The ONU is disconnected and the authorization information is saved in the network management database.



Caution:

You can select only one card in the Switch Object (Authorized ONU Information) dialog box.

Other Operations

Replace the selected object.

1. In the **ONU Authorization View** tab, click the  button.
2. In the displayed Switch Object (Authorized ONU Information) dialog box, reselect the desired card or PON port and click **OK**. The ONU Authorization View tab displays the information of the authorized ONUs corresponding to the selected object.

6.5 ONU Registration Management

The UNM2000 allows you to query and manage the registration information (registration failure and times of repeated registration) of the ONUs.

6.5.1 ONU RMS Error Information Query

You can query the ONU RMS error information to understand the RMS error reason.

Procedure

1. Select **Resource**→**ONU RMS Error Information Query** from the main menu.
2. In the **Query ONU RMS Error Information** dialog box, set the query conditions.
3. Click **OK**, the **ONU RMS Error Information** displays the ONU RMS error reason.

6.5.2 Querying the ONU Network Access Interception Logs

Through the ONU network interception log, you can check whether multiple ONUs apply to access the network for the same MAC address. This can help the maintenance engineers query the network access failure.

Procedure

1. Select **Resource**→**ONU Network Intercept Log Query** from the main menu.
2. In the **ONU Network Intercept Log Query** dialog box, set the query conditions.
3. Click **OK**. The **ONU Network Intercept Log** will display the ONUs intercepted from network.

6.6 Rule Tasks of Enabling the ONU Port

You can set the automatic enabling and disabling time period of the ONU port, which is convenient for you to remotely manage the time period in which the ONU port can be used.

6.6.1 Viewing Rule Tasks

You can view the port enabling rule tasks already set in the system to understand the object source included in each task, execution result and other related information.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Data Synchronization**→**ONU Port Enable Rule Task** in the left pane to view the existing tasks.
3. Click a task in the left pane to view the task type, execution type, task progress, task status, execution result and start time of the task.
4. Double-click a task in the right pane to view the attributes of the task (including basic information, object source and extended information).

6.6.2 Creating a Rule Task

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Right-click **ONU Port Enable Rule Task** in the left pane or right-click in the right pane and then select **Create** to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

6.6.3 Executing Rule Tasks

The following introduces how to execute the ONU port enabling rule tasks.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Data Synchronization**→**ONU Port Enable Rule Task** in the left pane to view the existing tasks.
3. Right-click the desired rule task and select **Execute Now** from the shortcut menu, or click the task and then click the **Execute Now button** at the bottom of the tab to execute the ONU port enabling rule task.

Other Operations

Right-click a rule task and select **View** from the shortcut menu to view the executed object and execution status in the lower pane.

6.7 Authorizing Cards

Users need to authorize the cards of the equipment.

Procedure

1. In the main menu of the NE manager GUI, select **Configuration**→**Set Card Authentication** to display the **Set Card Authorization** tab to view the authorization information of cards.
2. Configure the card authorization according to the parameter description in Table 6-4 and button description in Table 6-5.

Table 6-4 Parameters

Parameter	Meaning
EMS Configuration	The type of card configured in the UNM2000.
Device Configuration	The type of card stored in the device RAM memory.
Actual Configuration	The type of card physically inserted into the device.

Table 6-5 Buttons

Button	Operation
	Set the EMS configuration as the card configuration.
	Set the device configuration as the card configuration.
	Set the actual configuration as the card configuration.
	Add all cards.
	Delete all cards.
	Hide empty slots.

3. After completing the card authorization, click  to deliver the configuration to the device.

6.8 Synchronizing ONUs Manually

You can manually synchronize the ONU authorization information on the device to the UNM2000.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. In the main menu of the NE Manager GUI, select **Configuration**→**Manual ONU Synchronization**. The Manually synchronizing the ONU succeeded alert box appears at the lower right corner, indicating the ONU authorization information is synchronized to the UNM2000.

6.9 Obtaining Unauthorized ONUs

You can obtain the information of the unauthorized ONUs.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. In the NE manager window, select **Configuration**→**Obtain Unauthorized ONU** to display the **Switch Object(Unauthorized ONU List)** dialog box.
2. Select a desired PON port and click **OK**. The **ONU Authorization View** tab appears, displaying the unauthorized ONUs.

Subsequent Operation

- ◆ Click  to read the information of unauthorized ONUs from the device.
- ◆ Click  to open the **Switch Object (Unauthorized ONU List)** dialog box and reselect the desired PON port.
- ◆ Click , select the range in the **Configure the Selection Range** dialog box and click **OK** to authorize the ONU in the displayed **ONU Authorization** tab.

6.10 Authorizing ONUs Manually

You can authorize the ONUs manually.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. In the NE manager window, select **Configuration**→**Manual ONU Authorization** from the main menu to display the **Manually Authorize ONU** dialog box.
2. Configure the basic information and authentication information, and click **Write Database** or **Write Equipment** or according to Table 6-6 to authorize the ONU manually.

Table 6-6 Buttons

Button	Application
Write database	It is applicable to the situation when the ONU is not physically connected. When the ONU is connected, you can write the configuration in the database into the device through Configuration Synchronization .
Write device	It is applicable to the situation when the ONU is physically connected.

6.11 OTDR Link Management

You can set parameters, perform test, view test status and deliver the test command for the OTDR link via the OTDR link management.

Prerequisite

- ◆ You have the authority of **Maintainer Group** or higher authority.
- ◆ The ODMA, ODMB or ODMC card is configured.

Procedure

1. Select **Configuration**→**OTDR Link Management** from the main menu in the NE manager GUI to open the **OTDR Link Management** dialog box.
2. Parameter configuration (taking the **Port Mapping Relation** as an example).
 - 1) Select **Test Config**→**Port Mapping Relation** from the operation tree in the NE manager.
 - 2) Click  and set the added row in the dialog box that appears and click **OK**.

- 3) Click  to save data to database.
3. Execute the manual test.
 - 1) Select **Test**→**Manual Test** from the operation tree in the NE manager.
 - 2) Set the test parameters in the dialog box that appears and click **OK**.
 - 3) After the test is completed, view the test result in **Export**.

Other Operations

- ◆ View test history:
 - 1) Select **Test**→**Test Records** from the operation tree in the NE manager.
 - 2) Set the query conditions in the dialog box that appears.
 - 3) View the test history data in the **Test Records** dialog box.
- ◆ Read the connection status of the OTDR card / optical link / remote equipment from the equipment. The following takes querying optical link status as an example.
 - 1) Select **Test State**→**Find Optical Link Status** from the operation tree in the NE manager.
 - 2) Click  to read the equipment status.
 - 3) View the results in the **Find Optical Link Status** dialog box.
- ◆ Reboot the equipment and cards. The following takes rebooting the remote equipment as an example.
 - 1) Select **Commands**→**Remote Device Reset** from the operation tree in the NE manager.
 - 2) Set the ODTR slot number and port number in the **Remote Device Reset** tab.
 - 3) Click  to deliver to the equipment.

6.12 System Maintenance

This section introduces the operations of NE system maintenance, including system software upgrade, system software backup, configuration file export, configuration file import, display card upgrade and ONU upgrade.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

The system maintenance operations are similar. The following takes exporting the system configuration files as an example.

1. In the NE manager window, select **Configuration**→**System Maintenance**→**Export Configuration File** to open the **Export Configuration File** dialog box.
2. Set parameters in the dialog box and click **Export Configuration File**. After the **Alert** box prompts the command is successful, you can view the exported configuration file in the FTP server customized in the command parameters.

6.13 Upgrading Cards

You can create tasks for the upgrade operations required for OLT system cards (system cards, service cards, TDM cards, voice cards and OLT firmware) and the ONU system software and firmware so as to implement automatic upgrade.



Caution:

The upgrade of NE software is risky, which may cause interruption of NE services. Please upgrade the NE software in strict accordance with the published upgrade guide of the corresponding NE. It is recommended to contact the FiberHome Technical Engineer for NE software upgrade.

6.13.1 System Software Upgrade Task

You can create the system software upgrade task to upgrade the system software of multiple objects. By selecting the file type of the object source, you can upgrade the core switch card, IDM software, voice interface card, OLT firmware, time card software and OTDR card. The following introduces how to view, create and execute the upgrade task of the system software.

6.13.1.1 Viewing Upgrade Task

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The FTP server is configured. See [Setting the XFTP Server](#).

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**System Software Upgrade Task** in the left pane to view the existing upgrade tasks of the system software.
3. Click a task in the left pane to view the object information and execution status of the task.
4. Double-click a task in the right pane to view the attributes of the task (including basic information, object source and extended information).

6.13.1.2 Creating an Upgrade Task

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The FTP server is set. See [Setting the XFTP Server](#).
- ◆ The upgrade package has been saved in the FTP server directory.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Right-click **System Software Upgrade Task** in the left pane or right-click the right pane and select **Create** from the shortcut menu to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs according to the upgrade requirement, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

Other Operations

If the system software upgrade task does not meet the upgrade requirement or is expired, you can right-click the task to **delete**, **disable**, view or modify the **attribute**.

6.13.1.3 Operation Upgrade Task

This operation applies only to the upgrade tasks whose **Execution Cycle** is **One time**.



Caution:

For the tasks that are automatically executed periodically, do not click **Execute Now**. Wrong operation may interrupt services.

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The FTP server is set. See [Setting the XFTP Server](#).
- ◆ The upgrade package has been saved in the FTP server directory.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**System Software Upgrade Task** in the left pane to view the existing upgrade tasks of the system software.
3. Right-click a task that meets the system software upgrade requirement and select **Execute Now** from the shortcut menu, or select the task and click **Execute Now** at the lower right corner of the tab to execute the system software upgrade task.

Other Operations

Right-click the executed system upgrade task and select **View** in the shortcut menu to view the executed object and execution status in the lower pane.

6.13.2 Tasks of Upgrading ONUs in a Batch Manner

You can select different object sources in the ONU batch upgrade task to upgrade the CPU / IAD software and firmware of the ONU in a batch manner.

6.13.2.1 Viewing Upgrade Task

Prerequisite

The FTP server is configured. See [Setting the XFTP Server](#).

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**ONU Batch Upgrade Task** in the left pane to view the existing ONU batch upgrade tasks.
3. Click a task in the left pane to view the object information and execution status of the task.
4. Double-click a task in the right pane to view the attributes of the task (including basic information, object source and extended information).

6.13.2.2 Creating an Upgrade Task

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The FTP server is set. See [Setting the XFTP Server](#).
- ◆ The upgrade package has been saved in the FTP server directory.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Right-click **ONU Batch Upgrade Task** in the left pane or right-click in the right pane and select **Create** to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs according to the upgrade task requirement, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

Other Operations

If the ONU software upgrade task does not meet the upgrade requirement or is expired, you can right-click the task to **delete**, **disable**, view or modify the **attribute**.

6.13.2.3 Operation Upgrade Task

This operation applies only to the upgrade tasks whose **Execution Cycle** is **One time**.

**Caution:**

For the tasks that are automatically executed periodically, do not click **Execute Now**. Wrong operation may interrupt services.

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The FTP server is set. See [Setting the XFTP Server](#).
- ◆ The upgrade package has been saved in the FTP server directory.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**ONU Batch Upgrade Task** in the left pane to view the existing ONU batch upgrade tasks.
3. Right-click a task that meets the ONU batch upgrade requirement and select **Execute Now** from the shortcut menu, or select the task and click **Execute Now** at the lower right corner of the tab to execute the ONU batch upgrade task.

Other Operations

Right-click the executed ONU batch upgrade task and select **View** from the shortcut menu to view the executed object and execution status in the lower pane.

6.13.3 Tasks of Upgrading System Cards in a Batch Manner

You can upgrade the service cards of multiple objects in a batch manner via the task of upgrading the service cards in a batch manner.

6.13.3.1 Managing Tasks of Upgrading Service Cards in a Batch Manner

Prerequisite

The FTP server is configured. See [Setting the XFTP Server](#).

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**Batch Upgrade of the Service Card** in the left pane to view the existing upgrade task of the system software.
3. Click a task in the left pane to view the object information and execution status of the task.
4. Double-click a task in the right pane to view the attributes of the task (including basic information, object source and extended information).

6.13.3.2 Creating an Upgrade Task

Prerequisite

- ◆ The FTP server is set. See [Setting the XFTP Server](#).
- ◆ The upgrade package has been saved in the FTP server directory.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Right-click **Batch Upgrade Task of the Service Card** in the left pane or right-click the right pane and select **Create** to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs according to the service card upgrade task requirement, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

Other Operations

If the service card upgrade task does not meet the upgrade requirement or is expired, you can right-click the task to **delete**, **disable**, view or modify the **attribute**.

6.13.3.3 Operation Upgrade Task

This operation applies only to the upgrade tasks whose **Execution Cycle** is **One time**.



Caution:

For the tasks that are automatically executed periodically, do not click **Execute Now**. Wrong operation may interrupt services.

Prerequisite

- ◆ The FTP server is set. See [Setting the XFTP Server](#).
- ◆ The upgrade package has been saved in the FTP server directory.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**Batch Upgrade of the Service Card** in the left pane to view the existing upgrade task of the system software.
3. Right-click a task that meets the requirement on service card batch upgrade and select **Execute Now** from the shortcut menu, or select the task and click **Execute Now** at the lower right corner of the tab to execute the system software upgrade task.

Other Operations

Right-click the executed service card batch upgrade task and select **View** from the shortcut menu to view the executed object and execution status in the lower pane.

6.13.4 System Software Upgrade Task

You can upgrade cards and ONUs in a batch manner using the system software task.

6.13.4.1 Viewing Upgrade Task

Prerequisite

The FTP server is set. See [Setting the XFTP Server](#).

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**System Software Upgrade Task** in the left pane to view the existing upgrade task of the system software.
3. Click a task in the left pane to view the object information and execution status of the task.
4. Double-click a task in the right pane to view the attributes of the task (including basic information, object source and extended information).

6.13.4.2 Creating an Upgrade Task

Prerequisite

The FTP server is set. See [Setting the XFTP Server](#).

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.

2. Right-click **System Software Upgrade Task** in the left pane or right-click in the right pane and select **Create** to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs according to the system software upgrade task requirement, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

Other Operations

If the system software upgrade task does not meet the upgrade requirement or is expired, you can right-click the task and **delete**, **disable**, view or modify the **attribute**.

6.13.4.3 Operation Upgrade Task

Prerequisite

- ◆ The FTP server is set. See [Setting the XFTP Server](#).
- ◆ The upgrade package has been saved in the FTP server directory.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**System Software Upgrade Task** in the left pane to view the existing upgrade task of the system software.
3. Right-click a task that meet the system software upgrade requirement and select **Execute Now** from the shortcut menu, or select the task and click **Execute Now** at the lower right corner of the tab to execute the system software upgrade task.

Other Operations

Right-click the executed system upgrade task and select **View** in the shortcut menu to view the executed object and execution status in the lower pane.

6.14 Managing Test Tasks

The test task includes the POTS port external / internal line task and the VoIP pinging test task.

6.14.1 Managing POTS Port Internal / External Line Test Tasks

Via the task of the POTS port internal / external line test, you can detect whether the POTS port of the ONU is normal.

6.14.1.1 Viewing Test Tasks

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Test Task**→**POTS Port Inter & Outer Line Test Task** in the left pane to view the current tasks of POTS port internal / external line test.
3. Click a task in the left pane to view the object information and execution status of the task.
4. Double-click a task in the right pane to view the attributes of the task (including basic information, object source and extended information).

6.14.1.2 Creating a Test Task

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Right-click **POTS Port Inner & Outer Line Test Task** in the left pane or right-click in the right pane and then select **Create** to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

Other Operations

When the POTS port internal / external line test tasks do not meet the upgrade or will expire, you can right-click the task to select the operations, such as **Delete**, **Disable**, and viewing and modifying attributes.

6.14.1.3 Executing a Test Task

Prerequisite

You have the authority of **Operator Group** or higher authority.



Caution:

The execution of the test task will influence the use of services and therefore it is recommended to execute the test task when service traffic is at a relatively low volume.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Test Task**→**POTS Port Inter & Outer Line Test Task** in the left pane to view the current tasks of POTS port internal / external line test.
3. Right-click the desired test task and select **Execute Now** from the shortcut menu, or click the task and then click the **Execute Now button** at the bottom of the tab to execute the POTS port internal / external test task.

Other Operations

Right-click a test task and select **View** from the shortcut menu to view the executed object and execution status in the lower pane.

6.14.2 Managing VOIP PING Tasks

The VoIP PING task can be used to detect the MGC IP address corresponding to the ONU, helping isolate failures.

6.14.2.1 Viewing Tasks

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.

2. Select **Test Task**→**VOIP PING Task** to view the existing VOIP PING tasks.
3. Click a task in the left pane to view the object information and execution status of the task.
4. Double-click a task in the right pane to view the attributes of the task (including basic information, object source and extended information).

6.14.2.2 Creating a Task

The VOIP PING test is used to check whether the network management system can ping the IP address of the MGC related to the ONU. This function is used to isolate the fault in failure detection.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Right-click **VOIP PING Task** in the left pane or right-click in the right pane and select **Create** to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required. Table 6-7 describes the **Parameter Settings** in the **Extend information** tab. Then, click **OK**. The new task will appear in the task list.

Table 6-7 Description of VOIP PING Parameters

Parameter	Description
-n	Sends the ECHO data packets with the number specified by COUNT
-w	The timeout interval, unit: ms
-l	Sends the ECHO data packets with the assigned traffic
-i	Sets the TTL field to the assigned value
-v	Sets the TOS field to the assigned value
-r	Assigns the number of routes to be passed through in the Recorded Route field
-s	The time stamp of the hop number assigned by the COUNT
-t	Pings the object computer continuously
-a	Resolutes the address into the NetBios name of the computer

Table 6-7 Description of VOIP PING Parameters (Continued)

Parameter	Description
-f	If the Not-Section flag is transmitted in a packet, this packet will not be sectioned by the gateways at the route
-j	Sets TTL to the given value
-k	Uses the computer list assigned by computer-list to list the route packet



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

Other Operations

When the VOIP PING test tasks do not meet the upgrade requirements or is expired, you can right-click the task to **delete**, **disable**, view or modify the **attribute**.

6.14.2.3 Running Tasks

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Test Task**→**VOIP PING Task** to view the existing VOIP PING tasks.
3. Right-click a test task and select **Execute Now** from the shortcut menu, or select the task and click **Execute Now** at the lower right corner of the tab to execute the VOIP PING test task.

Other Operations

Right-click a test task and select **View** from the shortcut menu to view the executed object and execution status in the lower pane.

6.15 Managing NE Automatic Discovery Tasks

You can set the NE automatic discovery task to automatically discover the NEs in the specified IP range and then synchronize the NEs to the UNM2000 so as to automatically create NEs in the UNM2000.

6.15.1 Viewing NE Automatic Discovery Tasks

You can set the NEs which can be discovered automatically within a specified IP address range as desired.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Resource**→**Auto NE Discovery** or select **System**→**Policy Task Management**→**Data Synchronization**→**Auto Detect NE Task** to view the existing auto NE discovery tasks.
2. Right-click a task, click **Attribute** from the shortcut menu. You can view the related information of this task, such as execution cycle, execution time, IP address range.

Subsequent Operation

- ◆ Right-click a corresponding task and select **Execute Now**, or select the task and click **Execute Now** at the lower right corner of the tab to execute the NE auto discovery task.
- ◆ Right-click an NE that is discovered automatically in the right pane, and select **Create Selected NE** or **Create All** to automatically save the NE data in the UNM2000.

6.15.2 Creating an NE Automatic Discovery Task

When changes are made to IP segments managed by the UNM2000 and new NEs of devices are added in these IP segment, you can create NE automatic discovery tasks to enable the UNM2000 to manage the devices in the entire network.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Resource**→**Auto Detect NE Task** from the main menu to open the **Auto Detect NE Task** dialog box.
2. Click the **Create** button at the bottom of the tab, or right-click **Auto Detect NE Task** in the left pane, or right-click in the right pane and select **Create** from the shortcut menu to open **Create Auto Detect NE Task** dialog box.
3. Set the parameters in the **Basic information** and **Extend information** tabs as required, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

4. Click the desired NE automatic discovery task in the left pane to view the IP address, NE type and status.

7 Alarm Management

The alarm is the main information source for knowing about the operating condition of the equipment and the fault isolation. You need to monitor and handle alarms in a timely manner, so as to ensure the normal operation of the network.

- Basic Concepts
- Setting Alarm Related Parameters
- Managing Alarm / Event Templates
- Synchronizing Alarms
- Monitoring Network Alarms
- Handling Alarms
- Customizing Alarms
- Alarm / Event Remote Notification
- Managing the Alarm / Event Data
- Alarm Logs
- Managing Alarm Frequency Analysis Rules

7.1 Basic Concepts

This section introduces the basic concepts related to alarm management, including alarm browsing, alarm notification mode, alarm level, alarm classification, current alarm, alarm history, alarm and event, alarm statistics and alarm saving, facilitating you in alarm processing.

Alarm Browsing

By browsing alarms, the network maintainer can understand the running status of the network devices and the UNM2000 timely. The alarm browsing operation includes browsing the current alarms or alarm history of the UNM2000, NEs, cards and services, as well as synchronizing, verifying and confirming the alarms.

- ◆ Browsing alarms: You can browse the alarms of the devices or services in the UNM2000 to understand the running status of the network or device.
 - ▶ Browsing current alarms: Browses the current alarms of all levels of the entire network.
 - ▶ Browsing the alarms of the specified NE: By selecting the device in the main topology, you can browse the current alarms of the selected device quickly.
 - ▶ Browsing the alarm log: By browsing the alarms which meet the query condition, you can browse the required alarm information quickly.
- ◆ Confirming alarms: If an alarm is confirmed, the alarm is processed. You can select the desired alarm and confirm it in the current alarm window.
 - ▶ Manual confirmation: You can select the desired alarm and confirm it in the current alarm window.
 - ▶ Automatic confirmation: You need to enable the alarm automatic confirmation function. After an alarm is processed, the UNM2000 will clear the alarm immediately or at the specified time according to the settings.
- ◆ Confirming and clearing alarms: You can select the desired alarm to confirm it and clear it at the same time in the current alarm window. This alarm will be saved in the alarm history database.

- ◆ Synchronizing alarms: In case the UNM2000 restores from the communication interruption with the device or the UNM2000 restarts, you need to synchronize the alarm to ensure consistent alarms in the UNM2000 and on the device. The UNM2000 will check whether the alarms in the UNM2000 database and on the NE device are consistent. If not, the alarms on the NE device will be synchronized to the UNM2000 database and overwrite the alarms in the database.
- ◆ Checking alarms: Checks whether the current alarm at the UNM2000 side exists in the current alarms at the NE side. If yes, the alarms at the UNM2000 side keep unchanged. If not, the UNM2000 clears the alarm.
- ◆ Refreshing alarms: Obtains the latest alarms from the UNM2000 alarm database and displays them at the client.
- ◆ Clearing alarms: Clears the alarms from the current alarm database of the UNM2000 and from the NE and saves them to the alarm history database.
- ◆ Filtering alarms: You can set the filter conditions to filter the alarm not focused in the alarm browsing window.
- ◆ Alarm remarks: Adds remarks for the alarms already processed, convenient for alarm management.

Alarm Notification Mode

Obtaining the alarm information timely is very important to alarm processing and network maintenance. The UNM2000 provides multiple ways of alarm notification.

- ◆ Alarm indicator color: The UNM2000 uses the changes of the alarm indicator LEDs to help you quickly locate the alarmed object. By default, the alarm indicator of the UNM2000 indicates critical alarms in red, major alarms in orange, minor alarms in yellow and alert alarms in blue. You can customize the colors of the alarm indicator to indicate alarms of different levels.
- ◆ Alarm sound: The UNM2000 client provides the audible and visual alarm when it is connected to the alarm box device. You can determine the level of the reported alarm according to the indicator color and sound of the alarm box. Upon the reporting of a new alarm, the UNM2000 immediately triggers the alarm box to play the alarm sound and the corresponding alarm indicator flickers.

- ◆ Remote alarm notification: The UNM2000 provides the following two ways of remote alarm notification for users who are not on site.
 - ▶ Sends alarms via email automatically to the specified users.
 - ▶ Sends alarms via SMS automatically to the specified users.

Alarm Level

Alarm levels are used to identify the severity, importance and urgency of the alarms. The UNM2000 classifies the alarms into the following four levels in terms of severity: critical alarms, major alarms, minor alarms and warning alarms. The alarms of different levels have different meanings and should be processed differently, as shown in Table 7-1.

Table 7-1 Description and Handling Method of Alarms of Different Levels

Alarm Level	Meaning	Handling Method
Critical alarm	Indicates the alarms on the failures that are global or may cause corruption of NEs and services.	Handled urgently.
Major alarm	Indicates the alarms on the failures of cards or services in a certain range.	Processed timely.
Minor alarm	Indicates the alarms on failures of general cards or services.	Alarm reason should be found timely to eliminate the failure.
Warning alarm	Indicates the alarms that may influence the service quality of devices or resources other than system performance and service. Some of them are just information prompting the devices are back to normal.	Handled accordingly.

Alarm status

The alarm status includes alarm confirmation and clearance. Different handling methods should be adopted for alarms in different status. Alarms can be divided into the following different statuses according to whether the alarm has been confirmed or cleared.

- ◆ Unconfirmed and uncleared
- ◆ Confirmed but uncleared
- ◆ Unconfirmed but cleared

- ◆ Confirmed and cleared

Alarm Classification

Alarms can be divided into NE alarms and UNM2000 alarms according to their occurrence locations.

- ◆ NE alarms: Indicates the alarms on the failures of NEs.
- ◆ UNM2000 alarms: Indicates the alarms on the failures of the UNM2000 environment.

Current Alarm and Alarm History

Alarms are divided into current alarm and alarm history. Their respective meanings are as follows:

- ◆ Current alarms: Indicates the NE alarms saved in the current alarm database of the core switch card or the UNM2000 alarms saved in the current alarm database of the UNM2000.
- ◆ Alarm history: Indicates the NE alarms cleared and then saved in the alarm history database of the core switch card or the UNM2000 alarms confirmed by users, cleared from the current alarm database and then saved to the alarm history database.

Alarm Statistics

Alarm statistics indicates gathering the alarm data according to your desired conditions. The alarm statistics are convenient for you to analyze the running status of the device.

Alarm Saving

If the alarm history data stored in the UNM2000 exceeds the threshold, the UNM2000 operation will be influenced. The alarm data saving function can save the alarm history data in the UNM2000 as files to the designated file folder, so as to improve the UNM2000 operation performance. The UNM2000 supports manual saving and overflow saving.

- ◆ **Overflow saving:** You can set the maximum alarm saving capacity and the UNM2000 will regularly check the alarm history data. When the alarm history data reach the preset capacity, the UNM2000 will save the data to a specified file to decrease its load.
- ◆ **Save Manually:** You can save the alarm history data in the UNM2000 to a specified file folder manually at anytime. You can set the manual saving period. When the alarm history data saved in the database reach the preset time period, the UNM2000 will save the data to a designated file folder.

Alarm and Event

When detecting the status changes of the managed objects, the UNM2000 presents them via alarms or events.

- ◆ The alarm indicates the notification generated when the system detects a failure.
- ◆ The event indicates any changes occurring on the managed objects.

7.2 Setting Alarm Related Parameters

Set the alarm-related parameters, including the alarm reporting rules, alarm filter rules, alarm history definition and other local settings.

7.2.1 Managing Alarm Reporting Rules

You can set the alarm reporting rules to automatically report the alarms that you concern most. These alarms will be automatically reported to the UNM2000 upon their occurrence. For the unnecessary alarms, you can set not to report them so as to minimize the influence on the UNM2000 performance caused by a large number of alarms.

7.2.1.1 Viewing Alarm Reporting Rules

You can view whether the existing alarm reporting rules meet the requirements for current network maintenance.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Alarm** → **Setting Alarm Reporting Settings** from the main menu to display the **Alarm Reporting Setting** tab.
2. Select **Report Rule** in the left pane, and view the existing reporting rules in the right pane.
3. Click  before **Report Rule**, select the corresponding alarm reporting rule, and then view the related information of the rule in the right pane.

7.2.1.2 Setting Alarm Reporting Rules

When the existing alarm reporting rules cannot meet the requirements for device maintenance, you can create alarm reporting rules as described below.

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The desired alarm reporting rule has been planned according to the maintenance requirement.

Procedure

1. Select **Alarm** → **Setting Alarm Reporting Settings** from the main menu to display the **Alarm Reporting Setting** tab.
2. Select one of the following access methods to open the **Create Alarm Report Rule** dialog box.

No.	Access Method
1	Click Report Rule in the left pane, and click Create in the right pane.
2	Select Report Rule in the left pane, right-click in the blank area in the right pane and select Create from the shortcut menu.
3	Right-click Report Rule in the left pane and select Create from the shortcut menu.

3. In the **Create Alarm Report Rule** dialog box, set the alarm reporting rules as required.



Note:

- ◆ Click **Copy from Other Rule**, select the reporting rules in the **Select the Report Rule** dialog box, and copy the related information of the selected reporting rule. This can improve the setting efficiency.
 - ◆ If the continuous reporting mode is enabled, the alarms meeting the reporting rules will be reported again after the set time interval expires.
-

4. Click **OK**.

Other Operations

Right-click the alarm reporting rule entry in the right pane and select the **Delete**, **Refresh**, **Enable / Disable**, **Print**, **Copy Cell** or **Export** operation.

7.2.2 Managing Alarm Filter Rules

The alarm filter rules are used to filter some NE alarms so that you can focus on important alarms, improving the failure solving efficiency. After the alarm filter rules are set, the filtered alarms will neither be saved into the alarm database nor be displayed.

7.2.2.1 Setting the Project Alarm Filtering

During the project installation, commissioning, cutover and maintenance, massive alarms may occur, which will distract maintainers from significant alarms. You can automatically filter all the reported alarms and alarm clearance information during the project construction by setting the project alarm filtering. The filtered alarms are neither saved in the database nor displayed in the client terminal.

Procedure

1. Select **Alarm**→**Shield Project Alarms** in the main menu to open the **Shield Project Alarms** tab.
2. Click the **Added Filtered NE of Project Alarm** at the lower right corner of the tab or right-click in the blank area of the tab to select **Added Filtered NE of Project Alarm**.
3. In the **Please select the need to generate masking rules NE** dialog box, select the NE object to set to the project construction status, and click **OK**.
4. Refer to Table 7-2 to set the relevant project alarm filtering parameters.

Table 7-2 Parameter Descriptions of Project Alarm Filtering

Parameter	Description
Start Time	The start time of filtering the alarms of the selected NE object; the default time is the current system time.
Auto Stopped	Select this item and the filtering end time will become valid, otherwise the End Time is unavailable.
End Time	After the end time has expired, the alarm filtering of the selected NE will be stopped. The default value is the current time plus 24 hours.
End Now	The alarm filtering of the selected NE will be stopped as soon as this option is selected.

5. After completing the settings, click **Save All** at the lower right corner of the tab, or simply right-click the blank area in the tab and select **Save All** to save the project alarm filtering settings.

Other Operations

Delete the project alarm filtering.

1. Select the project alarm filter entry, and select **Delete** at the lower right corner of the tab, or simply right-click the project alarm filter entry to select **Delete**.
2. In the displayed **Confirm to Delete** alert box, click **Yes**.

7.2.2.2 Viewing Alarm Filter Rules

You can view whether the existing alarm filter rules meet the maintenance requirements of the UNM2000 and the NE.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Alarm**→**Setting**→**Alarm Shield Rule Management** from the main menu to open the **Alarm Shield Rule Management** tab.
2. Select **View Current Alarm Shield Rule** in the left pane, and view the existing current alarm shield rules in the right pane.
3. Click before **Current Alarm Shield Rule**, select the corresponding alarm filter rule, and view the related information of the rule in the right pane.

7.2.2.3 Setting Alarm Filter Rules

When the existing alarm filter rules cannot meet the management and maintenance requirements of the UNM2000 and NEs, you can create alarm filter rules as described below.

Prerequisite

- ◆ You have the authority of **Operator Group** or higher authority.
- ◆ The desired alarm filter rule has been planned according to the maintenance requirement.

Procedure

1. Select **Alarm**→**Setting**→**Alarm Shield Rule Management** from the main menu to open the **Alarm Shield Rule Management** tab.
2. Select one of the following access methods to open the **Create Alarm Report Rule** dialog box.

No.	Access Method
1	Click Alarm Shield Rule Management in the left pane and click Create in the right pane.
2	Click Alarm Shield Rule Management in the left pane, right-click in the right pane and select Create from the shortcut menu.
3	Right-click Alarm Shield Rule Management in the left pane and select Create from the shortcut menu.

3. In the **Create Current Alarm Shield Rule** dialog box, set the alarm filter rule according to the planning.



Note:

Click **Copy from Other Rule** to open the **Select Shield Rule** dialog box and select the desired filter rule to copy its rule settings. This can improve the setting efficiency.

4. Click **OK**.

Other Operations

Right-click the alarm reporting rule entry in the right pane and select the **Delete**, **Refresh**, **Enable / Disable**, **Print**, **Copy Cell** or **Export** operation.

7.2.2.4 Setting Northbound Interface Filter Rules

When some alarms need not be reported to the third-party EMS through the northbound interface, you can set northbound interface alarm filter rules to filter these alarms so as to improve the alarm processing efficiency.

Background Information

- ◆ The filter rules do not apply to the alarms already reported. They are only applicable to the matching alarms reported after the filter rules are set.
- ◆ The filtered alarms will not be reported to the northbound interface.

Procedure

1. Select **Alarm**→**Setting****Northbound Interface Shield Rule Management** from the main menu to open the **Northbound Interface File Rule Management** tab.
2. Click **Create Rule**.
3. In the displayed **Northbound Interface Filter Rule** dialog box, set the filter rules.
4. Click **OK** to add a northbound interface alarm filter rule and filter the current alarm in specific condition. You can view the added northbound interface alarm filter rule in the **Northbound Interface File Rule Management** tab.

Other Operations

In the **Filter Rule of North** tab, right-click a northbound interface alarm rule and select the menus from the shortcut menu to perform the corresponding operations, including **Modify Rule**, **Delete Rule**, **Disable Rule**, **Copy Rule**, etc.

7.2.2.5 Setting Alarm Flashing Rules

When some alarms need not be reported, you can set alarm flashing rules to filter these alarms so as to improve the alarm processing efficiency.

Procedure

1. Select **Alarm**→**Setting**→**Alarm Vibration Shield Rule Management** from the main menu to open the **Alarm Vibration Shield Rule Management** tab.
2. Click **Vibration** in the left pane.
3. Click **Create** to create a rule.
4. In the **Create Current Alarm Vibration Shield Rule** dialog box, set the alarm filter rule.
5. Click **OK** to add an alarm filter rule and filter the current alarm in specific condition. The newly added alarm filter rules can be viewed in the **Alarm Vibration Shield Rule Management** tab.

Other Operations

In the **Alarm Vibration Shield Rule Management** tab, right-click an alarm filter rule and select the operations, such as **Delete** and **Copy**.

7.2.3 Setting the Audible Alarms

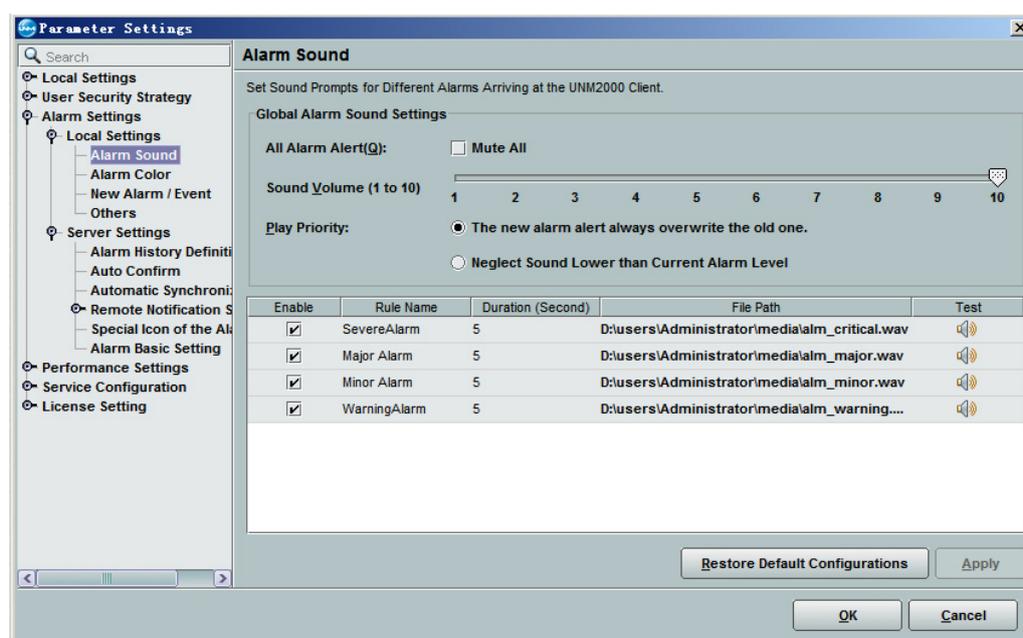
You can set different sounds for alarms of different levels and set the play priority of the alarm sounds. When an alarm occurs, the loudspeaker on the computer running the client will play the corresponding sound to notify of the reported alarm of the specific level.

Background Information

This setting is only applicable to the current client end.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Alarm settings**→**Local Setting**→**Alarm Sound** in the left pane to open the dialog box.



3. Set the parameters according to your needs and then click **Apply**. The settings will take effect immediately.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the default values.

7.2.4 Enabling / Disabling the Audio Alarm

The following introduces how to enable / disable the audio alarm. This operation is only valid to the current client end. The UNM2000 client will play different alarm sounds for alarms of different levels upon their occurrence in the UNM2000 or NE. You can select whether to enable the audio alarm in the UNM2000.

Background Information

This setting is only applicable to the current client end.

Procedure

- ◆ Disable the audio alarm.
Click  to change it to .
- ◆ Enable the audio alarm.
Click  to change it to .



Note:

For other setting items related to the audio alarm, see [Setting the Audible Alarms](#).

7.2.5 Setting the Display Modes of New Alarms / Events

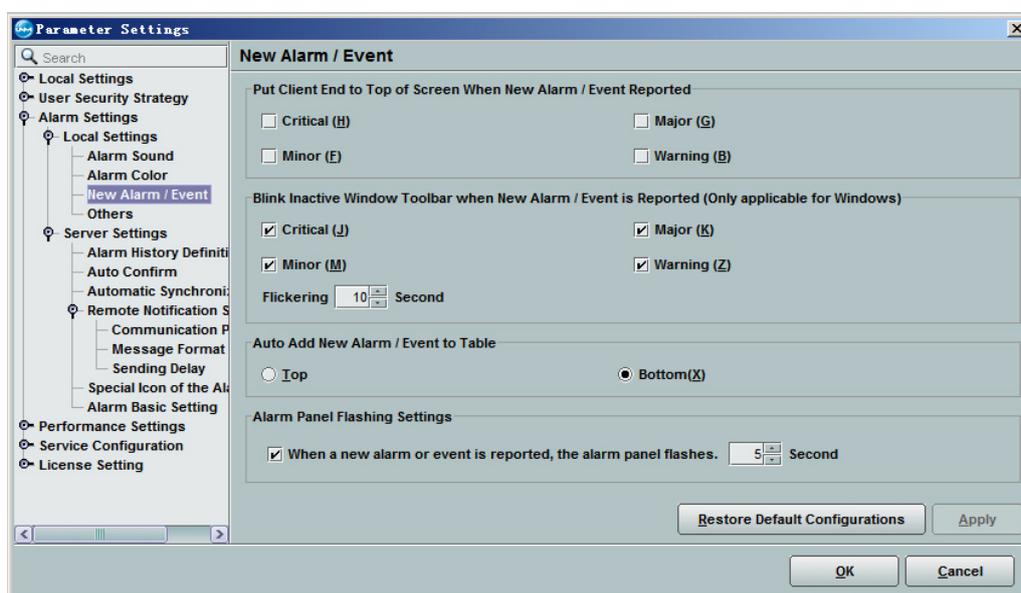
You can set the display modes of new alarms / events as required.

Background Information

This setting is only applicable to the current client end.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Alarm settings**→**Local Setting**→**New Alarm / Event** in the left pane to open the dialog box.



3. Set the parameters according to your needs and then click **Apply**. The settings will take effect immediately.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the default values.

7.2.6 Setting the Alarm Color

You can set different colors for alarms of different levels, which is convenient for you to browse the focused alarms.

Background Information

- ◆ After the colors corresponding to alarms of different levels are set, the alarm icons in the topology view, alarm entries queried and alarm indicators on the alarm bulletin board will appear in the set colors.
- ◆ The UNM2000 provides four colors corresponding to four alarm levels. Critical alarms: ; major alarms: ; minor alarms: ; prompt alarms:  above the list.
- ◆ The GUI display settings are applicable to all users at any client.

Procedure

1. Select **System**→**Parameter Settings**→**Alarm Settings**→**Local Alarm**→**Alarm Color** dialog box.
2. In the **Set a Color for the Alarm Level** combo box, click  on the right to select the desired color for each alarm level.
3. In the **Set the Background Color of the List Corresponding to the Alarm** combo box, click  on the right to select the desired colors for different confirmation statuses.
4. Click **Apply**→**OK** to apply the settings.

7.2.7 Setting Other Items of the Local Alarms

Other local alarm settings include the alarm monitoring template, maximum number of startup templates as well as whether to enable alarm automatic reporting upon client startup.

Background Information

This setting is only applicable to the current client end.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Alarm settings**→**Local Setting**→**Others** in the left pane to open the dialog box.

3. Set the parameters according to your needs and then click **Apply**. The settings will take effect immediately.
4. Select **Alarm**→**Alarm Query Template Management** from the main menu to view the parameters already set.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the default values.

7.2.8 Setting the Definition of the Alarm History

You can set the delay for switching current alarms to the alarm history as required.

Background Information

When the current alarms have been confirmed and cleared, they will be switched to the alarm history after the set delay time.

Procedure

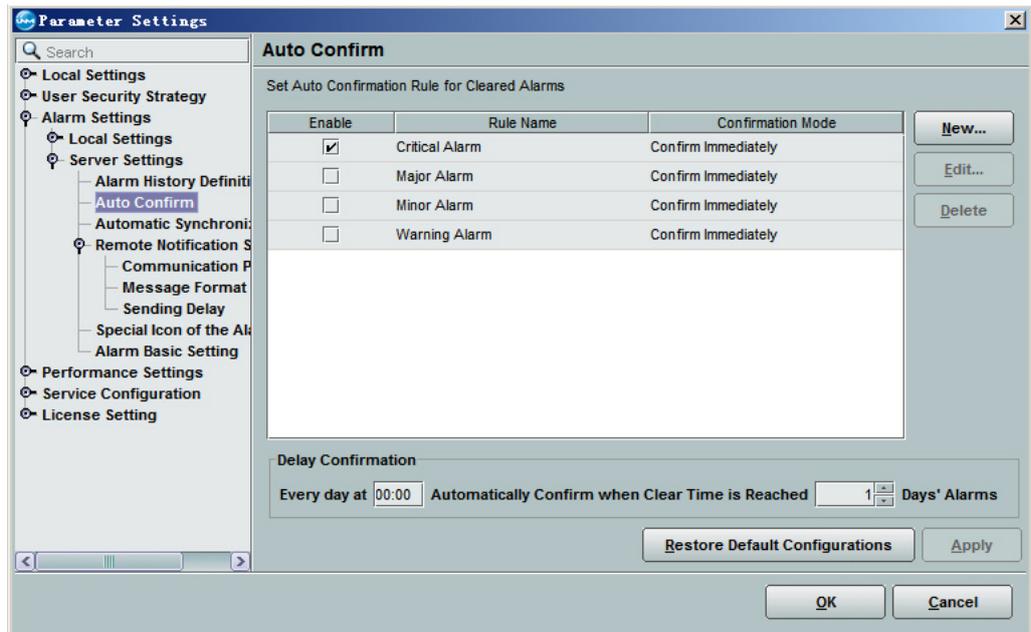
1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Alarm Settings**→**Server Settings**→**Alarm History Definition** in the left pane to open the dialog box.
3. Set the delay for switching current alarms to the alarm history and then click **Apply** to apply the settings.

7.2.9 Setting the Alarm Automatic Confirmation Rules

For convenient maintenance, the UNM2000 provides the automatic confirmation by alarm level or by rule for the unconfirmed but cleared alarms. You can set the automatic confirmation rules for the cleared alarms.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Alarm Settings**→**Server Settings**→**Auto Confirm** in the left pane to open the dialog box.



3. Click **Add** to open the dialog box.
4. Set the parameters in the **Basic information**, **Confirming Condition**, **Alarm Source** and **Alarm Source Type** tabs respectively. Then click **OK** to create an automatic confirmation rule.
5. Return to the **Auto Confirm** dialog box, and click **Apply** to make the settings valid.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the default values.

7.2.10 Converting Events to Alarms

You can change the events into alarms by adding or deleting events in a batch manner. The UNM2000 will process the alarms transformed from events as alarms.

Prerequisite

The authority of the **Event to Alarm Settings** function is configured in the authority and domain division management. Only the user who has the corresponding authority can perform this function.

Procedure

1. Select **Alarm**→**SettingEvent to Alarm Settings** from the UNM2000 main menu.
2. In the **Event to Alarm Settings** tab, select the desired event entries.
3. Click **Save**.

7.2.11 Customizing Alarms

Through custom alarm settings, the UNM2000 can display different types of alarms based on how much users pay attention to these alarms or how users find these alarms. In this way, the maintenance engineers can better monitor the equipment, and quickly isolate the failure and solve the problems.

7.2.11.1 Viewing Custom Special Alarms

This function helps you understand the defined special alarm types.

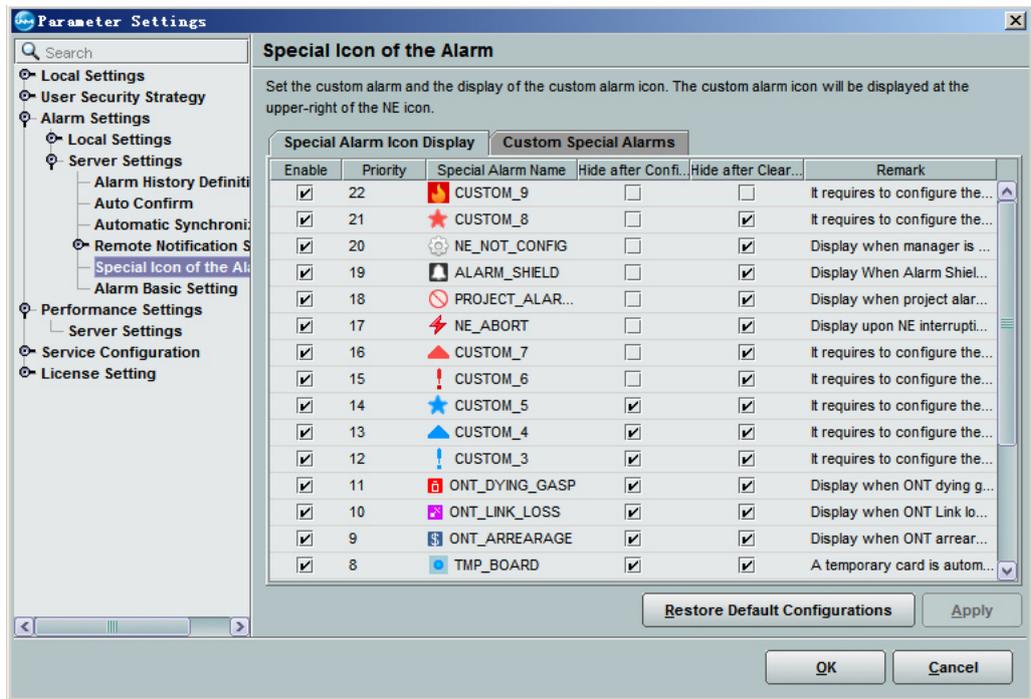
Prerequisite

You have the authority of **Operator Group** or higher authority.

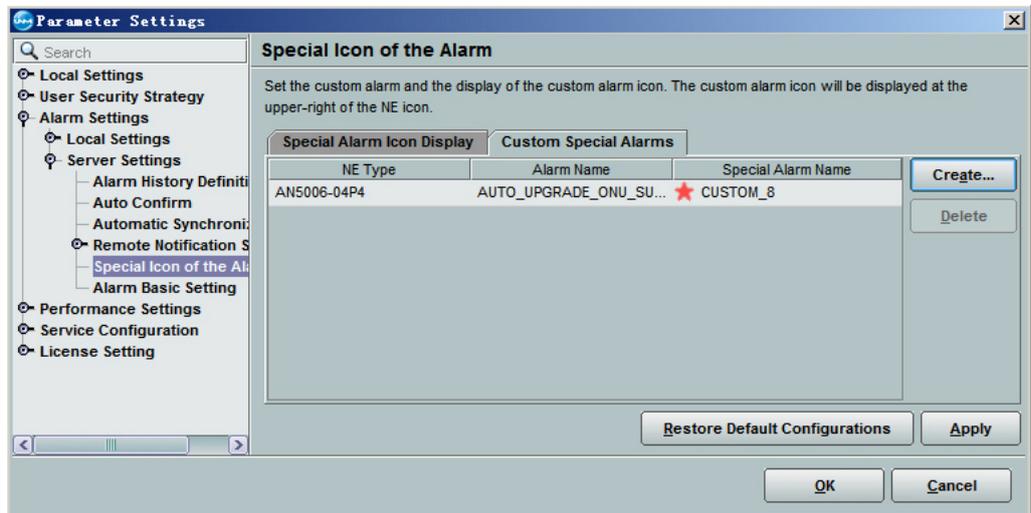
Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.

2. Select **Alarm Settings**→**Server Settings**→**Special Icon of the Alarm** in the left pane to open the dialog box.



3. Click the **Custom Special Alarms** tab to view the special alarms already defined.



7.2.11.2 Customizing Special Alarms

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Alarm Settings**→**Server Settings**→**Special Icon of the Alarm** in the left pane to open the dialog box.
3. Click the **Custom Special Alarms** tab.
4. Click **Create**, select the NE type, alarm name, and special alarm name in the **Custom Special Alarms** dialog box, and then click **OK**.
5. Click **Apply** after the settings are completed, and the settings will be valid.

Subsequent Operation

Select the useless custom special alarms, and click **Delete** to delete them.

7.2.11.3 Setting Special Alarm Icons

Background Information

By setting the special alarm icons, you can view the special alarm icon at the upper-right corner of the NE icon when the corresponding alarm occurs at the NE, so as to obtain the alarm information in a timely manner.

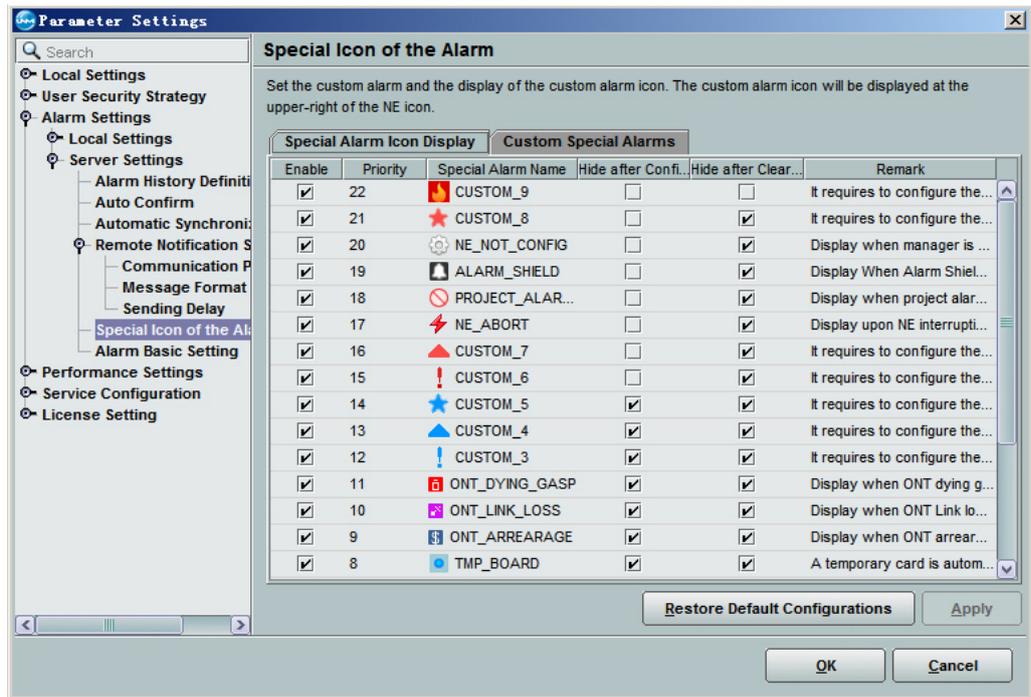
- ◆ When multiple alarms occur at the NE, the special icon of the alarm with the highest priority will be displayed at the upper-right corner of the NE icon.
- ◆ The priority of an alarm ranges from 1 to 22, with 22 being the highest.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Alarm Settings**→**Server Settings**→**Special Icon of the Alarm** in the left pane to open the dialog box.



3. In the **Special Alarm Icon Display** tab, and select **Enable**, **Hide after Confirmation** or **Hide after Clearing** as required.
 - ▶ If **Enable** is selected, the special icon of this alarm appears at the upper-right corner of the NE icon upon the occurrence of the alarm.



Note:

For enabling the custom alarms, see [Customizing Special Alarms](#).

- ▶ If **Hide after confirmation** is selected, after the corresponding alarm is confirmed, the special icon of this alarm at the upper-right corner of the NE will be hidden.
- ▶ If **Hide after Clearing** is selected, after the corresponding alarm is cleared, the special icon of this alarm at the upper-right corner of the NE will be hidden.

4. Click **Apply** after the settings are completed, and the settings will be valid.

7.3 Managing Alarm / Event Templates

The UNM2000 supports setting the alarm / event query conditions or statistical conditions as templates. You can use the predefined alarm / event template to quickly set the filter conditions and attributes of alarms / events.

7.3.1 Alarm Template

The alarm template is used to save the alarm query / statistical conditions. The alarm template simplifies the setting operation and enables you to quickly complete the settings of the alarm browsing and alarm attributes.

The UNM2000 allows you to set the alarm templates for different objects, such as network blocks, NEs, and cards..

The alarm templates include the following types:

- ◆ Current alarm query template
- ◆ Alarm history query template
- ◆ Alarm log query template
- ◆ Current alarm log statistical template
- ◆ Alarm history log statistical template
- ◆ Alarm filter template

The following introduces how to view, add, delete and modify various alarm templates.

7.3.1.1 Viewing Alarm Templates

You can view the alarm template already set and saved. If the current alarm template meets your requirements for querying alarms, you can use the template directory without the need to set the conditions.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Alarm**→**Alarm Query Template** to open the **Alarm Query Template Management** tab.
2. Select **Alarm Profile** in the left pane of the **Alarm Query Template Management** tab, and view the quantity and attributes of various preset templates in the right pane.
3. Click the desired alarm template type and select the specific number of this type of template to view the details.

7.3.1.2 Creating an Alarm Template

You can save the commonly used alarm query / statistical conditions as a template so that you can directly use the template next time for the same query or statistics, without the need to set the conditions again.



Note:

The following uses the current alarm query template as an example. You can follow the same procedures to add other templates with the only difference in the access method.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Alarm**→**Alarm Query Template** to open the **Alarm Query Template Management** tab.
2. Select one of the following access methods to open the **Create Current Alarm Template** dialog box.

No.	Access Method
1	Select Current Alarm Query Template in the left pane, and click Create Current Alarm Template in the right pane.
2	Select Current Alarm Query Template in the left pane, right-click in the right pane and select Create Current Alarm Template from the shortcut menu.
3	Right-click Current Alarm Query Template in the left pane and select Create Current Alarm Template from the shortcut menu.

- Set the alarm query conditions in the **Create Current Alarm Template** dialog box as needed.



Note:

Click **Copy from Other Template**, select the alarm profile in the **Select Template** dialog box, and copy the related information of the selected alarm profile. This can improve the setting efficiency.

- Click **OK**.

Subsequent Operation

Select **Current Alarm Query Template** in the left pane, select the corresponding entry in the right pane and click the corresponding button at the bottom, or right-click the desired entry to perform the operations, such as **Delete**, **Refresh**, **Print**, **Copy Cell** or **Export** from the shortcut menu.

7.3.1.3 Modifying an Alarm Template

When setting the alarm template, you can modify the settings in case the query condition setting error occurs.



Note:

The following uses the current alarm query template as an example. You can follow the same procedures to modify other templates with the only difference in the access method.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Alarm**→**Alarm Query Template** to open the **Alarm Query Template Management** tab.
2. Select **Alarm Profile** in the left pane of the **Alarm Query Template Management** tab, and view the quantity and attributes of various preset templates in the right pane.
3. Click the desired alarm template type and select the specific number of this type of template to view the details.
4. Modify the relevant information of the alarm template in the right pane and click **Apply**.

7.3.1.4 Setting the Template Attributes

At the UNM2000 client, you can set the alarm template as a monitoring template, startup template or default template to facilitate monitoring, querying or gathering statistics of alarms.

Background Information

- ◆ **Default template:** When you query or gather statistics of the alarms via the menu, the UNM2000 will use this template to open the tab of the corresponding functions. Only one default template can be set for a type of alarm templates.
- ◆ **Monitoring profile:** The **Alarm Statistics** dialog box in the toolbar of the UNM2000 client will display the alarm statistics according to this template. The monitoring template needs to be a current alarm template. You can set five monitoring templates at most.

**Note:**

After the monitoring template is set to the current template in the **Alarm Statistics** dialog box, the four indicators (in different colors) on the toolbar will display the statistics data of alarms with various levels according to the current template.

- ◆ Monitoring profile: The Alarm Statistics dialog box in the toolbar of the UNM2000 client will display the alarm statistics according to this template. The monitoring template need to be a current alarm template. You can set five monitoring templates at most.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Alarm** → **Alarm Query Template** to open the **Alarm Query Template Management** tab.
2. Set the alarm template attribute, that is, set the alarm profile to be a monitoring template or startup template.
 - ▶ Set the alarm template as a monitoring template.
 - a) In the left pane of the **Alarm Query Template Management** tab, select **Monitor Template Management**.
 - b) Right-click in the blank area of the right pane and select **Select**, or click the **Select** button at the lower-right corner.
 - c) In the **Select Template** dialog box, select the corresponding alarm and click **OK** to set the template as a monitoring template.
 - d) Select a monitoring template and click **Delete Template Settings**, or right-click the monitoring template and select **Delete Template Settings** to undo setting the alarm template as a monitoring template.
 - ▶ Set the alarm template as a startup template.
 - a) In the left pane of the **Alarm Query Template Management** tab, select **Startup Template Management**.

- b) Right-click in the blank area of the right pane and select **Select**, or click the **Select** button at the lower-right corner.
- c) In the **Select Template** dialog box, select the corresponding alarm and click **OK** to set the template as a startup template.
- d) Select the starting template and click **Delete Template Settings**, or right-click the startup template and select **Delete Template Settings** to undo setting the alarm template as a startup template.

7.3.2 Event Template

The event template simplifies the setting operation and enables you to quickly complete the settings of the event browsing. The event template is used to save the event query or statistical conditions.

The UNM2000 allows you to set the event templates for different objects, such as network blocks, NEs, and cards. Monitoring and managing events can ensure the normal operation of the network.

7.3.2.1 Viewing Event Templates

Save the frequently used event query conditions into a template, so as to use the template for quick query in the future.

Procedure

1. In the main menu, select **Alarm**→**Event Query Template** to open the **Event Query Template** tab.
2. Click **Event Report Query Template** in the left pane to view the existing event query templates.
3. Click the desired event template type and select the specific number of template entries of this type to view the details.

7.3.2.2 Creating an Event Template

Save the frequently used event query conditions into a template, so as to use the template for quick query in the future.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Alarm**→**Event Query Template** to open the **Event Query Template** tab.
2. Select one of the following access methods to open the **New Event Query Template** dialog box.

No.	Access Method
1	Click Event Report Query Template in the left pane and click Create Event Query Template in the right pane.
2	Right-click Event Report Query Template in the left pane and select Create Event Query Template from the shortcut menu.
3	Click Create Event Query Template in the left pane, right-click in the right pane and select Create Event Query Template from the shortcut menu.

3. Set the parameters in the **Basic Information**, **Filter Info**, and **Event Source** tabs as required, and click **OK**. Then the new event query template will be displayed in the template list.



Note:

Click **Select Template**, and you can copy all settings except **Template Name** from other templates. This can improve the setting efficiency.

Other Operations

Right-click the corresponding query template, and select operations such as **Copy**, **Delete**, **Refresh**, **Set as Default Template / Cancel Default Template**, **Print**, **Copy Cell** or **Export**.



Note:

The default profile (**All Object**) of the system cannot be copied, deleted, and modified.

7.3.2.3 Modifying an Event Template

When setting the event template, you can modify the event query template settings in case the query condition setting error occurs.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Alarm**→**Event Query Template** to open the **Event Query Template** tab.
2. Click **Event Report Query Template** in the left pane to view the existing event query templates.
3. Click the event reporting query template to view the detailed settings of the template.
4. Modify the event query reporting template in the right pane and click **Save All**.

7.4 Synchronizing Alarms

Synchronizing alarms includes synchronizing the current alarms of NEs and the UNM2000. With this function, you can synchronize the alarms at the NE side with those at the UNM2000 side and synchronize the current alarms of the UNM2000 with the alarms in the alarm database of the UNM2000. The UNM2000 supports manual alarm synchronization.

7.4.1 Synchronizing Alarms Manually

In case of network interruption, the alarms at the UNM2000 side may be inconsistent with those at the NE side. To actually reflect the alarm data of the NEs, you can synchronize the alarms of the selected NEs to the UNM2000 so as to ensure the alarm data at the UNM2000 and at the NE side are consistent.

Background Information

Generally, the UNM2000 will automatically synchronize the alarm data at the NE side with those at the UNM2000.

Procedure

1. Right-click the object in the main topology and select **Open NE Manager** from the shortcut menu to access the NE Manager GUI.
2. Right-click the corresponding NE in the object tree pane and select **Manual Alarm Synchronization** from the shortcut menu. Then click **Close** in the displayed alert box. The manual alarm synchronization is completed.

7.5 Monitoring Network Alarms

By monitoring the network alarms, you can know the operating status of the network in a timely manner.

The UNM2000 classifies the alarms into the current alarms and the alarm history according to the alarm statuses.

- ◆ **Current alarm:** the alarm data saved in the current alarm database of the UNM2000.

The alarm frequently generated by the same object will be displayed as one entry in the current alarm list. You can view the alarm log to query all the alarm records.

- ◆ **Alarm history:** the current alarms that have been cleared and those confirmed and cleared will be added into the alarm history after a preset period.

The alarm history will be saved into the alarm history database from the current alarm database. See [Setting the Definition of the Alarm History](#) regarding how to set the delay time for transferring the current alarms to the alarm history.

7.5.1 Viewing current alarms

You can view the current alarms of the entire network or a certain object, so as to analyze the alarm information and perform the troubleshooting.

Procedure

1. Select one of the access methods in Table 7-3 to open the **Query Current Alarm** dialog box.

Table 7-3 Access Methods for Viewing Current Alarms

Operation	Access Method
Viewing current alarms	Select Alarm → Current Alarm from the main menu.
	Right-click the corresponding NE in the object tree pane, and select Current Alarm from the shortcut menu.
	Right-click the corresponding NE in the topology view, and select Current Alarm from the shortcut menu.
	In the NE manager window, select Alarm → Current Alarm from the main menu.
	In the Device Tree pane of the NE manager window, right-click the corresponding card or port, and select Current Alarm from the shortcut menu.
	In the Diagram pane of the NE manager window, right-click the corresponding card, and select Current Alarm from the shortcut menu.

2. Querying Current Alarms
 - ▶ Query current alarms by alarm template.



Note:

If the current alarm query template is set, the system collects the current alarms according to the query conditions set in the template. For setting the alarm template, see [Alarm Template](#).

- a) In the **Current Alarm** tab, click **Query by Template**. The current alarm tab displays the alarms queried by the template.
- ▶ Set the query condition to view the current alarms.
 - a) In the **Current Alarm** tab, click **Query**. The **Query Current Alarm** window appears.
 - b) Set the query conditions in the **Basic Information**, **Alarm Source** and **Advanced Information** tabs as needed.



Note:

After setting the query conditions in the **Current alarm query** dialog box, you can click **Save as template** to save the query conditions as a profile. When needing to query according to the same conditions, you can select this profile directly, without repeated settings.

- c) After completing the settings, click **OK** to view the current alarms meeting the conditions.

No.	Icon	Level	Name	Confirmation S.	Clear Status	Alarm Source	Location Information	Port No.	Frequen.	First Occurrence Time	Latest Occurrence Time	Duration
35966...		Critical	LFAN	Unconfirmed	Not Cleared	MXCFEOL001	MXCFEOL001-HU1A[20]:	2	1	2017-10-23 15:26:42	2017-10-23 15:26:42	2 minutes 1 Seconds
35966...		Critical	RA_Q2	Unconfirmed	Not Cleared	LBSFEOL001	LBSFEOL001-GC8B[1]:	2	1	2017-10-23 15:26:42	2017-10-23 15:26:42	2 minutes 0 Seconds
35966...		Minor	T_RIP	Unconfirmed	Not Cleared	DLSFEOL002	DLSFEOL002-HS1WA[9]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Minor	EX3	Unconfirmed	Not Cleared	CBRFEOL001	CBRFEOL001-GC2B[12]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Minor	RMT_T	Unconfirmed	Not Cleared	OZAFEOL001	OZAFEOL001-HU2A[19]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Minor	LTL5	Unconfirmed	Not Cleared	LPZFEOL001	LPZFEOL001-HU2A[19]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Minor	LTT9	Unconfirmed	Not Cleared	MCNFEOL004	MCNFEOL004-HU2A[20]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Critical	RAH_LEAK	Unconfirmed	Not Cleared	MCNFEOL002	MCNFEOL002-HS1WA[9]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Minor	LTL2	Unconfirmed	Not Cleared	IPLFEOL001	IPLFEOL001-PWR2[4]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Minor	LTL2_HDB3	Unconfirmed	Not Cleared	LBSFEOL001	LBSFEOL001-HU1A[19]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Critical	FAIL	Unconfirmed	Not Cleared	IBAFEOL001	IBAFEOL001-FAN2[1]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Major	MAIN_OPM	Unconfirmed	Not Cleared	TAGFEOL005	TAGFEOL005-GC0B[1]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Critical	V53CO_LC_13ERR	Unconfirmed	Not Cleared	DIGFEOL001	DIGFEOL001-PUBA[14]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Minor	SYNC_LOSS	Unconfirmed	Not Cleared	CMNFEOL001	CMNFEOL001-FAN2[2]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Critical	ORALM	Unconfirmed	Not Cleared	MRNFEOL001	MRNFEOL001-FAN2[2]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Critical	LCOOLC1	Unconfirmed	Not Cleared	LBSFEOL001	LBSFEOL001-GC8B[1]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Warning	ES_LIMIT_MS	Unconfirmed	Not Cleared	CAIFEOL004	CAIFEOL004-GC0B[5]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Critical	OOL2G5	Unconfirmed	Not Cleared	TSCFEOL002	TSCFEOL002-GC8B[5]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Critical	LASERP2	Unconfirmed	Not Cleared	TCBFEOL002	TCBFEOL002-GC0B[7]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Major	TRIB_OPM_LOW	Unconfirmed	Not Cleared	LLLFEOL001	LLLFEOL001-GC8B[2]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Critical	SLOS	Unconfirmed	Not Cleared	IMUFEOL004	IMUFEOL004-GC8B[1]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Major	L1_ALM	Unconfirmed	Not Cleared	TBFEOL001	TBFEOL001-GC8B[2]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Minor	LASER_TCT	Unconfirmed	Not Cleared	QCYFEOL002	QCYFEOL002-PWR2[5]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Minor	LTHW-2	Unconfirmed	Not Cleared	GPWFEOL002	GPWFEOL002-PWR2[4]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds
35966...		Critical	SDH_TIM	Unconfirmed	Not Cleared	TOLFEOL001	TOLFEOL001-HU2A[19]:	2	1	2017-10-23 15:26:43	2017-10-23 15:26:43	2 minutes 0 Seconds

Subsequent Operation

You can perform the following operations as needed.

- ◆ Click the shortcut icons at the upper left corner of the **Current Alarm** tab to perform the following operations.
 - ▶ Click to set whether to automatically report updated alarms.
 - ▶ Click to set whether the system automatically scrolls the alarm display table when the alarms are reported.
 - ▶ Click to select the corresponding template for query.
 - ▶ Click to set whether the current alarm window displays only the critical alarms.
 - ▶ Click to set whether the current alarm window displays only the major alarms.

- ▶ Click  to set whether the current alarm window displays only the minor alarms.
- ▶ Click  to set whether the current alarm window displays only the prompt alarms.
- ◆ Click the buttons at the bottom-right corner of the **Current Alarm** tab to perform the corresponding operations.
 - ▶ Select an alarm and click **View Details** to view the details of the selected alarm.
 - ▶ Select an alarm and click **Confirm Alarm**. The **Confirmation Status** of the alarm becomes **User Confirmation**.
 - ▶ Select an alarm and click **Clear Alarm**. The **Clear Status** of the alarm becomes **User Clearance**.

7.5.2 Viewing Alarm History

You can view the alarm history of a certain object or all objects in the entire network to understand the alarms occurred so as to facilitate failure analysis.

Background Information

- ◆ The alarms already confirmed and cleared are categorized into the alarm history while the alarms in other status are categorized as the current alarms.
- ◆ When the number of alarms exceeds the default threshold preset, only the latest alarm history will be displayed and the earlier alarm history will not be displayed. To view the earlier alarm history, you can set the filter condition to query.

Procedure

1. Select one of the access methods in Table 7-4 to open the **Alarm History Query** dialog box.

Table 7-4 Access Methods for Viewing the Alarm History

Operation	Access Method
Viewing Alarm History	In the Diagram pane of the NE manager window, right-click the corresponding card and select Alarm History from the shortcut menu.

Table 7-4 Access Methods for Viewing the Alarm History (Continued)

Operation	Access Method
	Right-click the corresponding NE in the object tree pane and select Alarm History from the shortcut menu.
	Right-click the corresponding NE in the topology view and select Alarm History from the shortcut menu.
	Select Alarm → Alarm History from the main menu in the NE manager window.
	In the Device Tree pane of the NE manager window, right-click the corresponding card or port and select Alarm History from the shortcut menu.
	Select Alarm → Alarm History from the main menu.

2. Viewing Alarm History

- ▶ View the alarm history by alarm template.



Note:

If the alarm history query template is set, the system collects the alarm history according to the query conditions set in the template. For setting the alarm template, see [Alarm Template](#).

- a) In the **Alarm History** tab, click **Query by Template**. The alarm history tab displays the alarms queried by the template.
- ▶ Set the query conditions to view the alarm history.
 - a) In the **Alarm History** tab, click **Query** to bring up the **Alarm History Query** window.
 - b) Set the query conditions in the **Basic Information**, **Alarm Source** and **Advanced Information** tabs as needed.



Note:

After setting the query conditions in the **Alarm History Query** dialog box, you can click **Save as template** to save the query conditions as a profile. When needing to query according to the same conditions, you can select this profile directly, without repeated settings.

- c) After completing the settings, click **OK** to view the alarm history meeting the set conditions.

No.	Icon	Level	Name	Confirmation S.	Clear Status	Alarm Source	Location Information	Port No.	Occurrence Time	(Reverse) Confirming Time	(Re)Confirmed By	Clear Time	Clear User
35966	Minor	C_SWR		Auto Confirm...	Equipment Cl.	MLZFEOL001	MLZFEOL001.FAN[2]	2	2017-10-23 15:25:59	2017-10-23 15:28:05		2017-10-23 15:27:45	
35966	Major	MS_EXC		Auto Confirm...	Equipment Cl.	TMSFEOL001	TMSFEOL001.GC8B[5]	2	2017-10-23 15:25:18	2017-10-23 15:28:05		2017-10-23 15:27:24	
35965	Major	OTH_SCH_SD		Auto Confirm...	Equipment Cl.	BTAFEOL001	BTAFEOL001.HSWA[9]	2	2017-10-23 15:24:33	2017-10-23 15:28:05		2017-10-23 15:26:27	
35965	Major	DECODE_SW		Auto Confirm...	Equipment Cl.	MLZFEOL001	MLZFEOL001.PUBA[11]	2	2017-10-23 15:22:57	2017-10-23 15:28:05		2017-10-23 15:27:21	
35965	Minor	OURL		Auto Confirm...	Equipment Cl.	DSLFEOL005	DSLFEOL005.GC8B[8]	2	2017-10-23 15:22:43	2017-10-23 15:28:05		2017-10-23 15:24:43	
35965	Warning	TFFW1		Auto Confirm...	Equipment Cl.	PONFEOL001	PONFEOL001.HU1A[19]	2	2017-10-23 15:22:19	2017-10-23 15:28:05		2017-10-23 15:26:56	
35965	Minor	ALL_ERR		Auto Confirm...	Equipment Cl.	SRAFEOL001	SRAFEOL001.FAN[2]	2	2017-10-23 15:22:04	2017-10-23 15:28:05		2017-10-23 15:24:56	
35965	Major	LD_TEMP_H		Auto Confirm...	Equipment Cl.	PLDFEOL001	PLDFEOL001.HSWA[10]	2	2017-10-23 15:21:37	2017-10-23 15:28:05		2017-10-23 15:27:07	
35965	Critical	T_DOF		Auto Confirm...	Equipment Cl.	ALAFEOL002	ALAFEOL002.GC8B[17]	2	2017-10-23 15:21:20	2017-10-23 15:25:12		2017-10-23 15:25:10	
35965	Critical	OSC_OH_LOS		Auto Confirm...	Equipment Cl.	PNBFEOL001-N	PNBFEOL001-NMSA[4]HS	2	2017-10-23 15:21:10	2017-10-23 15:27:12		2017-10-23 15:26:16	
35965	Warning	SES_LMIT(T)		Auto Confirm...	Equipment Cl.	PONFEOL001	PONFEOL001.HSWA[10]	2	2017-10-23 15:21:10	2017-10-23 15:28:05		2017-10-23 15:25:58	
35965	Minor	LP_AIS		Auto Confirm...	Equipment Cl.	BWDFEOL001	BWDFEOL001.HSWA[10]	2	2017-10-23 15:21:03	2017-10-23 15:28:05		2017-10-23 15:26:57	
35965	Minor	ERR_HW		Auto Confirm...	Equipment Cl.	DSLFEOL005	DSLFEOL005.GC8B[7]	2	2017-10-23 15:20:47	2017-10-23 15:28:05		2017-10-23 15:22:47	
35965	Critical	V52BCCERR		Auto Confirm...	Equipment Cl.	SAJFEOL001	SAJFEOL001.HU1A[19]	2	2017-10-23 15:20:43	2017-10-23 15:27:12		2017-10-23 15:26:40	
35965	Minor	GCTRL_ERROR		Auto Confirm...	Equipment Cl.	PONFEOL001	PONFEOL001.PWR[2]	2	2017-10-23 15:20:43	2017-10-23 15:28:05		2017-10-23 15:24:18	
35965	Minor	RND1_SWR		Auto Confirm...	Equipment Cl.	PONFEOL001	PONFEOL001.PWR[2]	2	2017-10-23 15:20:40	2017-10-23 15:28:05		2017-10-23 15:23:25	
35965	Critical	TD3_LOP		Auto Confirm...	Equipment Cl.	TDDFEOL001	TDDFEOL001.FAN[2]	2	2017-10-23 15:20:31	2017-10-23 15:23:12		2017-10-23 15:22:45	
35965	Critical	LASER_TCT		Auto Confirm...	Equipment Cl.	TDDFEOL001	TDDFEOL001.GC8B[12]	2	2017-10-23 15:20:17	2017-10-23 15:27:12		2017-10-23 15:27:08	
35965	Critical	E14_FAIL		Auto Confirm...	Equipment Cl.	PONFEOL001	PONFEOL001.HU1A[20]	2	2017-10-23 15:20:11	2017-10-23 15:22:12		2017-10-23 15:21:30	
35965	Warning	GROUP_MS_UAS		Auto Confirm...	Equipment Cl.	NGAFEOL001	NGAFEOL001.HU1A[20]	2	2017-10-23 15:20:01	2017-10-23 15:28:05		2017-10-23 15:26:50	
35965	Minor	LTTW41		Auto Confirm...	Equipment Cl.	DVOFEOL001	DVOFEOL001.GC8B[3]	2	2017-10-23 15:20:00	2017-10-23 15:28:05		2017-10-23 15:27:16	
35965	Critical	CLIENT_RXLOL		Auto Confirm...	Equipment Cl.	URDFEOL001	URDFEOL001.GC8B[6]	2	2017-10-23 15:19:55	2017-10-23 15:27:12		2017-10-23 15:26:18	
35965	Critical	WLOGRCK		Auto Confirm...	Equipment Cl.	CLDFEOL001	CLDFEOL001.HU1A[19]	2	2017-10-23 15:19:55	2017-10-23 15:25:12		2017-10-23 15:24:29	
35965	Warning	SDH_ES_LMIT		Auto Confirm...	Equipment Cl.	MLZFEOL001	MLZFEOL001.FAN[2]	2	2017-10-23 15:19:20	2017-10-23 15:28:05		2017-10-23 15:23:11	
35965	Critical	LFA_01		Auto Confirm...	Equipment Cl.	GRKFEOL001	GRKFEOL001.HSWA[10]	2	2017-10-23 15:19:19	2017-10-23 15:23:12		2017-10-23 15:22:47	

Subsequent Operation

You can perform the following operations as needed.

- ◆ Perform operations by clicking shortcut icons. Click the shortcut icons at the upper left corner to perform the following operations.
 - ▶ Click  to select a different template for query.
 - ▶ Click  to set whether the alarm history window displays only the critical alarms.
 - ▶ Click  to set whether the alarm history window displays only the major alarms.
 - ▶ Click  to set whether the alarm history window displays only the minor alarms.
 - ▶ Click  to set whether the alarm history window displays only the prompt alarms.
- ◆ Perform operations by clicking buttons. Click the buttons at the lower right corner of the tab to perform the following operations.
 - ▶ Select an alarm and click **View Details** to view the details of the selected alarm.
 - ▶ Click **Refresh** to refresh the alarms.

- ▶ Right-click an alarm, and you can perform the following operations via the shortcut menu: isolating, refreshing, and exporting, etc. For operations related to alarm handling, see [Handling Alarms](#).

7.5.3 Viewing Related Alarms

You can view the NE alarms to understand the running status of the NE.

Procedure

1. Open the **Current Alarm** or **Alarm History** tab according to [Viewing current alarms](#) and [Viewing Alarm History](#).
2. Right-click the corresponding alarm and select **View Current Alarm of Attributed NE / View NE Alarm History** to view the current alarm / alarm history of the NE corresponding to the alarm.

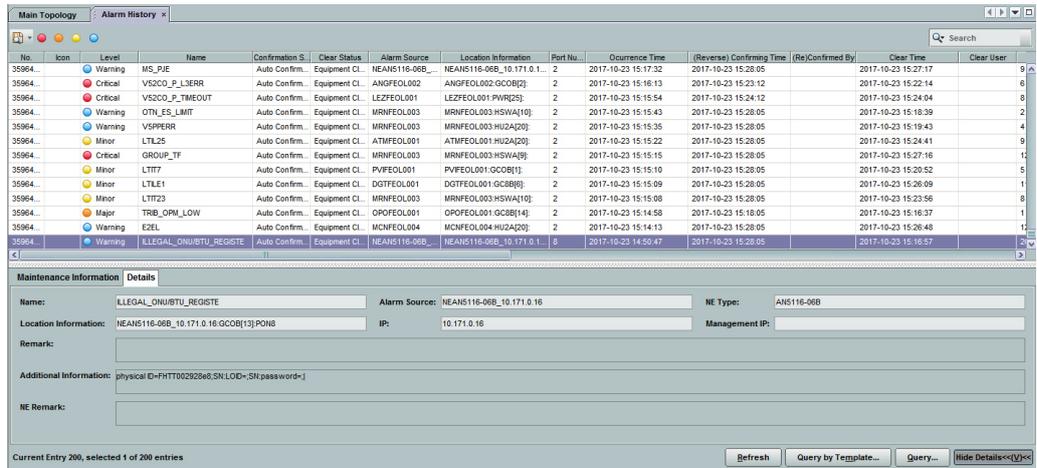
The left screenshot shows a table of alarms with columns: No., Icon, Level, Name, Confirmation S., Clear Status, Alarm Source, Location Information, Port No., and Frequent. The row for 'ERR3_01' is highlighted. The right screenshot shows the detailed view of the 'ERR3_01' alarm, with the same columns and a 'View Details' button at the bottom right.

7.5.4 Viewing Alarm Details

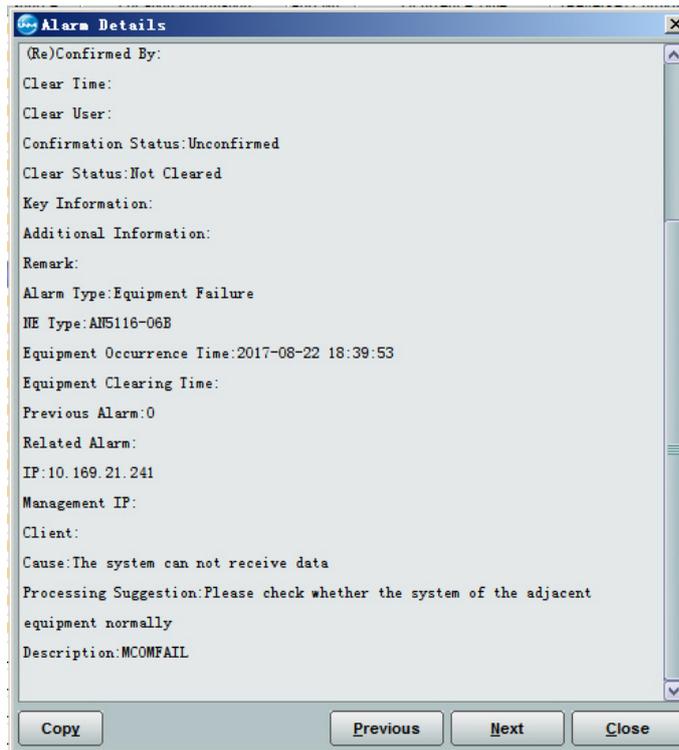
By viewing the alarm details, you can obtain the alarm name, alarm reason, processing suggestion and location.

Procedure

1. Open the **Current Alarm** or **Alarm History** tab according to [Viewing the Current Alarms](#) and [Viewing Alarm History](#).
2. Select an alarm and click **View Details** in the lower right corner to view the details of the selected alarm.



- Right-click the alarm and select **View Detail** to view the alarm details in text. You can click **Copy** to copy the alarm details to the clipboard.



Subsequent Operation

You can process the alarms according to the processing suggestions in the **Maintenance Experience**.

7.5.5 View alarm logs.

You can query the log information for the alarms of the entire network or the selected object via viewing the alarm logs.

Procedure

1. Select **Alarm** → **Alarm Log** → **Query Alarm Log** from the main menu to open the **Query Alarm Logs** dialog box.
2. View alarm logs.
 - ▶ Query the alarm logs by log template.



Note:

If the default log query template is set, the system collects the alarm logs according to the query conditions set in the template. For setting the alarm template, see [Creating an Alarm Template](#).

- a) In the **Query Alarm Logs** tab, click **Select Template**.
 - b) In the displayed **Select Template** window, select the desired template and click **OK**.
 - c) In the **Query Alarm Logs** tab, click **OK**. The Alarm Log tab displays the alarm logs matching the conditions preset in the template.
- ▶ Set the query condition to view alarm logs.
- a) Set the query conditions in the **Query Alarm Logs** dialog box.
 - b) Click **OK** to view the alarm logs meeting the conditions.

No.	Icon	Level	Name	Confirmation S.	Clear Status	Alarm Source	Port No.	Occurrence Time	(Reverse) Confirming Time	(Re)/Confirmed By	Clear Time	Clear User
4013		Critical	CPU_INVERSION_FAILED	Unconfirmed	Not Cleared	????ANS516-01...	0	2017-10-20 11:38:29				
4012		Major	CONFIG_HAVENOT_SAVED	Unconfirmed	Not Cleared	????ANS516-01...	0	2017-10-13 13:31:50				
4011		Major	CONFIG_HAVENOT_SAVED	Unconfirmed	Not Cleared	????ANS516-01...	0	2017-10-18 14:23:51				
4010		Critical	LINK_LOSS	Unconfirmed	Not Cleared	????ANS116_02...	2	2017-09-29 16:38:48				
4009		Critical	LINK_LOSS	Unconfirmed	Not Cleared	????ANS116_02...	1	2017-09-29 16:38:48				
4008		Critical	LINK_LOSS	Unconfirmed	Not Cleared	????ANS116_02...	2	2017-09-29 16:38:48				
4007		Critical	LINK_LOSS	Unconfirmed	Not Cleared	????ANS116_02...	1	2017-09-29 16:38:48				
4006		Major	CONFIG_HAVENOT_SAVED	Unconfirmed	Not Cleared	????ANS116_02...	0	2017-09-29 16:38:48				
4005		Warning	ILLEGAL_ONUBTU_REGISTE	Unconfirmed	Not Cleared	????ANS516-01...	8	2017-10-23 14:36:23				
4004		Critical	LACP_LINK_DOWN	Unconfirmed	Not Cleared	????ANS516-01...	4	2017-10-18 15:48:39				
4003		Critical	LACP_LINK_DOWN	Unconfirmed	Not Cleared	????ANS516-01...	3	2017-10-18 15:48:39				
4002		Critical	LACP_LINK_DOWN	Unconfirmed	Not Cleared	????ANS516-01...	2	2017-10-18 15:48:39				
4001		Critical	LACP_LINK_DOWN	Unconfirmed	Not Cleared	????ANS516-01...	1	2017-10-18 15:48:39				
4000		Major	CONFIG_HAVENOT_SAVED	Unconfirmed	Not Cleared	10.171.0.22	0	2017-10-23 09:29:58				

Total 14 entries

Buttons: Refresh, Query by Template..., Query..., Confirm Alarm, Clear Alarm, View Details(U)

**Note:**

After setting the query conditions in the **Alarm log query** dialog box, you can click **Save as template** to save the query conditions as a profile. When querying according to the same conditions, you can select this profile directly, without repeated settings.

Subsequent Operation

You can also perform the following operations as required after completing the alarm log query information.

- ◆ Click the shortcut icons at the upper-left corner of the **Alarm Log** tab to perform the corresponding operations.
 - ▶ Click  to select a different template for query.
 - ▶ Click  to set whether to display logs of critical alarms only in the **Alarm Log** tab.
 - ▶ Click  to set whether to display logs of major alarms only in the **Alarm Log** tab.
 - ▶ Click  to set whether to display logs of minor alarms only in the **Alarm Log** tab.
 - ▶ Click  to set whether to display logs of prompt alarms only in the **Alarm Log** tab.
- ◆ Click the buttons at the bottom-right corner of the **Alarm Log** tab to perform the corresponding operations.
 - ▶ Select an alarm and click **View Details** to view the details of the selected alarm. For specific information, see [Viewing Alarm Details](#).
 - ▶ Click **Refresh** to refresh the alarms.
 - ▶ Click **Query by the Template** to select another template for query.
 - ▶ Click **Query** to open the **Query Alarm Logs** dialog box. Then reset the query condition for query.

- ◆ Select the shortcut menus. Right-click an alarm and select the corresponding shortcut menu to confirm, clear or locate the alarm. For operations related to alarm handling, see [Handling Alarms](#).

7.5.6 Viewing the Alarm Log Statistics

You can set the statistics conditions for the statistics of alarm logs.

Procedure

The procedures of gathering the alarm log statistics are similar. The following takes gathering the current alarm log statistics as an example.

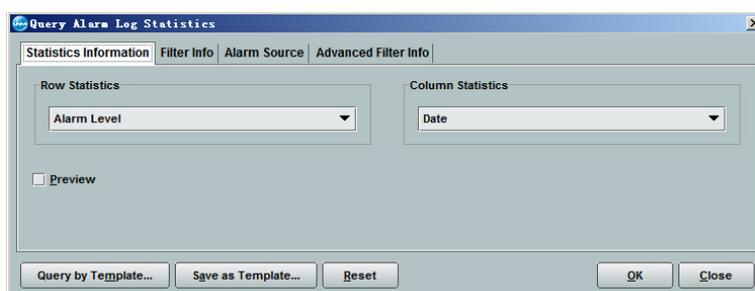
1. Select **Alarm**→**Alarm Log**→**Gather Current Alarm Log Statistics** from the main menu to open the **Query Alarm Log Statistics** dialog box.



Note:

If the default alarm log statistics profile has been set, the system will query according to the default profile. For the operations of setting the default alarm query profile, see [Alarm Template](#).

2. Set the statistics conditions in the **Alarm log statistics query** dialog box, and then click **OK**.

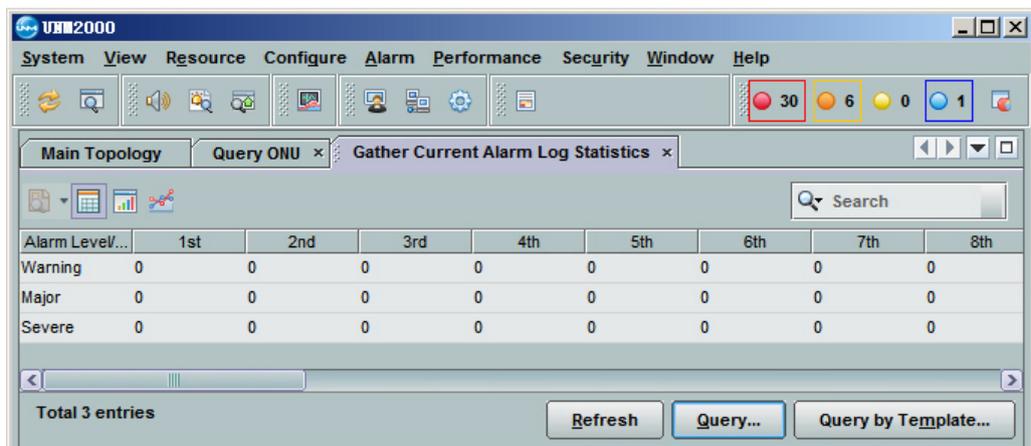




Note:

After setting the query conditions in the **Alarm log statistics query** dialog box, you can click **Save as template** to save the query conditions as a profile. When querying according to the same conditions, you can select this profile directly, without repeated settings.

3. After completing the settings, click **OK** to view the statistics information of alarm logs meeting the set conditions.



Subsequent Operation

You can perform the following operations as needed.

- ◆ Click the shortcut icons at the upper-left corner of the **Alarm Log Statistics** tab to perform the corresponding operations.
 - ▶ Click  to select a different template for query.
 - ▶ Click  to display the alarm log statistics in a table.
 - ▶ Click  to display the alarm log statistics in a chart. You can select different display and output modes through different operation buttons.
 - Click  to print the current page.
 - Click  to export the current page as an image.
 - Click  to select the alarm levels displayed on the current page.

- Click  to select the time point displayed in the chart of the list that appears.
- Click  to display the alarm log statistics in a curve chart.
- Click  to display the alarm log statistics in a bar chart.
- Click  to display the alarm log statistics in a pie chart.
- ▶ Click  to display the alarm log statistics in a curve comparison chart.

7.5.7 Viewing Alarm Statistics

The following introduces how to view the alarm statistics through the alarm panel.

Procedure

1. Click  on the shortcut toolbar of the main menu to open the **Alarm Statistics** dialog box.



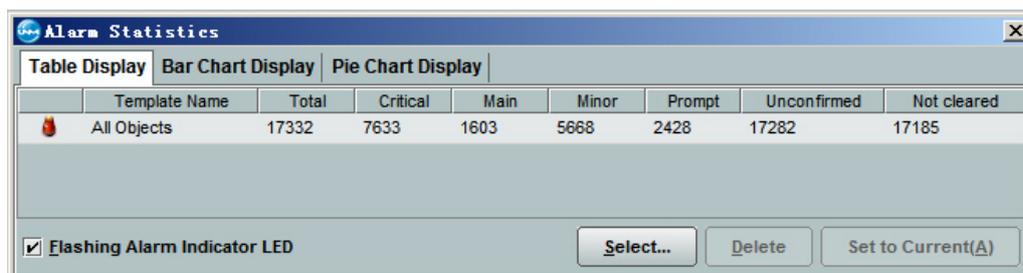
Note:

In the **Alarm Statistics** dialog box, the statistics are displayed in the way you have selected.

Subsequent Operation

- ◆ Select **Table Display**.

Click the Table Display tab, and select the corresponding monitoring template and the statistical classification item. In the display pane, the alarm statistical information is displayed in a table.

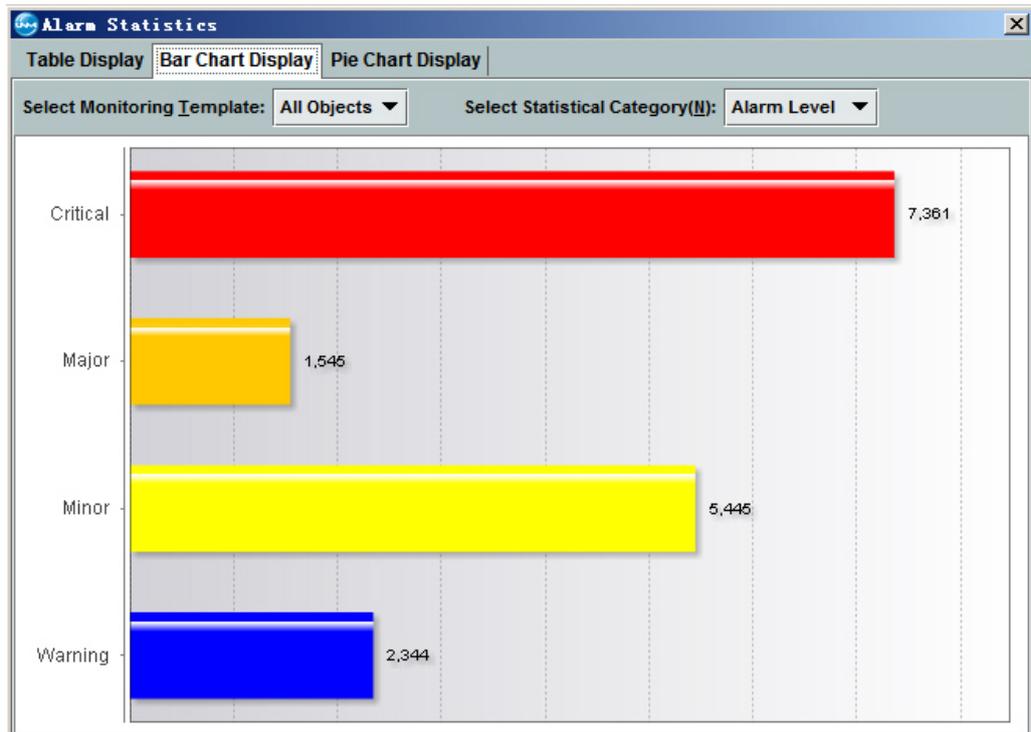


Template Name	Total	Critical	Main	Minor	Prompt	Unconfirmed	Not cleared
 All Objects	17332	7633	1603	5668	2428	17282	17185

Flashing Alarm Indicator LED

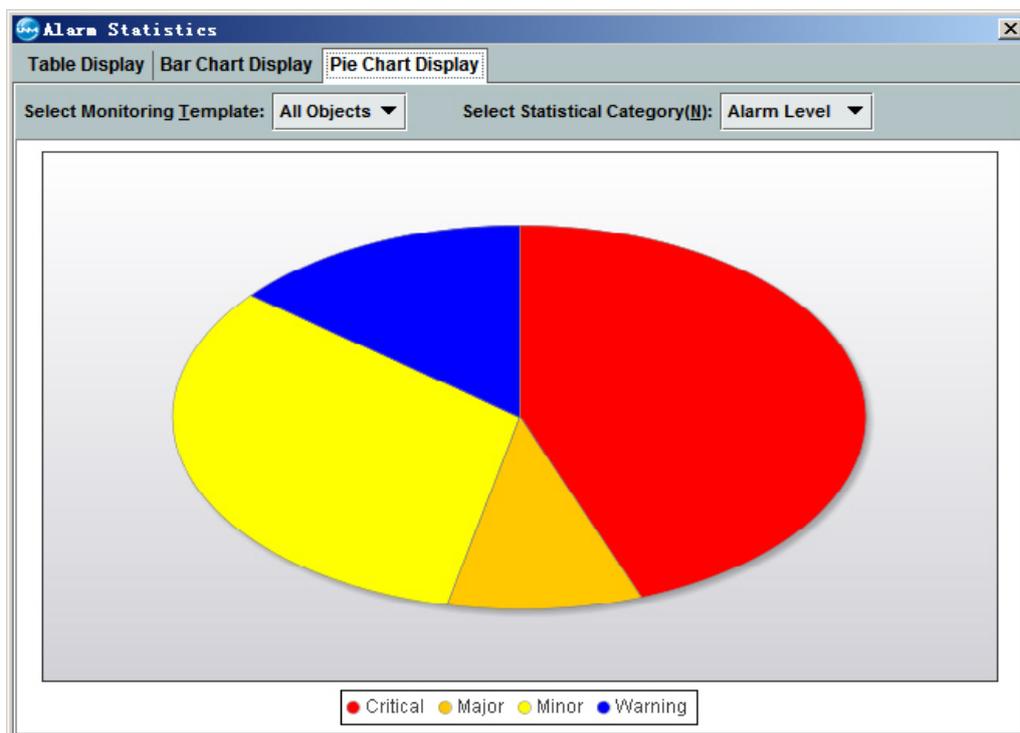
Select... Delete Set to Current(A)

- ▶ Select **Flashing Alarm Indicator LED** to flicker the corresponding LED automatically on the toolbar when an alarm occurs.
 - ▶ Click the **Select Template** or right-click in the table display area to select **Select Template**. In the displayed **Select Template** dialog box, select the corresponding template and view its statistical information.
 - ▶ Select the corresponding row in the table and click **Cancel Statistics** or right-click the row and select **Cancel Statistics** to cancel calculating the alarm information.
 - ▶ Select the corresponding row in the table and click **Set to Current** or right-click the row and select **Set to Current**. After setting the selected template as the current one, the four-color alarm indicator LEDs on the toolbar will display the corresponding information of the current template.
 - ▶ Right-click in the table display area to select **Alarm Query Template** to open the **Alarm Query Template Management** tab. Then add, delete or modify the alarm query template as needed. For details, see [Alarm Template](#).
- ◆ Select **Bar Chart Display**.
- Click the **Bar Chart Display** tab, and select the corresponding monitoring template and the statistical classification item. In the display pane, the alarm statistical information is displayed in a bar chart.



◆ **Select Pie Chart Display.**

Click the **Pie Chart Display** tab, and select the corresponding monitoring template and the statistical classification item. In the display pane, the alarm statistical information is displayed in a pie chart.



7.5.8 Querying Reported Events

By querying the reported events, you can obtain the running status of the system.

Procedure

1. Select **Alarm** → **Query Reported Events** from the main menu.
2. Set the query conditions in the **Query Reported Events** dialog box that appears and click **OK**.



Note:

- ◆ If the default template has been set, the system will query according to the default template.
- ◆ You can click **Copy from Template** in the **Query Reported Events** dialog box to select an existing template for query.
- ◆ After setting the query conditions, you can click **Save as Template** to save the current query conditions as a template.

3. In the **Query Reported Events** tab, view the query results.

No.	Icon	Level	Name	Occurrence Time	Location Info
67077...		Warning	TIME_ACK	2017-08-22 18:34:31	10.171.0.22:(SlotNo=9)
67077...		Warning	TIME_ACK	2017-08-22 19:35:04	10.171.0.22:(SlotNo=9)HSWA[09]
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-22 19:45:10	10.171.0.22:(SlotNo=13)GC4B[13]:PON1
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-22 19:45:10	10.171.0.22:(SlotNo=13)GC4B[13]:PON1
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-22 19:49:04	10.171.0.22:(SlotNo=13)GC4B[13]:PON2
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-22 19:49:04	10.171.0.22:(SlotNo=13)GC4B[13]:PON[2]-AN55...
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-22 19:51:54	10.171.0.22:(SlotNo=13)GC4B[13]:PON1
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-22 19:51:54	10.171.0.22:(SlotNo=13)GC4B[13]:PON[1]-AN50...
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-23 10:23:17	10.171.0.22:(SlotNo=1)GC8B[01]:PON1
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-23 10:23:17	10.171.0.22:(SlotNo=1)GC8B[01]:PON1
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-23 10:23:17	10.171.0.22:(SlotNo=1)GC8B[01]:PON1
67077...		Warning	ONU_AUTH_SUCCESS	2017-08-23 10:23:17	10.171.0.22:(SlotNo=1)GC8B[01]:PON1

Subsequent Operation

- ◆ Click the shortcut icons at the upper-left corner of the **Query Reported Events** tab to perform the corresponding operations.
 - ▶ Click to set whether to automatically report updated alarms.
 - ▶ Click to set whether the system automatically scrolls the alarm display table when the alarms are reported.
 - ▶ Click to select the corresponding template for query.
 - ▶ Click to set whether the current alarm window displays only the critical alarms.
 - ▶ Click to set whether the current alarm window displays only the major alarms.
 - ▶ Click to set whether the current alarm window displays only the minor alarms.
 - ▶ Click to set whether the current alarm window displays only the warning alarms.
- ◆ Click the buttons at the bottom of the **Query Reported Events** tab to perform the corresponding operations.
 - ▶ Click **Query** to reset the query conditions in the **Query Reported Events** dialog box and then click **OK**.

- ▶ Click **Query by Template**, select the desired template in the **Select Template** dialog box and then click **OK**.
- ▶ Select an event entry and click **View Details** to view the detailed information of the selected event.
- ◆ Right-click the event entry in the **Query Reported Events** tab and select the shortcut menu items to perform the corresponding operations.
- ◆ Select **Topology Location** to locate the source NE that triggered the event in the topology view so as to ascertain the physical position of the corresponding NE in the network.
- ◆ Select **View Event Report of the NE** to filter the events corresponding to the NE so as to analyze the running status of the NE.
- ◆ Select **Remark** to type the remark information of the selected event.
- ◆ Select **Copy Cell** to copy the information in the selected table cell to the clipboard.
- ◆ Select **Print** to print the event logs.
- ◆ Select **Export**→**Export All Records** to export all reported events in format of TXT, Excel, CSV, XML, PDF or HTML to the specified directory.
- ◆ Select **Export**→**Export Select Record** to export the selected events in format of TXT, Excel, CSV, XML, PDF or HTML to the specified directory.

7.5.9 Viewing Reported Alarms

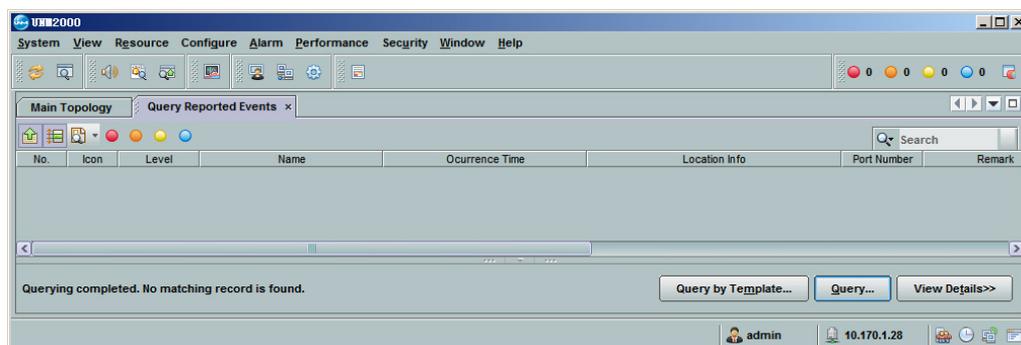
This section introduces how to view the reported alarms.

Prerequisite

The alarm reporting rules have been set and enabled.

Procedure

1. Select **Alarm**→**View the Reported Alarms** from the main menu.
2. In the **View Reported Alarm** tab, view the information on the alarms meeting the reporting conditions.



Note:

For the related operations of the buttons, shortcut icons, and shortcut menus in the **View Reported Alarm** tab, see [Viewing current alarms](#).

3. Click **Report Setting** at the bottom-right part of the tab, and access the **Alarm Report Setting** tab to re-configure the alarm reporting rules.
4. Click **Clear All Records** at the bottom-right part of the tab to clear all the records in the current tab. Then the tab will display the alarm information reported after the records are cleared.

7.6 Handling Alarms

When an alarm occurs, you should handle the alarm following certain procedures to eliminate the fault, including viewing the detailed alarm information, isolating the alarm, confirming the alarm and clearing the alarm.

7.6.1 Confirming Alarms

The UNM2000 supports manual alarm confirmation and automatic confirmation of the cleared alarms. The manual alarm confirmation indicates that the alarm has been processed by a user.

Procedure

- ◆ Confirm alarms manually.

- 1) See [Viewing current alarms](#) or [View alarm logs](#). for opening the **Current Alarm** or **Alarm Log** tab.
- 2) Confirm the alarms via one of the following ways:
 - Select the corresponding alarm and click **Confirm Alarm** in the lower right part of the tab.
 - Right-click the corresponding alarm and select **Confirm Alarm**.
 - Right-click the corresponding alarm and select **Confirm and Mark the Alarms**.

After manual alarm confirmation, the **Confirmation Status** of the corresponding alarm will turn to **User Confirmation**.

◆ Confirming alarms automatically

See [Setting the Alarm Automatic Confirmation Rules](#) for setting the automatic confirmation rules of the cleared alarms.

By default, the system clears the alarms one day after their occurrence time at 00:00 automatically and the **Confirmation Status** of the alarms will change to **Auto Confirm**.



Note:

If any alarm is to be re-focused, you can right-click this alarm and select **Unconfirm the Alarm**. The **Confirmation Status** of this alarm will subsequently change to **Unconfirmed**.

7.6.2 Clearing Alarms Manually

When the device failures are eliminated, the alarms will be cleared automatically. If the alarms cannot be cleared automatically, you can remove them manually.

Procedure

1. See [Viewing current alarms](#) or [View alarm logs](#). for opening the **Current Alarm** or **Alarm Log** tab.

2. Select one or more alarms and right-click to select **Clear Alarm**, or click **Clear Alarm** at the lower right corner of the tab. The **Clear Status** of the corresponding alarm changes to **User Clearance**.

7.6.3 Confirming and Clearing Alarms

When a device is faulty, you can confirm and clear alarms with one click.

Procedure

1. Select **System**→**Parameter Settings**→**Alarm Settings**→**Server Settings**→**Alarm Basic Setting** from the main menu.
2. In the **Alarm Basic Setting** dialog box, select **Show Confirming and Clearing Alarm Function**.
3. See [Viewing current alarms](#) or [View alarm logs](#). for opening the **Current Alarm** or **Alarm Log** tab.
4. Select the corresponding alarm and click **Confirm Alarm** in the lower right part of the tab or right-click the corresponding alarm and select **Confirm and Clear Alarm**.

7.6.4 Locating Alarms

This function enables you to locate the topological object, ONU list, card or port that generates this alarm.

Procedure

1. Refer to [Viewing current alarms](#), [Viewing Alarm History](#) or [View alarm logs](#). to open the **Current Alarm**, **Alarm History** or **Alarm Log** tab.
2. Right-click the corresponding alarm and select **Topology Location / Locate to Card or Port / Locate to ONU List**.

7.6.5 Shielding Alarms

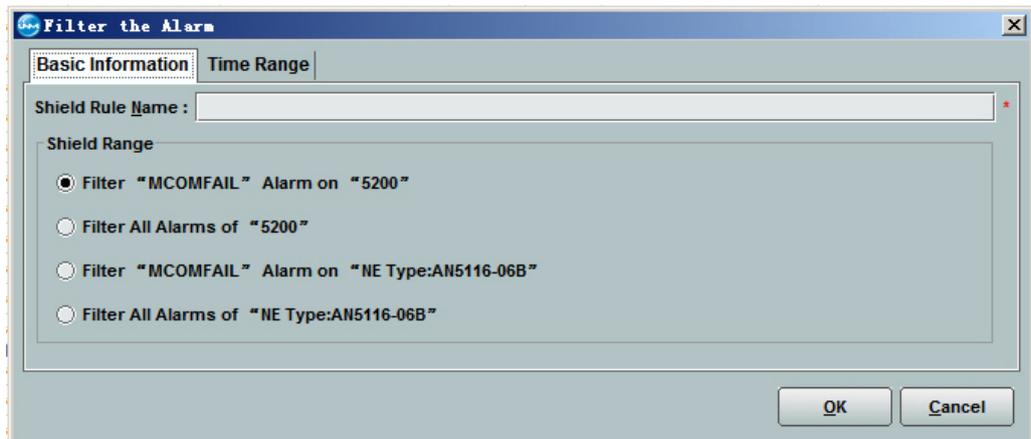
The following introduces how to shield a certain alarm in the current alarm query GUI. When some alarms do not need to be handled, you can filter these alarms.

Background Information

- ◆ The filter rules do not apply to the alarms already reported. They are only applicable to the matching alarms reported after the filter rules are set.
- ◆ The filtered alarms are neither in the alarm database nor displayed.

Procedure

1. See [Viewing current alarms](#) for opening the **Current Alarm** tab.
2. Right-click the corresponding alarm and select **Filter**.
3. In the **Filter Alarm** dialog box, set the filter rules.



4. Click **OK** to add an alarm filter rule and filter the current alarm in specific condition.



Note:

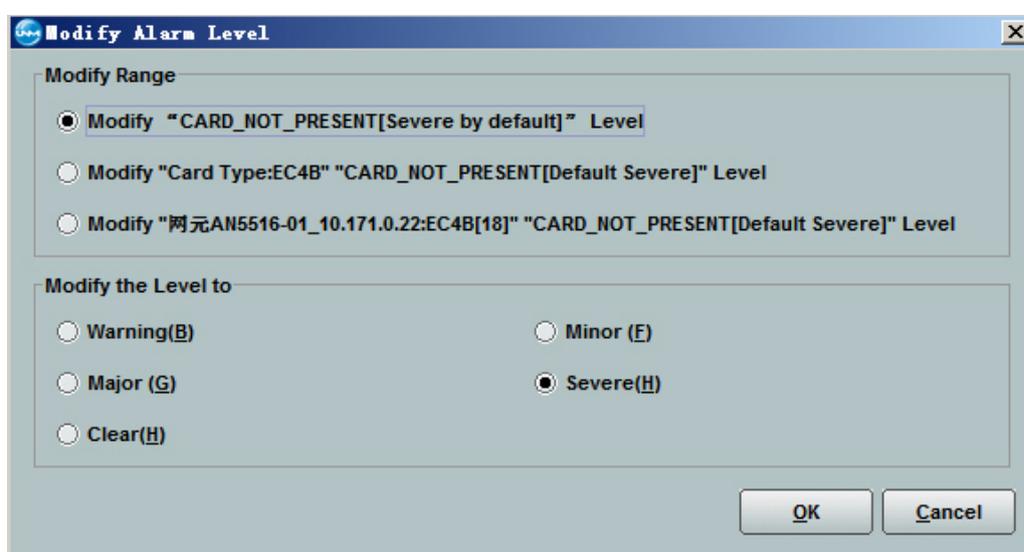
- ◆ The newly added alarm filter rules can be viewed in the **Alarm Shield Rule Management** tab.
- ◆ To cancel the alarm filter settings, clear the **Enable** option or delete the corresponding filter rules. See [Viewing Alarm Filter Rules](#).

7.6.6 Modifying Alarm Levels

You can set the alarm level for the UNM2000 alarms to improve the alarm monitoring efficiency.

Procedure

1. See [Viewing current alarms](#) for opening the **Current Alarm** tab.
2. Right-click the corresponding alarm and select **Modify the Level**.
3. In the **Modify Alarm Level** dialog box, set the parameters in **Modify Range** and **Modify the Level to**.



4. Click **OK**.

7.6.7 Editing Alarm Remarks

You can edit the alarm remarks to record additional information about the alarm for maintenance.

Procedure

1. See [Viewing current alarms](#) for opening the **Current Alarm** tab.
2. Right-click the corresponding alarm and select **Modify the Remark**.
3. In the **Edit Alarm Remark** dialog box, enter the alarm remarks.

4. Click **OK**. You can view the entered alarm remark in the **Remark** column of the corresponding alarm.

7.6.8 Exporting the Alarm Information

This section introduces how to print or export the alarm information.

Procedure

1. Refer to [Viewing current alarms](#), [Viewing Alarm History](#) or [View alarm logs](#). to open the **Current Alarm**, **Alarm History** or **Alarm Log** tab.
2. Export the alarm Information.
 - ▶ Print alarms.
 - a) Select the alarm information entry and right-click to select **Print**.
 - b) In the **Print Preview** dialog box, set the page setup and other print options.
 - c) Click **Print** and select printer and other printing settings in the displayed **Print** dialog box.
 - d) Click **OK**.
 - ▶ Export alarms.
 - Export all alarm entries. Right-click anywhere in the tab and select **Export**→**Export All Records**to export all the alarm entries in format of TXT, Excel, CSV, XML, PDF or HTML.
 - Export the selected alarm entry. Select the alarm entry and right-click to select **Export**→**Export Selected Record** to export the selected alarm entries in format of TXT, Excel, CSV, XML, PDF or HTML.

7.6.9 Editing Alarm Maintenance Experience

By recording the alarm maintenance experience, you can handle the alarms of the same type quickly and conveniently.

Procedure

1. See [Viewing current alarms](#) for opening the **Current Alarm** tab.
2. Right-click the corresponding alarm and select **Maintenance Experience**.
3. In the **Edit Maintenance Experience** dialog box, select the applicable range, enter the maintenance experience and click **OK**.



Note:

The recorded maintenance experience can be viewed in the corresponding detailed alarm information. Besides, you can manage the maintenance according to [Managing Maintenance Experience](#).

7.6.10 Managing Maintenance Experience

By managing the maintenance experience, you can refer to the maintenance experience for handling the alarms of the same type.

Procedure

1. Select **Alarm** → **Setting** → **Alarm Maintenance Experience Management** from the main menu.
2. View the alarm maintenance experience in the **Alarm Maintenance Experience Management** tab.
3. Do as follows:
 - ▶ In the right pane, click the button at the lower right part of the corresponding entry, or right-click the entry, and select operations such as **Edit**, **Delete**, **Copy Cell**, **Print** or **Export**.
 - ▶ Filter the maintenance experience entries. Click  at the top of the left pane to switch the tree structure and sort alarms by alarm name or type. Then click the tree node to filter the maintenance experience entries in the right pane.
 - ▶ Click the **Import / Export** data in the table on the right button at the top of the right pane to import / export the maintenance experience in the XML format.

- ▶ If no corresponding maintenance experience exists in the maintenance experience library, users can create the new maintenance experience according to step 4.
4. Create the maintenance experience.
 - 1) In the right pane of the **Alarm Maintenance Experience Management** tab, click **New**, or right-click in the blank area and select **Add** from the shortcut menu.
 - 2) In the **New Alarm Maintenance Experience** dialog box, set **Equipment Type**, **Alarm Name**, enter the maintenance experience information and click **OK**.

7.7 Customizing Alarms

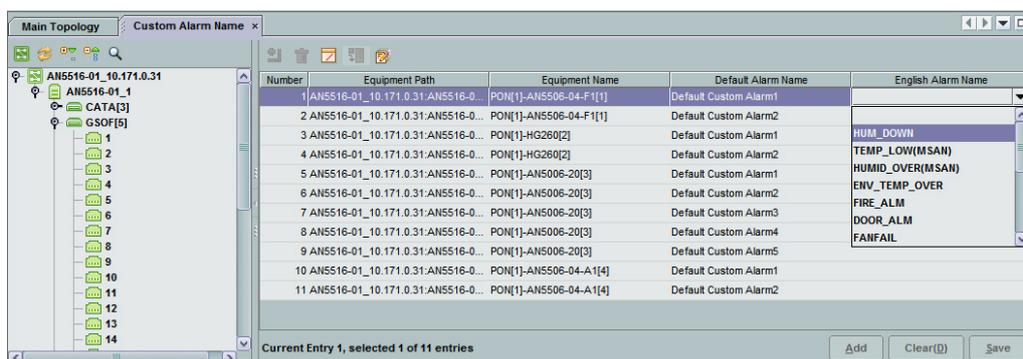
Customize the alarm names or levels according to the maintenance requirements for convenient management and efficient alarm monitoring.

7.7.1 Custom Alarm Name

To obtain the physical environment information of the equipment, you can customize the environmental alarms of the equipment, such as the fire alarm, the water alarm, and the too high / too low temperature alarm.

Procedure

1. Select **Alarm** → **Custom Alarm Name** from the main menu.
2. In the **Please Select a NE** dialog box, select the NE whose alarms are to be customized and click **OK**.
3. In the left pane of the **Custom Alarm Name** tab, select the PUBA card or ONU whose alarms are to be customized, click the **English Alarm Name** column and select the corresponding name.



4. Click **Save** to save the settings to the database.

Other Operations

- ◆ Clear the customized alarm: Select the row containing the customized alarm and click **Clear** to clear the customized alarm information. Then click **Save**.
- ◆ Define the alarm for the same object quickly: Click **Apply to Object of the Same Type** to make it valid and apply the changes to the cards of the same type.
- ◆ Display / hide the undefined alarm: Click **Display Undefined Alarm / Hide Undefined Alarm** to display or hide the alarms not defined on the GUI.
- ◆ Set the defined alarm row by row: Click **Hide Undefined Alarm**, click **Add** to set the alarm name, and click **Save**.

7.7.2 Custom Alarm Level

You can adjust the alarm levels of all objects, the designated types of equipment, or the designated equipment as required.

Procedure

1. Select **Alarm** → **Setting** → **Custom Alarm Level** from the main menu.
2. At the lower right corner of the **Customize Alarm Level** tab, click **Create**; or right-click in the blank area of the tab, and select **Create**.
3. In the **New Customized Rule of the Alarm Level** dialog box, set **Alarm Source**.

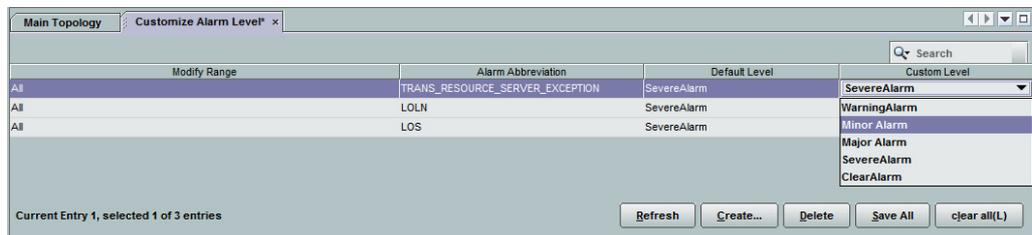
- ▶ Select **All Objects**, and the customized alarm levels apply to all objects.
- ▶ Select **Select Equipment**, click  on the right of **Object Name** and select the card of a certain device in the **Select Object** dialog box. Then click **OK**.
- ▶ Select **Select Equipment Type** and click  after Equipment Type and select a certain equipment type in the **Select Equipment Type** dialog box. Then click **OK**.



Note:

The priorities of custom alarm levels are as follows: equipment > equipment type > all objects.

4. Click **Select** to select the desired alarms in the **Select Alarm Name** dialog box, and click **OK**.
5. Click the **Custom Level** column of the corresponding alarm, and select the desired alarm level. Then click **OK**.



6. In the **Customize Alarm Level** tab, check the information related to the custom alarm levels, and click **Save All**.

Other Operations

- ◆ Delete the custom alarm level: In the **Customize Alarm Level** tab, select the desired alarm level and click **Delete**.
- ◆ Modify the custom alarm level: In the **Customize Alarm Level** tab, click the **Custom Level** column of the corresponding alarm entry to reset the alarm level. Then click **Save All**.

7.8 Alarm / Event Remote Notification

By setting the alarm / event remote notification parameters (such as rules and format), the UNM2000 sends the alarm / event information matching the conditions to the maintainers via email or SMS so that they can obtain the alarm / event information on the device and on the UNM2000 server timely even if they are not on site.

7.8.1 Setting the Notification Communication Parameters

To send the remote email or SMS notification through the UNM2000, you need to set the email notification parameters and SMS center relevant parameters.

Background Information

For setting the IP address, port, username, password and encoding protocol of the SMS center, please contact the SMS center.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. In the left pane, select **Alarm Settings**→**Server Settings**→**Remote Notification Settings**→**Communication Parameters** to open the dialog box.
3. Set the parameters in the **Email Notification**, **GSM Modem Settings** and **ISMG Settings** tabs respectively, and then click **Apply** to validate the settings.

7.8.2 Setting the Remote Notification Format of the Alarm / Event

You can set the remote notification format of the alarm / event, including setting the email subject and contents of the mail notification.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.

2. In the left pane, select **Alarm Settings**→**Server Settings**→**Remote Notification Settings**→**Message Format** to open the **Message Format** window.
3. Set the remote notification message format.
 - ▶ In the **Email Notification** tab, click the **Select the Field** buttons in the **Title** and **Content** panes respectively to select the subject and contents of the mail to be sent.
 - ▶ Select the **SMS Notification** tab, and click the **Select the Field** button to select the contents to be sent.
4. Click **Apply** after the settings are completed, and the settings will be valid.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the values set last time in case of setting error.

7.8.3 Setting the Remote Notification Sending Rules of the Alarm / Event

By setting the alarm / event remote notification rules (including the receiver information, notification conditions, alarm sources, and time limit), the alarms meeting the rules will be sent to the maintenance personnel so that they can obtain the alarm information timely even if they are not on site.

Prerequisite

The parameters such as communication parameters, short message format and sending delay have been set.

Procedure

1. Select AlarmSettingAlarm Notification Settings from the main menu.
2. Execute the following operations as needed.
 - ▶ In the right pane, click the button at the lower part of the corresponding entry, or right-click the entry, and select operations such as **Disable/Enable**, **Delete**, **Copy Cell**, **Print** or **Export**.

- ▶ In the left pane, select the corresponding receiver, modify the relevant information if necessary in the right pane. Click **Save All**.
 - ▶ If the current alarm / event remote notification rules cannot meet the requirements, you can create rules according to Step 3.
3. Add an alarm or event remote notification rule.
 - 1) Select one of the following methods to open the **Create Alarm Remote Notification Rule** dialog box.
 - Select **Recipient Info** in the left pane, and click **Create Receiver Information** in the right pane.
 - Select **Recipient Info** in the left pane, right-click in the right pane, and select **Create Receiver Information** from the shortcut menu.
 - Right-click **Recipient Info** in the left pane, and select **Create Receiver Information** from the shortcut menu.
 - 2) Set the related information such as the recipient information, notification conditions, alarm sources, and time limit as required.
 - 3) After the setting is completed, click **OK**.

7.8.4 Setting the Sending Delay of the Alarm / Event Remote Notification

Set the delayed duration to send the remote notification upon the occurrence of the alarm / event. If the alarm is still not cleared after the duration, the remote notification will be sent; otherwise, it will not be sent.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. In the left pane, select **Alarm Settings**→**Server Settings**→**Remote Notification Settings**→**Sending Delay** to open the dialog box.

Sending Delay

If an alarm occurs, the alarm auto notification rule sends a notification only when the alarm is not cleared in the specified time period.

Alarm Delay Settings

NE Type: Search

Select	No.	Name	Level	Alarm Forward Time ...
<input type="checkbox"/>	1	SPI_LOS	● Critical	10
<input type="checkbox"/>	2	PPI_TF	● Critical	10
<input type="checkbox"/>	3	PPI_LOS	● Critical	10
<input checked="" type="checkbox"/>	4	PPI_AIS	● Minor	10
<input type="checkbox"/>	5	LIS	● Critical	10
<input type="checkbox"/>	6	MS_SD	● Minor	10
<input type="checkbox"/>	7	HP_RDI	● Minor	10
<input type="checkbox"/>	8	HP_RDI_S	● Minor	10
<input type="checkbox"/>	9	HP_RDI_C	● Minor	10
<input type="checkbox"/>	10	PJE_LIMIT	● Warning	10
<input type="checkbox"/>	11	FANALM	● Minor	10
<input type="checkbox"/>	12	FANIND	● Warning	10

Select All / Clear None Select All/Clear the Selected Rows

- Select the NE types and alarm codes needing transmission delay. Users can isolate the target alarm codes rapidly via the searching function.



Note:

- ◆ If an alarm is not set here, the system will send the corresponding remote notification immediately after this alarm occurs without delay.
 - ◆ You can modify the delay time interval of a certain alarm as required.
- Click **Set the Alarm Delay Time**.
 - Set the alarm delay time interval and then click **Apply**. Update the **Alarm Forward Time** of the selected alarm code to the new values set.
 - Click **Apply** after the settings are completed, and the settings will be valid.

7.8.5 Sending Alarm / Event Remote Notification

The maintainer of the local equipment room, by analyzing and editing the current alarms / events of different stations through the UNM2000 client, send the alarms / events of different areas or stations to the maintainer whose is nearest to the failure location according to the distribution of maintainers. By this way, the alarms / events can be quickly processed, improving the device maintenance efficiency.

Prerequisite

- ◆ The parameters and rules of the alarm / event remote sending are set.
- ◆ You have the authority of **Operator Group** or higher authority.

Procedure

1. Right-click the NE in the main topology, and select **Current Alarm** from the shortcut menu.
2. In the **Current Alarm** dialog box, right-click an alarm entry and select **Remote Notification**→**Email/Message** to open the **Send a Mail to Notify** or **Notify via SMS** dialog box.
3. Select **Receiver**, enter the **Title** and **Content**, and then click **OK**.

7.9 Managing the Alarm / Event Data

If the alarm history data stored in the UNM2000 exceeds the threshold, the UNM2000 operation will be influenced. The alarm data saving function can save the alarm history data in the UNM2000 as files to the designated file folder, so as to improve the UNM2000 operation performance. The UNM2000 supports manual saving and overflow saving.

- ◆ **Overflow saving:** You can set the maximum alarm saving capacity and the UNM2000 will regularly check the alarm history data. When the alarm history data reach the preset capacity, the UNM2000 will save the data to a specified file to decrease its load.

- ◆ **Manual saving:** You can save the alarm history data in the UNM2000 to a specified file folder manually at anytime. You can set the manual saving period. When the alarm history data saved in the database reach the preset time period, the UNM2000 will save the data to a designated file folder. You can mark the saving time in the name of the folder where the file is saved.

7.9.1 Setting the Alarm / Event Overflow Saving

Set the alarm / event overflow saving task. The UNM2000 regularly checks whether the alarm / event history data in the database meets the preset conditions. If the overflow saving conditions are met, the UNM2000 saves the alarm / event history data automatically. The saved alarm / event history data will be deleted from the database.

Background Information

The UNM2000 provides the default overflow saving tasks of history data, which cannot be deleted. You can modify the overflow saving conditions of the corresponding task as needed.

Procedure

1. Select **System**→**Save Data** to open the **Save the Data** tab.
2. Select **Save History Data**→**Overflow Saving**→**Historical Overflow Save** from the left pane to view the existing historical data overflow save task.
3. Select any one access method from the table below to open the **Attribute** dialog box of the corresponding historical data saving task.
 - ▶ Double-click the corresponding overflow saving task in the right pane.
 - ▶ Right-click the corresponding overflow saving task in the right pane and select **Attribute**.
 - ▶ In the left pane, click  on the left side of Overflow Saving, and right-click the corresponding overflow saving task to select **Attribute**.

The screenshot shows a 'Property' dialog box with two tabs: 'Basic information' and 'Extend information'. The 'Basic information' tab is selected. The 'Task name' field contains 'Save Operation Log Overflow'. Below it is an 'Enable' checkbox which is checked. The 'Task Type' section has three radio buttons: 'One time', 'Every', and 'Every week'. 'Every week' is selected. To the right of 'Every' is a spinner box showing '1' and the text 'day(s)'. Below 'Every week' is a dropdown menu showing 'Monday' and a button with three dots. To the right of this is another dropdown menu with three dots. The 'Execution time' field contains '00:00:00'. The 'Start time' field contains '2013-08-08 17:43:30'. The 'End time' field is checked and contains '2017-10-23 10:16:11'. At the bottom right are 'OK' and 'Cancel' buttons.

4. Set the attribute of the overflow saving task, referring to Table 7-5.

Table 7-5 Descriptions of the Alarm / Event Overflow Saving Task Settings

Parameter		Description
Basic Information	Task Name	The name of the overflow saving task, which cannot be edited by users.
	Enable	Select it to enable the task.
	Task Type	Sets the execution cycle of the task. The default value is Every 2 days .
	Execution Time	Sets the execution time of the task.
	Start Time	Sets the start time of the task.
	End Time	Sets the end time of the task.
Extended information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the data history that meets the overflow saving conditions into files. You can convert the data history into CSV files and save them into the sever haddisk or into the FTP server. ◆ Select Delete Directly to delete the data history that meets the overflow saving conditions directly.
	Overflow Limit	If the data history exceeds the maximum saving entry number or exceeds the record threshold, a pre-set proportion of the database will be saved.
	Capacity Limit	The data history that exceeds the reserving days of the database will be saved during the saving task.

5. Click **OK**.
6. Select the corresponding overflow saving task in the left pane and click **Execute Now** in the upper right pane. View the execution result in the bottom right pane.

7.9.2 Setting the Manual Alarm / Event Saving

The UNM2000 supports saving alarm history and performance history manually, preventing insufficient space in database.

Background Information

The UNM2000 provides the default manual saving tasks of alarm history / events, which cannot be deleted. You can modify the parameters of the corresponding saving task as needed.



Note:

The name of the manually saved file can be marked with the saving time. You can turn on the switch to mark the saving time in the name of the saved file by modifying the background configuration file. For specific operations, contact the FiberHome technical engineer.

Procedure

1. Select **System**→**Save Data** from the main menu to open the **Save Data** tab.
2. Select **Save History Data**→**Save Manually**→**Alarm History** from the left pane to view the existing manual saving task of alarm history.
3. Select any one access method from the table below to open the **Attribute** dialog box of the corresponding manual historical data saving task.
 - ▶ Double-click the corresponding manual saving task in the right pane.
 - ▶ Right-click the corresponding manual saving task in the right pane and select **Attribute**.
 - ▶ In the left pane, click  on the left side of **Save Manually**, and right-click the corresponding manual saving task to select **Attribute**.

- Set the attribute of the overflow saving task, referring to Table 7-6.

Table 7-6 Descriptions of the Alarm / Event Overflow Saving Task Settings

Parameter		Description
Parameter		Description
Basic Information	Task Name	The name of the saving task, which cannot be edited by users.
	Enable	Select it to enable the task.
	Task Type	Sets the execution cycle of the task.
Extended Information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the data history that meets the overflow saving conditions into files. You can convert the data history into CSV files and save them into the sever harddisk or into the FTP server. ◆ Select Delete Directly to delete the data history that meets the overflow saving conditions directly.
	Data Generation Time	Sets the generation time and end time of the data.
	Selecting the Object	Sets the range of the object to be exported.
	Records that Matched the Saving Conditions	Displays the number of the data entries that comply with the saving conditions. This item cannot be edited.

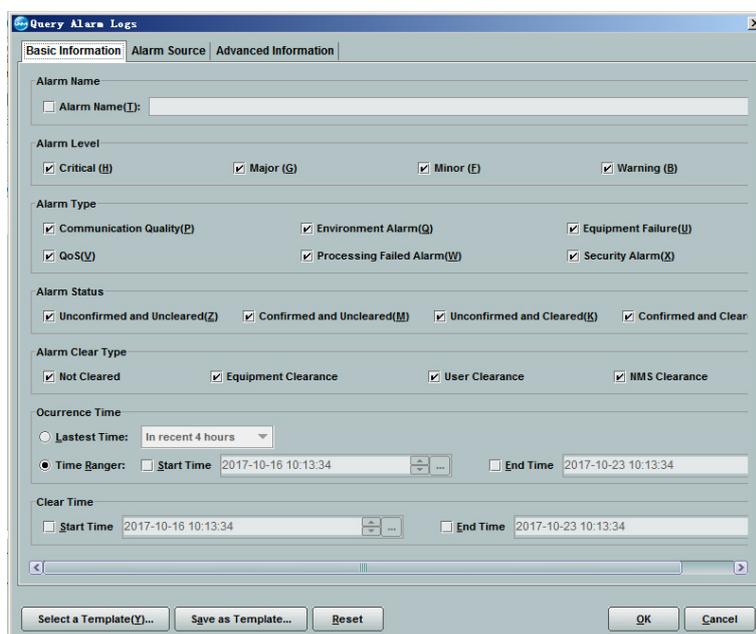
- Select the corresponding manual saving task in the left pane and click **Execute Now** in the upper right pane. View the execution result in the bottom right pane.

7.10 Alarm Logs

The **Alarm Log** function supports querying alarm logs, collecting statistics on alarm history logs and current alarm logs. You can set the statistical conditions as needed to query the statistical result of alarm logs.

Query Alarm Log

- Select **Alarm**→**Alarm Log**→**Query Alarm Log** from the main menu.
- Set the query conditions according to the query requirements.



Note:

- ◆ Click **Select a Template** to select the alarm log query template.
- ◆ Click **Save as Template** to save the query conditions already set as an alarm log query template.

3. Click **OK**. The **Alarm Log** tab lists the query result.

Collecting Statistics of Alarm History Logs

1. Select **Alarm** → **Alarm Log** → **Alarm History Log Statistics** from the main menu.
2. Set the conditions for querying alarm history logs according to the statistical requirements.

Alarm Type/Date	1st	2nd	3rd	4th
TRANS_RESOURCE_SERVER_EXCEPT...	1	0	2	3
LOLN	4	1	3	0
LOUP	0	3	2	3
LOS_UP	1	2	2	3
LOS	1	2	4	2
PORT_LOF	0	2	2	4
MATRIX UNAVAILABLE	3	3	3	2
LPR	4	2	1	1
LCD	3	3	0	4
TEMP_LIMIT_ALARM	2	3	1	2



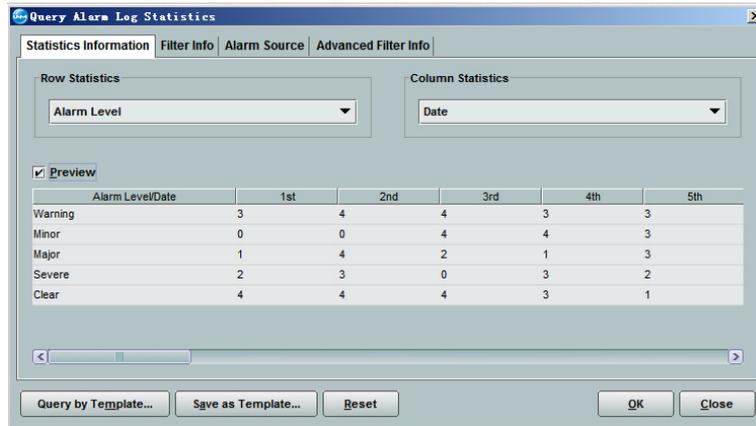
Note:

- ◆ Click **Query by Template** to select the statistical template of alarm history logs.
- ◆ Click **Save as Template** to save the query conditions already set as an statistical template of alarm history logs.

3. Click **OK**. The **History Alarm Log Statistics** tab lists the query result.

Collecting Statistics of Current Alarm Logs

1. Select **Alarm**→**Alarm Log**→**Current Alarm Log Statistics** from the main menu.
2. Set the conditions for querying current alarm logs according to the statistical requirements.



Note:

- ◆ Click **Query by Template** to select the statistical template of alarm history logs.
- ◆ Click **Save as Template** to save the query conditions already set as an statistical template of alarm history logs.

3. Click **OK**. The **Current Alarm Log Statistics** tab lists the query result.

7.11 Managing Alarm Frequency Analysis Rules

For alarms with a large quantity but little impact in current networks (such as ONU fiber cut alarm, power disconnection alarm and MGC link alarm), you can set the alarm frequency analysis rules and set **Handling Strategy** and **Triggering Conditions** for different alarms. The UNM2000 will filter the alarms or generate new alarms based on the rules.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. On the UNM2000 main menu, select **Alarm**→**Setting**→**Alarm Frequency Analysis Rule** to open the **Alarm Frequency Analysis Rule** tab.

2. In the **Alarm Frequency Analysis Rule** tab, select **Add** to open the **Object** dialog box.
3. In the **Basic Information** tab of the **Object** dialog box, select **Alarm Name** and set **Handling Strategy** and **Triggering Conditions**.
4. In the **Object** dialog box, select the **Object Source** tab to set the applicable objects of the alarm frequency analysis rule.
5. Select the created alarm frequency analysis rule, click **Enable** to enable the rule.

8 Performance Management

The UNM2000 performs strong performance management functions. By monitoring the performance, you can detect the silent failures during network running to prevent network failures.

- Basic Concepts
- Managing Performance Query Templates
- Setting the Performance Collection Time
- Configuring the Performance Classification Switch in a Batch Manner
- Managing the Card Performance
- Managing Performance Collection
- Managing Performance Data
- Managing Statistics Export Task

8.1 Basic Concepts

With the performance management function, you can detect the silent failure of network running to avoid network failure risks. You need to grasp the relevant basic concepts before performing the performance monitoring operation.

Current Performance and Performance History

The performance data includes the current performance data and performance history data. You can check whether the service is running normally in a specified time period by browsing the performance data.

◆ Current Performance

The current performance refers to the data saved in the current performance register of the NE. The current performance data can be divided into 15-minute current performance and 24-hour current performance in terms of monitoring period. When browsing the current performance, the UNM2000 will query the performance data directly from the current performance register at the NE side.

◆ Performance History

The performance history refers to the performance data of NEs detected in the past specified time period. When querying the performance history data, you can select whether to query the performance history data at the NE side or at the UNM2000 side according to the location where the data are stored.

The current performance data whose saved time exceeds the specified time period will be saved to the NE performance history register.

Performance Threshold

By setting the performance threshold, you can filter the performance events that change in the normal value range so that you can focus the critical performance events.

The threshold is also called tolerance, which indicates the performance value that meets the requirements for normal running of the device. If a certain performance indicator exceeds the preset performance threshold, the performance degradation trend has reached the degree that needs to be focused. Generally, it is recommended to reserve a certain value margin when setting the performance threshold so as to detect anomalies in advance.

Performance Saving

The performance saving function can save the performance history data in the UNM2000 as files to the designated file folder, so as to improve the UNM2000 operation performance.

Performance Comparison

You can compare the performance data of the specified object in different time periods to view the corresponding running status.

8.2 Managing Performance Query Templates

The UNM2000 supports setting the performance query conditions or statistical conditions as templates. You can use the preset template to quickly query the performance data.

8.2.1 Viewing Performance Templates

The following introduces how to view the performance template.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Performance**→**Performance Query Template** to open the **Performance Query Template Management** tab.
2. Click  before **Performance History Query Template** to select the corresponding template and view the details of the template in the right pane.

8.2.2 Creating a Performance Query Template

To avoid setting conditions every time upon query, you can set the commonly used performance query conditions as a template so that you can use it next time. The following introduces how to create a performance query template.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Performance** → **Performance Query Template** to open the **Performance Query Template Management** tab.
2. Select one of the following access methods to open the **New Performance Query Template** dialog box.

No.	Access Method
1	In the Performance History Query Template tab, click  at the upper left corner.
2	Select Performance History Query Template in the left pane, right-click in the blank area of the right pane and select New Performance History Query Template from the shortcut menu.
3	Right-click Performance History Query Template in the left pane and select New Performance History Query Template from the shortcut menu.

3. In the **Performance History Query Template** dialog box, set **Template Information**, **Basic Information** and **Advanced Information** tabs.



Note:

Click **Copy from Other Performance Query Template**, select the template in the **Select Template** dialog box, and copy the basic information and advanced information of the selected template, improving the setting efficiency.

4. Click **OK**.

Other Operations

In the right pane, click the button at the lower part of the corresponding entry, or right-click the entry, and select operations such as Delete, Refresh, Set as / Cancel Default Template, Copy Cell, Print or Export.

8.2.3 Modifying a Performance Query Template

When setting the performance query template, you can modify the settings in case the query condition setting error occurs.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the main menu, select **Performance**→**Performance Query Template** to open the **Performance Query Template Management** tab.
2. Click  before **Performance History Query Template** to select the corresponding template in the left pane and view the details of the template in the right pane.
3. Modify the settings of the template in the right pane as needed and click **Save All**.

Other Operations

In the right pane, click the button at the lower part of the corresponding entry, or right-click the entry, and select operations such as Delete, Refresh, Set as / Cancel Default Template, Copy Cell, Print or Export.

8.3 Setting the Performance Collection Time

You can set the collection time of the 24-hour performance as required.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.

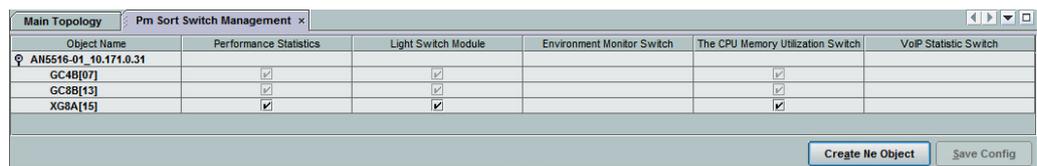
2. Select **Performance Settings**→**Server Settings** in the left pane to open the dialog box.
3. Set the 24-hour performance collection time and then click **Apply** to apply the settings.

8.4 Configuring the Performance Classification Switch in a Batch Manner

The UNM2000 is added with the new function of **Performance Classification Switch Configuration**. You can view the performance switch of the designated OLT NE and modify the existing switches in a batch manner via the UNM2000, as well as deliver the configurations to the device.

Procedure

1. On the UNM2000 main menu, select **Performance**→**Performance Switch Config** to open the **Pm Sort Switch Management** tab.
2. Click **Create NE Object** to open the **Add Object** dialog box and then select one or multiple NEs.
3. Click **OK**. The UNM2000 reads the performance classification switch status of the selected device.



Object Name	Performance Statistics	Light Switch Module	Environment Monitor Switch	The CPU Memory Utilization Switch	VoP Statistic Switch
♀ AN5516-01_10.171.0.31					
GC4B[07]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
GC3B[13]	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	
XG8A[15]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	

4. Modify the performance classification switches in a batch manner and then click **Save Config**.

8.5 Managing the Card Performance

This section introduces how to manage the card performance, including viewing the current performance, performance history, performance comparison, real-time performance and performance history trend.

- ◆ **Current performance:** Views the current 15-minute performance and the performance of the latest sixteen 15-minute time intervals. These data are not saved in the database.
- ◆ **Performance history:** Views the performance history data of the selected object in the designated time range.
- ◆ **Real-time performance:** Views the real-time performance data of the selected object. The collection period can be 10 seconds or 30 seconds; the collection interval can be 15 minutes, 30 minutes, one hour, or 24 hours.
- ◆ **Performance comparison:** Compares the performance data in designated period of an designated object, so as to understand the operating status of this object in different periods.
- ◆ **Performance history trend:** Views the change trend of the performance history data of the designated object.

8.5.1 Viewing the Current Performance

You can query the current performance so as to understand the running status of devices.

Prerequisite

- ◆ The performance classification function of the corresponding device is **Enabled**.
- ◆ You have the authority of **Operator Group** or higher authority.

Procedure

1. Right-click a desired NE from the object tree on the left side of the **Main Topology** tab, or in the physical topology view on the right side. Select **Open NE Manager** from the shortcut menu.
2. Select one of the following ways to view the current performance.
 - ▶ In the **Device Tree** pane of the **NE Manager** window, right-click a card or port, and select **Current Performance** from the shortcut menu.
 - ▶ In **Subrack View** of the **NE Manager** window, right-click a card, and select **Current Performance** from the shortcut menu.

Number	Object Name	Performance Group	Performance Code Type	Performance Code	English Performan...	Performance Value	Unit	Begin Time
1	PON2	Packet Counters	XTU-C RXOCTETS	XTU-C RXOCTETS	XTU-C RXOCTETS	0	Bytes	2017-10-23 16:00:05
2	PON2	Packet Counters	UPTotalFrame	UPTotalFrame	UPTotalFrame	0	Packets	2017-10-23 16:00:05
3	PON2	Packet Counters	UP UnicastFrames	UP UnicastFrames	UP UnicastFrames	0	Packets	2017-10-23 16:00:05
4	PON2	Packet Counters	UPMulticastFrames	UPMulticastFrames	UPMulticastFrames	0	Packets	2017-10-23 16:00:05
5	PON2	Packet Counters	UPBroadcastFrames	UPBroadcastFrames	UPBroadcastFram...	0	Packets	2017-10-23 16:00:05
6	PON2	Packet Counters	UPUndersizeFrames	UPUndersizeFrames	UPUndersizeFram...	0	Packets	2017-10-23 16:00:05
7	PON2	Packet Counters	UPOversizeFrames	UPOversizeFrames	UPOversizeFrames	0	Packets	2017-10-23 16:00:05
8	PON2	Error Frame Count...	UPCRC-32Errors	UPCRC-32Errors	UPCRC-32Errors	0	Packets	2017-10-23 16:00:05
9	PON2	Manage Packet C...	UPMPCP	UPMPCP	UPMPCP	0	Packets	2017-10-23 16:00:05
10	PON2	Manage Packet C...	UPOAM	UPOAM	UPOAM	0	Packets	2017-10-23 16:00:05
11	PON2	Packet Counters	UPFramesDropped	UPFramesDropped	UPFramesDropped	0	Packets	2017-10-23 16:00:05
12	PON2	Packet Counters	XTU-R RXOCTETS	XTU-R RXOCTETS	XTU-R RXOCTETS	109507	Bytes	2017-10-23 16:00:05
13	PON2	Packet Counters	DownTotalFrame	DownTotalFrame	DownTotalFrame	1304	Packets	2017-10-23 16:00:05
14	PON2	Packet Counters	DownUnicastFrames	DownUnicastFrames	DownUnicastFra...	1	Packets	2017-10-23 16:00:05
15	PON2	Packet Counters	DownMulticastFrames	DownMulticastFrames	DownMulticastFra...	115	Packets	2017-10-23 16:00:05
16	PON2	Packet Counters	DownBroadcastFrames	DownBroadcastFrames	DownBroadcastF...	1188	Packets	2017-10-23 16:00:05
17	PON2	Manage Packet C...	DownMPCP	DownMPCP	DownMPCP	43	Packets	2017-10-23 16:00:05
18	PON2	Manage Packet C...	DownOAM	DownOAM	DownOAM	21	Packets	2017-10-23 16:00:05
19	PON2	Packet Counters	DOWN_LOST_FRAMES	DOWN_LOST_FRAMES	DOWN_LOST_FR...	0	Packets	2017-10-23 16:00:05
20	PON2	Error Frame Count...	DownCRC-32Errors	DownCRC-32Errors	DownCRC-32Errors	0	Packets	2017-10-23 16:00:05
21	PON2	Error Frame Count...	DownOversizeFrames	DownOversizeFrames	DownOversizeFr...	0	Packets	2017-10-23 16:00:05
22	PON2	Error Frame Count...	DownUndersizeFrames	DownUndersizeFrames	DownUndersizeFr...	0	Packets	2017-10-23 16:00:05
23	PON2	Traffic Analysis	DROPPED_PKTS_PRO...	DROPPED_PKTS_PRO...	DROPPED_PKTS_...	0	%	2017-10-23 16:00:05

3. In the **15 Minutes** drop-down box, select the corresponding item to query the first to sixteenth 15-minute performance of the object.
4. (Optional) Right-click in the current performance tab and select **Print, Copy Cell** or **Export**.

Subsequent Operation

Set the query conditions for current performance and then query again.

1. Click **Query** to display the **Current Performance Query** dialog box.
2. In the **Current Performance Query** dialog box, set **Select the 15-minute Performance, Performance Code Type, Object** and **Performance Code**, and then click **OK**.

8.5.2 Viewing Performance History

View the performance history to obtain the abnormal performance data of the equipment, so as to instruct the current maintenance.

Prerequisite

- ◆ The performance classification function of the corresponding device is **Enabled**.
- ◆ The performance collection scheme has been set, and the system has waited for one test period (15 minutes or 24 hours) at least.
- ◆ You have the authority of **Operator Group** or higher authority.

Procedure

1. Select the access method mentioned in Table 8-1 to open the **Performance History Query** dialog box.

Table 8-1 Access Method of Viewing the Performance History

Operation	Access Method
Viewing the performance history	Select Performance → History Performance from the main menu.
	Right-click the corresponding NE in the object tree pane and select Performance History from the shortcut menu.
	In the Device Tree pane of the NE manager window, right-click the corresponding card or port and select Performance History from the shortcut menu.
	In the Diagram pane of the NE manager window, right-click the corresponding card and select Performance History from the shortcut menu.

2. Set the query conditions in the **Performance History Query** dialog box.



Note:

- ◆ In the **Advance Information** tab, you can select 10 query objects at most.
 - ◆ To avoid repeated setting of query conditions, you can click **Save as Template** to save the current performance history query conditions as a template, which can be selected for query by clicking **Query According to Template** later.
3. After completing the settings, click **OK**; then the query results will be displayed in the **Performance History** tab.

8.5.3 Viewing the Performance Comparison

You can compare the performance data of the specified object in different time periods to view the corresponding running status.

Prerequisite

- ◆ Wait until at least two measurement periods (15 minutes for each measurement period) expire above the list.
- ◆ The performance statistics function is enabled.
- ◆ You have the authority of **Operator Group** or higher authority.

Procedure

1. Right-click a desired NE from the object tree on the left side of the **Main Topology** tab, or in the physical topology view on the right side. Select **Open NE Manager** from the shortcut menu.
2. Select one of the following methods to open the **Performance Comparison Query** dialog box.
 - ▶ In the **Device Tree** pane of the **NE Manager** window, right-click a card or port, and select **Performance Comparison** from the shortcut menu.
 - ▶ In **Subrack View** of the **NE Manager** window, right-click a card, and select **Performance Comparison** from the shortcut menu.
3. In the **Performance Comparison Query** dialog box, set performance comparison query conditions.



Note:

Select at least two periods from the **15 Minutes** drop-down list.

4. Click **OK** and view the performance comparison result in the **Card Performance Comparison** tab.



Note:

The system displays the comparison result in **List View, Compare Based on the Object** and **Histogram** by default. You can select other display modes as needed.

Subsequent Operation

Click  or  at the top of the right pane to print the comparison results or export them in *.jpeg files and save them to a specified directory.

8.5.4 Viewing Real-time Performance

You can monitor performance data of the selected resources in real time.

Prerequisite

You have the authority of **Operator Group** or higher authority.

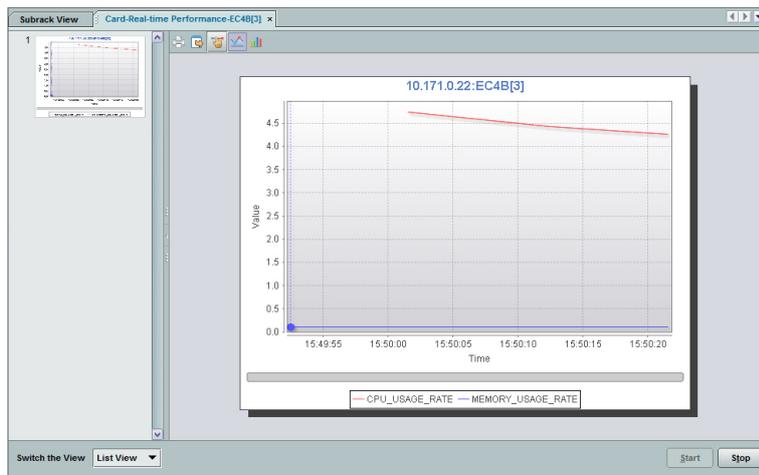
Procedure

1. Right-click a desired NE from the object tree on the left side of the **Main Topology** tab, or in the physical topology view on the right side. Select **Open NE Manager** from the shortcut menu.
2. Select one of the following methods to open the **Real-time Performance Query** dialog box.
 - ▶ In the **Device Tree** pane of the **NE Manager** window, right-click a card or port, and select **Real-time Performance** from the shortcut menu.
 - ▶ In **Subrack View** of the **NE Manager** window, right-click a card, and select **Real-time Performance** from the shortcut menu.
3. In the dialog box that appears, set **Collection Cycle, Time Length, Object** and **Performance Code**.
4. Click **OK**. After a while, you can view the real-time performance of the selected object in the **Real-time Performance** tab.



Note:

- ◆ The system displays the real-time performance in **List View** and **Curve Chart** by default. You can select other display modes as needed.
- ◆ Click **Stop** to stop collecting real-time performance.



Subsequent Operation

Click  or  at the top of the right pane to print real-time performance results or export them in *.jpeg files and save them to a specified directory.

8.5.5 View Performance History Trend

You can view the performance history charts so as to understand the performance data change trend of the specified object and the running status of the network.

Prerequisite

- ◆ The object to be queried has its performance history data.
- ◆ You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Performance** → **View Performance History Trend** from the main menu.

2. Set the query conditions in the **Performance History Query** dialog box.



Note:

- ◆ In the **Advance Information** tab, you can select 10 query objects at most.
- ◆ To avoid repeated setting of query conditions, you can click **Save as Template** to save the current performance history query conditions as a template, which can be selected for query by clicking **Query According to Template** later.

-
3. After completing the settings, click **OK**; then the query results will be displayed in the **History property trend** tab.



Note:

The system displays the performance history in the **List view** or **Curve Chart** mode by default. You can select other display modes as required.

Subsequent Operation

Click  or  at the top of the right pane to print real-time performance results or export them in *.jpeg files and save them to a specified directory.

8.6 Managing Performance Collection

You can use the scheduled performance collection to query or process the performance data of the NE. The UNM2000 enables you to collect the performance data through **NE Performance Indicator Collection** and **NE Performance Threshold Collection** and export the result as a file to reduce repeated work.

8.6.1 Managing Performance Indicator Sets

The following introduces how to view and set the performance indicator sets.

8.6.1.1 Viewing Performance Indicator Sets

View the existing performance indicator sets so as to quickly set the collection indicator of the performance collection task.

Prerequisite

- ◆ You have the authority of **Inspector Group** or higher authority.
- ◆ The NE time is synchronized with the EMS time.

Procedure

1. Select **Performance** → **Collection Task Management** from the main menu to open the **Collection Task Management** tab.
2. In the **Collection Task Management** tab, click **Indicator Set** and view the existing indicator sets in the right pane.
3. In the **Collection Task Management** tab, double-click the desired indicator set to view the details of the indicator set, including **Basic Information** and **Member**.

Subsequent Operation

- ◆ **Modify the indicator set**
In the left pane, select the corresponding indicator set, modify the relevant information if necessary in the right pane. Click **Save All**.
- ◆ **Other Operations**
In the right pane, select the corresponding entry and click the button at the bottom, or simply right-click the entry and select **Delete**, **Print**, **Copy Cell** or **Export** from the shortcut menu.

8.6.1.2 Creating a Performance Indicator Set

Set the performance indicator set so as to quickly set the collection indicator of the performance collection task.

Prerequisite

- ◆ You have the authority of **Inspector Group** or higher authority.
- ◆ The NE time is synchronized with the EMS time.

Procedure

1. Select **Performance**→**Collection Task Management** from the main menu to open the **Collection Task Management** tab.
2. Select one of the following access methods to open the **Create Indicator Set** tab.

No.	Path
Creating a performance indicator set	Select Performance Collection Management in the left pane and then right-click in the right pane to select Create Indicator Set from the shortcut menu.
	Select Performance Collection Management in the left pane and then right-click in the right pane to select Create Indicator Set from the shortcut menu.
	Right-click Indicator Set in the left pane and select Create Indicator Set from the shortcut menu.
	Click Indicator Set in the left pane and click Create Indicator Set in the right pane.
	Click the Indicator Set in the left pane, right-click in the right pane and select Create Indicator Set from the shortcut menu.

3. Set the parameters in the **Basic Information** and **Member** tabs of the **Create Indicator Set** dialog box.



Note:

Click the **Copy from Other Indicator Set** to open the **Select Indicator Set** dialog box. Then select the desired indicator set to copy its parameter settings, so as to improve setting efficiency.

4. Click **OK**.

8.6.2 Managing Performance Threshold Sets

The following introduces how to view, create and use the performance threshold sets.

8.6.2.1 Viewing the Performance Threshold Set

View the performance threshold sets already set and select the desired threshold set to quickly complete the statistics and query of performance threshold.

Prerequisite

- ◆ You have the authority of **Inspector Group** or higher authority.
- ◆ The NE time is synchronized with the EMS time.

Procedure

1. Select **Performance** → **Collection Task Management** from the main menu to open the **Collection Task Management** tab.
2. In the **Collection Task Management** tab, select **Threshold Set** and view the existing threshold sets in the right pane.
3. In the **Collection Task Management** tab, double-click the desired performance threshold set to view the details of the threshold set, including **Basic Information** and **Member**.

Subsequent Operation

- ◆ Modify the performance threshold set
In the left pane, select the corresponding performance threshold set, modify the relevant information in the right pane and then click **Save All**.
- ◆ Other Operations
In the right pane, select the corresponding entry and click the button at the bottom, or simply right-click the entry and select **Delete**, **Print**, **Copy Cell** or **Export** from the shortcut menu.

8.6.2.2 Creating a Performance Threshold Set

You can monitor the performance data by setting the performance threshold. If the performance data exceeds the preset threshold value, the threshold crossing alarm will be generated.

Prerequisite

- ◆ You have the authority of **Inspector Group** or higher authority.
- ◆ The NE time is synchronized with the EMS time.

Procedure

1. Select **Performance**→**Collection Task Management** from the main menu to open the **Collection Task Management** tab.
2. Select one of the following access methods to open the **Create Threshold Set** tab.

Operation	Path
Creating a performance threshold set	Select Performance Collection Management in the left pane and then right-click in the right pane to select Create Threshold Set from the shortcut menu.
	Select Threshold Set in the left pane and then right-click in the right pane to select Create Threshold Set from the shortcut menu.
	Right-click Threshold Set in the left pane and select Create Threshold Set from the shortcut menu.
	Select Performance Collection Management in the left pane and then right-click in the right pane to select Create Threshold Set from the shortcut menu.
	Select Threshold Set in the left pane and click Create Threshold Set in the right pane.

3. Set the information in the **Basic Information** and **Member** dialog boxes. For details, see Table 8-2.

Table 8-2 Threshold Set Parameters

Parameter		Description
Basic Information	Threshold Set Name	Sets a name for the threshold set.
	NE Type	Selects the corresponding NE type.
	Comment	Enters the remark information for the threshold set.
Member	Performance Code	Clicks Select to select the performance codes for which the performance threshold is to be set.
	Upper Threshold Value	Sets the upper limit for the corresponding performance code.

Table 8-2 Threshold Set Parameters (Continued)

Parameter		Description
	Lower Threshold Value	Sets the lower limit for the corresponding performance code.
	Upper Clear Limit	Sets the upper clearing limit for the corresponding performance code. The upper clearing limit must be smaller than the upper limit.
	Lower Clear Limit	Sets the Lower clearing limit for the corresponding performance code. The lower clearing limit must be greater than the lower limit.
	Alarm Code	Sets the threshold-crossing alarm code for the corresponding performance code. The following options are available: <ul style="list-style-type: none"> ◆ PM_THRESHOLD_CRITICAL ◆ PM_THRESHOLD_MAJOR ◆ PM_THRESHOLD_MINOR ◆ PM_THRESHOLD_WARNING
	Object Type	Sets the applied object of the corresponding performance code. The objects include the followings. <ul style="list-style-type: none"> ◆ All ◆ Local Board ◆ Local Board Port ◆ ONU ◆ ONU Port
Note: The performance threshold parameters must be meet the following conditions: Upper limit > upper clearing limit > lower clearing limit > lower limit.		

4. Click **OK**.

8.6.3 Managing Performance Collection Tasks

The following introduces how to view and create performance collection tasks.

8.6.3.1 Viewing Performance Collection Task

View the performance collection task already set and select the desired task set to collect the performance.

Prerequisite

- ◆ You have the authority of **Inspector Group** or higher authority.
- ◆ The NE time is synchronized with the EMS time.

Procedure

1. Select **Performance**→**Collection Task Management** from the main menu to open the **Collection Task Management** tab.
2. In the **Collection Task Management** tab, select **Collection Task** and view the existing collection tasks in the right pane.
3. In the **Collection Task Management** tab, double-click the desired collection task in the right pane to view the details of the task, including **Basic Information**, **Collection Object**, **Collection Specification** and **Collection Cycle**.

Subsequent Operation

- ◆ Modify the performance collection task.
In the left pane, select the corresponding performance collection task, modify the relevant information in the right pane and then click **Save All**.
- ◆ Other Operations
In the right pane, select the corresponding entry and click the button at the bottom, or simply right-click the entry and select **Disable**, **Delete**, **Print**, **Copy Cell** or **Export** from the shortcut menu.

8.6.3.2 Creating a Performance Collection Task

You can monitor the performance data by setting the performance collection task.

Prerequisite

- ◆ You have the authority of **Inspector Group** or higher authority.
- ◆ The NE time is synchronized with the EMS time.

Procedure

1. Select **Performance**→**Collection Task Management** from the main menu to open the **Collection Task Management** tab.
2. Select one of the following access methods to open the **Create Collection Task** tab.

No.	Path
1	Click Performance Collection Management in the left pane and click Create Collection Task in the right pane.
2	Select Performance Collection Management in the left pane and then right-click in the right pane to select Create Collection Task from the shortcut menu.
3	Click Collection Task in the left pane and click Create Collection Task in the right pane.
4	Select Collection Task in the left pane and then right-click in the right pane to select Create Collection Task from the shortcut menu.
5	Right-click Collection Task in the left pane and select Create Collection Task from the shortcut menu.

3. Set **Basic Information**, **Collection Object**, **Collection Specification**, **Collection Cycle** in the **Create Collection Task** dialog box.



Note:

Click **Copy from Other Collection Task**, select the collection task in the **Select Collection Task** dialog box, and copy the parameter settings of corresponding task to improve the setting efficiency.

4. Click **OK**.

8.7 Managing Performance Data

If the data history stored in the UNM2000 exceeds the threshold, the UNM2000 operation will be influenced. The performance data saving function can save the historical performance data in the UNM2000 as files to the designated file folder, so as to improve the UNM2000 operation performance. The UNM2000 supports manual saving and overflow saving.

- ◆ **Overflow saving:** You can set the maximum saving capacity of performance data and the UNM2000 will regularly check the historical performance data. When the historical performance data reach the preset capacity, the UNM2000 will save the data to a specified file to decrease its load.
- ◆ **Manual saving:** You can save the historical performance data in the UNM2000 to a specified file folder manually at anytime. You can set the manual saving period. When the historical performance data saved in the database reach the preset time period, the UNM2000 will save the data to a designated file folder. You can mark the saving time in the name of the folder where the file is saved.

8.7.1 Setting the Performance Overflow Saving

Set the performance overflow saving task. The UNM2000 regularly checks whether the performance history data in the database meets the preset conditions. If the overflow saving conditions are met, the UNM2000 saves the performance history data automatically. The saved performance history data history will be deleted from the database.

Background Information

The UNM2000 provides the default overflow saving tasks of history data, which cannot be deleted. You can modify the overflow saving conditions of the corresponding task as needed.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **System** → **Save Data** to open the **Save the Data** tab.
2. Select **Save History Data** → **Overflow Saving** → **15-min Performance History Saving** / → **24-hour Performance History Saving** from the left pane to view the existing overflow saving tasks of alarm history.
3. Select any one access method from the table below to open the **Attribute** dialog box of the corresponding overflow saving task of performance history.

No.	Access Method
1	Double-click the corresponding overflow saving task in the right pane.
2	Right-click the corresponding overflow saving task in the right pane and select Attribute .
3	In the left pane, click  before Overflow Saving , and right-click an 15-minute / 24-hour performance history overflow saving task and select Attribute .

- Set the attribute of the overflow saving task, referring to Table 8-3.

Table 8-3 Performance Overflow Saving Task Settings

Parameter		Description
Basic Information	Task Name	The name of the overflow saving task, which cannot be edited by users.
	Enable	Select it to enable the task.
	Task Type	Sets the execution cycle of the task. The default value is Every 2 days .
	Execution Time	Sets the execution time of the task.
	Start Time	Sets the start time of the task.
	End Time	Sets the end time of the task.
Extended information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the data history that meets the overflow saving conditions into files. You can convert the data history into CSV files and save them into the sever harddisk or into the FTP server. ◆ Select Delete Directly to delete the data history that meets the overflow saving conditions directly.
	Overflow Limit	If the data history exceeds the maximum saving entry number or exceeds the record threshold, a pre-set proportion of the database will be saved.
	Capacity Limit	The data history that exceeds the reserving days of the database will be saved during the saving task.

- Click **OK**.
- Select the corresponding overflow saving task in the left pane and click **Execute Now** in the upper right pane. View the execution result in the bottom right pane.

8.7.2 Setting Manual Performance Saving

The UNM2000 supports saving alarm history and performance history manually, preventing insufficient space in database.

Background Information

The UNM2000 provides the default manual saving tasks of alarm history / events, which cannot be deleted. You can modify the parameters of the corresponding saving task as needed.



Note:

The name of the manually saved file can be marked with the saving time. You can turn on the switch to mark the saving time in the name of the saved file by modifying the background configuration file. For specific operations, contact the FiberHome technical engineer.

Procedure

1. Select **System**→**Save Data** from the main menu to open the **Save Data** tab.
2. Select **Save History Data**→**Save Manually**→**15-min Performance History Saving** / →**24-hour Performance History Saving** from the left pane to view the existing manual saving task of performance history.
3. Select any one of the access methods below to open the **Attribute** dialog box of the corresponding manual saving task of performance history.

No.	Access Method
1	Double-click the corresponding manual saving task in the right pane.
2	Right-click the corresponding manual saving task in the right pane and select Attribute .
3	In the left pane, click  on the left side of Save Manually , and right-click the corresponding manual saving task to select Attribute .

4. Set the attribute of the overflow saving task, referring to Table 8-4.

Table 8-4 Description of the Manual Performance Saving Task Parameters

Parameter		Description
Basic Information	Task Name	The name of the saving task, which cannot be edited by users.
	Enable	Select it to enable the task.
	Task Type	Sets the execution cycle of the task.
Extend Information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the data history that meets the overflow saving conditions into files. You can convert the data history into CSV files and save them into the sever harddisk or into the FTP server. ◆ Select Delete Directly to delete the data history that meets the overflow saving conditions directly.
	Data Generation Time	Sets the generation time and end time of the data.
	Selecting the Object	Sets the range of the object to be exported.
	Records that Matched the Saving Conditions	Displays the number of the data entries that comply with the saving conditions. This item cannot be edited.

5. Select the corresponding manual saving task in the left pane and click **Execute Now** in the upper right pane. View the execution result in the bottom right pane.

8.7.3 Analysis of PON traffic statistics

The analysis of PON traffic statistics function supports analyzing traffic, optical power and device health. It provides abundant reports for analyzing and monitoring services and device running status so as to provide detailed data for network planning.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **Performance**→**Analysis of PON Traffic Statistics** from the main menu to open the **Query Traffic Statistical** dialog box.
2. Set the statistical type, period, object, performance code and then click **OK**. The **Traffic Statistical Chart** tab appears, displaying the statistical result.

Other Operations

By clicking the buttons on the toolbar of the **Traffic Statistical Chart** tab, you can print or export the statistical result or display the statistical result in different charts.

8.7.4 Enabling / disabling FTP Report

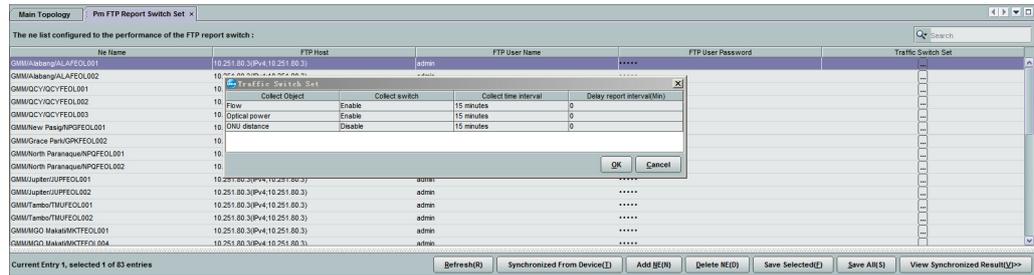
After the FTP report is enabled, you can collect the traffic data and back them up to a specified FTP server.

Prerequisite

- ◆ The FTP server is set (click SystemParameter Settings and then select **Service Configuration**→**FTP Server Management**).
- ◆ You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **Performance**→**Pm FTP Switch Management** from the main menu to open the **Pm FTP Report Switch Set** tab.
2. Click **Synchronized From Device** to synchronize the device data.
3. Click **Add NE** to open the **Please Select NE** dialog box and then select desired NEs.
4. Click **OK**.
5. Set the FTP server parameters, enable the traffic function and click **OK**.



6. Click **Save All**.

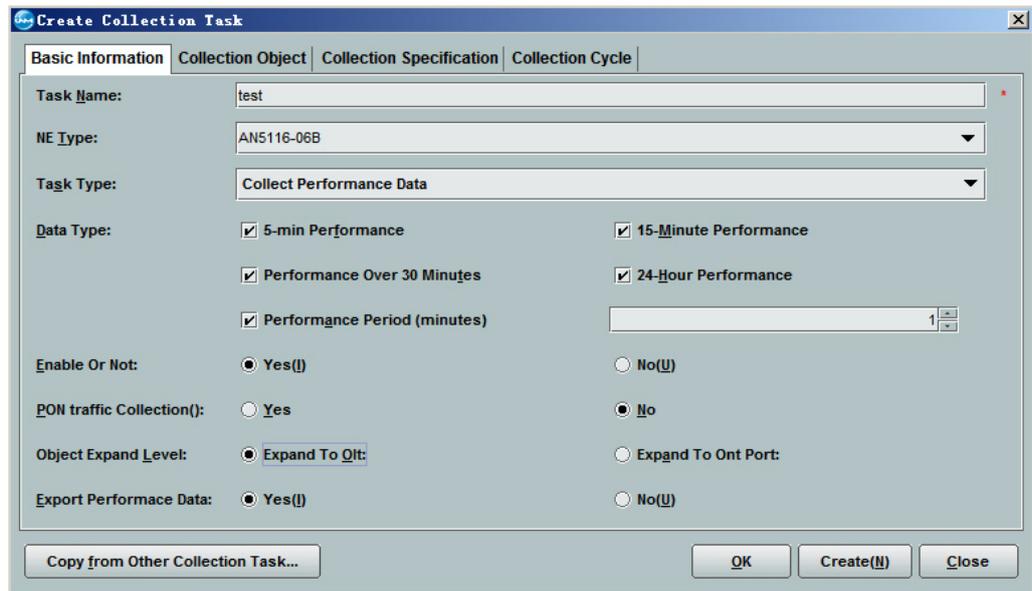
Other Operations

Right-click the NE object in the list or click the button at the bottom of the GUI to execute operations such as **Delete**.

Subsequent Operation

After enabling the FTP report, create a performance collection task to collect the performance such as traffic, optical power and ONU distance. The following takes collecting PON traffic data as an example.

1. Select **Performance** → **Collection Task Management** from the main menu to open the **Collection Task Management** tab.
2. Right-click **Collection Task** and select **Create Collection Task** from the shortcut menu.
3. In the **Create Collection Task** dialog box, set the task parameters and set **PON Traffic Collection** to **Yes** to enable the FTP collection.



4. Click **Create** to complete the settings.

8.7.5 Top Ranking Statistics

TopN Traffic Ranking supports PON traffic ranking and equipment health degree ranking, providing users with specialized and abundant reports.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **Performance** → **Top rank statistics** from the main menu to open the **Query Traffic Top Ranking** dialog box.

- Set the statistical type, period, object, performance code and then click **OK**. The **Traffic Statistical Top Ranking** tab appears, displaying the statistical result.

Other Operations

By clicking the buttons on the toolbar of the **Traffic Statistical Top Ranking** tab, you can **Print** or **Export** the statistical result or display the statistical result in different charts.

8.8 Managing Statistics Export Task

This task facilitate users to analyze traffic data of the equipment and supports exporting the analysis data. The statistics export task supports exporting traffic analysis, TopN traffic ranking, 15-minute performance, and 15-minute performance data of equipment traffic and health degree.

8.8.1 Export Task of Traffic Analysis

The export task of traffic analysis supports exporting the **PON Traffic Analysis**, **Equipment Health Degree Analysis** and **Optical Power Analysis** reports to the FTP server, so as to provide specialized and abundant report service to users.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Statistics Export Task**→**Traffic Statistic** in the left pane to view the existing export task of traffic analysis.
3. Click **Create** in the right pane.
4. Set the parameters such as basic information in the dialog box that appears and click **OK**.

Table 8-5 Parameter Description of the Export Task of Performance Traffic Analysis

Parameter		Description
Basic Information	Task Name	The name of the traffic analysis export task, which cannot be edited by users.
	Enable	Select it to enable the task.
	Report Type	Sets the analysis cycle of the report exporting.
	Execution Time	Sets the execution time of the task.
	Start Time	Sets the start time of the task.
	End Time	Sets the end time of the task.
Object Source	Selecting the Object	Sets the range of the object to be exported.
Extended information	Setting the XFTP Server	Sets the FTP server to save files.
	Report Template	Sets the template used by the exported report.

Other Operations

In the right pane, right-click the task entry to **Delete**, **Disable**, or view or modify **Attribute**.

8.8.2 Export Task of TopN Traffic Ranking

This task supports exporting the reports of **TopN Traffic Ranking** and **TopN Equipment Health Degree Ranking** to the FTP server, so as to provide specialized and abundant report service to users.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Statistics Export Task**→**Traffic TopN Ranking Statistic** in the left pane to view the existing export task of TopN traffic ranking.
3. Click **Create** in the right pane.
4. Set the parameters such as basic information in the dialog box that appears. Click **OK**.

Table 8-6 Parameter Description of the Export Task of TopN Traffic Ranking

Parameter		Description
Basic Information	Task Name	The name of the TopN traffic ranking export task, which cannot be edited by users.
	Enable	Select it to enable the task.
	Report Type	Sets the analysis cycle of the report exporting.
	Execution Time	Sets the execution time of the task.
	Start Time	Sets the start time of the task.
	End Time	Sets the end time of the task.
Object Source	Selecting the Object	Sets the range of the object to be exported.
Extended information	Setting the XFTP Server	Sets the FTP server to save files.
	Report Template	Sets the template used by the exported report.
	Object Type	Sets the object type in the exported report.
	Performance Specifications	Sets the performance specification in the exported report.
	Ranking Number	Sets the ranking number in the exported report.

Other Operations

In the right pane, right-click the task entry to **Delete**, **Disable**, or view or modify **Attribute**.

8.8.3 Export Task of 15-minute Performance

The export task of 15-minute performance supports exporting the **15-minute performance** report to the FTP server, so as to provide specialized and abundant report service to users.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Statistics Export Task**→**15 Minute Performance Export Task** in the left pane to view the existing export task of 15-minute performance.
3. Click **Create** in the right pane.
4. Set the parameters such as basic information in the dialog box that appears and click **OK**.

Table 8-7 Parameter Description of the Export Task of 15-minute Performance

Parameter		Description
Basic Information	Task Name	The name of the 15-minute performance export task, which cannot be edited by users.
	Enable	Select it to enable the task.
	Task Type	Sets the execution cycle of the report task.
Extended Information	Setting the XFTP Server	Sets the FTP server to save files.
	File Type	Sets the file type of the exported report.
	Start Time	Sets the start time of the task.
	End Time	Sets the end time of the task.
	Cycle	Sets the cycle of the report exporting.

Other Operations

In the right pane, right-click the task entry to **Delete**, **Disable**, or view or modify **Attribute**.

8.8.4 Export Task of Equipment Traffic and 15-minute Performance of Health Degree

The UNM2000 supports exporting the equipment flow and the 15-minute performance of health degree to the FTP server, so as to provide specialized and abundant report service to users.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Statistics Export Task**→**Traffic and Health Degree 15 Minute Performance Export Task** in the left pane to view the existing export task of equipment traffic and the 15-minute performance of health degree.
3. Click **Create** in the right pane.
4. Set the parameters such as basic information in the dialog box that appears and click **OK**.

Table 8-8 Parameter Description of the Export Task of Equipment Traffic and 15-minute Performance of Health Degree

Parameter		Description
Basic Information	Task Name	The name of the export task of equipment traffic and 15-minute performance of health degree. The name cannot be edited.
	Enable	Select it to enable the task.
	Task Type	Sets the execution cycle of the report task.
Object Source	Selecting the Object	Sets the range of the object to be exported.

Table 8-8 Parameter Description of the Export Task of Equipment Traffic and 15-minute Performance of Health Degree (Continued)

Parameter		Description
Extended information	Setting the XFTP Server	Sets the FTP server to save files.
	Start Time	Sets the start time of the task.
	End Time	Sets the end time of the task.

Other Operations

In the right pane, right-click the task entry to **Delete**, **Disable**, or view or modify **Attribute**.

9 Log Management

The logs record the operation information of the UNM2000 users and the important events occurred in the system. By querying, gathering statistics of and saving logs regularly, the administrator can detect illegal login and operations, and analyze the failures. By browsing and gathering statistics of login, the administrator can query the operation information of the EMS and save the logs.

- Log Management Policy
- Log Type
- Log Statistics
- Managing System Logs
- Managing Operation Logs
- Managing Security Logs
- Managing Northbound Interface Command Logs
- Managing Log Data

9.1 Log Management Policy

The log management policy includes UNM2000 log management, northbound interface command log management, log saving management, log forwarding management and log export management.

UNM2000 Logs

The UNM2000 logs include system logs, operation logs and security logs.

- ◆ The UNM2000 system logs record the tasks that influence the running of the UNM2000. By viewing the UNM2000 system logs, you can detect the failure that may influence the running of the UNM2000 and process it in a timely manner so as to ensure the normal running of the UNM2000.
- ◆ The operation logs record all the operations performed at the UNM2000 client end (such as creating logical domains, creating NEs and confirming alarms) except the operations that influence the security of the UNM2000. By viewing the operation logs, you can understand the operation performed at the UNM2000 client end so as to trace and audit the operations. This provides support to elimination of the influence caused by misoperation.
- ◆ The security logs record the operations performed at the UNM2000 client end that influence the security of the UNM2000, for example, user login, user logout and unlocking. By viewing the UNM2000 security logs, you can understand the operations performed at the UNM2000 client end that influence the security of the UNM2000. Querying the security logs on a regular basis can effectively ensure the security of the UNM2000.

Northbound Interface Command Logs

The northbound interface command logs record the operations performed on the device by the users on the UNM2000 client end via the northbound interface commands. You can view the northbound command logs to understand the northbound interface command operations performed on the device and obtain the device running information. The northbound interface command logs include the TL1 command logs and Web service command logs.

Log Saving

By setting the scheduled save task of logs, the UNM2000 will save the logs to the specified directory regularly, which provides convenience for viewing logs and reduces the records in the database so as to improve the running speed of the system.

Log Forwarding

The UNM2000 supports forwarding the UNM2000 logs to the FTP server to save various logs, providing reference for maintenance and relieving the storage pressure of the UNM2000 sever.

Log Export

The UNM2000 enables you to export the UNM2000 logs to the specified directory so as to reduce the storage pressure on the UNM2000 server. The logs can be exported as a TXT, Excel, CSV, XML, PDF or HTML file.

9.2 Log Type

The UNM2000 log types include system logs, operation logs, security logs and northbound interface command logs.

9.2.1 System Logs

The UNM2000 system logs record the running status of the UNM2000. By viewing the UNM2000 system logs, you can detect the failure that may influence the running of the UNM2000 and process it in a timely manner so as to ensure the normal running of the UNM2000.

The system logs are stored in the database. You can query the operation logs via the client end.

Description of Log Parameters

Parameter	Parameters
Danger Level	The danger level of the operation for the UNM2000, including Warning , Normal and Danger .
Source	The UNM2000 module in which the operations are performed.
Time	Time of the operation execution.
Operation Terminal	The operational terminal used for operation execution.
Operation Result	The operation result: Succeeded , Failed and Part Succeeded . <ul style="list-style-type: none"> ◆ Succeeded: The operation is successful and all the operation results are returned. ◆ Failed: The operation is failed. ◆ Part Succeeded: The operation is partly successful and partly failed; all the operation results are returned.
Details	Other information of the operation.

9.2.2 Operation Logs

The UNM2000 operation logs record all the operations performed at the UNM2000 client end (such as creating logical domains, creating NEs and confirming alarms) except the operations that influence the security of the UNM2000. By viewing the operation logs, you can understand the operation performed at the UNM2000 client end so as to trace and audit the operations.

The operation logs are stored in the database. You can view the operation logs via the client end.

Log Meaning

The operation logs record all the operations performed at the UNM2000 client end (such as creating logical domains, creating NEs and confirming alarms) except the operations that influence the security of the UNM2000.

Description of Log Parameters

Parameter	Parameters
Operation Name	The name of the operation performed by users in the UNM2000.
Danger Level	The danger level of the operation for the UNM2000, including Warning , Normal and Danger .
Username	The UNM2000 user who performs the operation.
Login Mode	The login mode of the user who performs the operation, including Login to NMS and Login to Northbound Interface .
User Type	The type of the UNM2000 user who performs the operation.
Operation Time	Time of the operation execution.
Operation Terminal	The IP address of the terminal used for operation execution.
Operation Object	Object of the operation.
Operation Result	<p>The operation result: Succeeded, Failed and Part Succeeded.</p> <ul style="list-style-type: none"> ◆ Succeeded: The operation is successful and all the operation results are returned. ◆ Failed: The operation is failed. ◆ Part Succeeded: The operation is partly successful and partly failed; all the operation results are returned.
Details	Other information of the operation.

9.2.3 Security Logs

The security logs record the operations performed at the UNM2000 client end that influence the security of the UNM2000, for example, user login, user logout and unlocking. By viewing the security logs, you can understand the operations performed at the UNM2000 client end that influence the security of the UNM2000. Querying the security logs on a regular basis can effectively ensure the security of the UNM2000.

The security logs are stored in the database. You can view the security logs via the client end.

Log Meaning

The security logs record the operations performed at the UNM2000 client end that influence the security of the UNM2000, for example, user login, user logout and unlocking.

Description of Log Parameters

Parameter	Parameters
Security Event	The security-related operations in the UNM2000.
Danger Level	The danger level of the operation for the UNM2000, including Warning , Normal and Danger .
Username	The UNM2000 user who performs the operation.
Login Mode	The login mode of the user who performs the operation, including Login to NMS and Login to Northbound Interface .
User Type	The type of the UNM2000 user who performs the operation.
Operation Time	Time of the operation execution.
Operation Terminal	The IP address of the terminal used for operation execution.
Operation Object	Object of the operation.
Operation Result	<p>The operation result: Succeeded, Failed and Part Succeeded.</p> <ul style="list-style-type: none"> ◆ Succeeded: The operation is successful and all the operation results are returned. ◆ Failed: The operation is failed. ◆ Part Succeeded: The operation is partly successful and partly failed; all the operation results are returned.
Details	Other information of the operation.

9.2.4 Northbound Interface Command Logs

The northbound interface command logs record the operations performed on the device by the users on the UNM2000 client end via the northbound interface commands. You can view the northbound command logs to understand the northbound interface command operations performed on the device and obtain the device running information. The northbound interface command logs include the TL1 command logs and Web service command logs.

Log Meaning

The northbound interface command logs records the operations performed on the equipment by the UNM2000 users on the UNM2000 client end via the northbound interface commands.

Description of Log Parameters

◆ Parameters of the TL1 Command Logs

Parameter	Parameters
Row Statistics	Set the row data of the statistical output table. The optional values include operation object, type, name and result.
Column Statistics	Set the column data of the statistical output table. The optional values include quantity, operation type and result.  Note: The values of the statistical row data and column data cannot be the same; otherwise, errors may occur.
Preview	If it is selected, the pattern of the statistical output table is displayed. The pattern of this table depends on the values of the statistical row and column.
Operation Result	The operation result includes Succeeded , Failed and Part Succeeded . ◆ Succeeded : The operation is successful and all the operation results are returned. ◆ Failed : The operation is failed. ◆ Part Succeeded : The operation is partly successful.
Start Time	The start time range includes Latest and Time Range . ◆ Latest : Set the time period from the last operation time to the current query, such as last four hours, last day and last two days. ◆ Time Range : Set the start time and end time of the TL1 command operations.
Operation Name	The name of the operation performed on NEs by NE users.
Operation Object	Object of the operation.
Command	The TL1 commands delivered to NEs by NE users.

◆ Parameters of Web Service Command Logs

Parameter	Parameters
Row Statistics	Set the row data of the statistical output table. The optional values include operation object, name, type, name and result.
Column Statistics	<p>Set the column data of the statistical output table. The optional values include quantity and operation result.</p> <hr/>  Note: The values of the statistical low data and column data cannot be the same; otherwise, errors may occur.
Preview	If it is selected, the pattern of the statistical output table is displayed. The pattern of this table depends on the values of the statistical row and column.
Operation Result	<p>The operation result includes Succeeded and Failed.</p> <ul style="list-style-type: none"> ◆ Succeeded: The operation is successful and all the operation results are returned. ◆ Failed: The operation is failed.
Start Time	<p>The start time range includes Latest and Time Range.</p> <ul style="list-style-type: none"> ◆ Latest: Set the time period from the last operation time to the current query, such as last four hours, last day and last two days. ◆ Time Range: Set the start time and end time of the TL1 command operations.
OLT IP	The IP address of the OLT in the Web service command log.
ONU MAC/SN	The MAC address or SN of the ONU in the Web service command log.
HG MAC	The MAC address or SN of the ONU in the Web service command log.
Failure reason	The reason why the operation failed.
Operation Name	The name of the operation performed on NEs by NE users.
Operation Object	Object of the operation.
Command	The TL1 commands delivered to NEs by NE users.

9.3 Log Statistics

The UNM2000 supports gathering the statistics of the system logs, operation logs, security logs and TL1 command logs. You can gather statistics and perform analysis for logs by setting **System Log Statistics Conditions** and **Query Filtering**

Conditions, so as to understand the statistics conditions of relevant operation quickly.

Procedure

The procedure of gathering statistics of logs of different types are similar. The following takes the system log as an example.

1. In the main menu, select **Security**→**Statistical System Logs**.
2. Set the query conditions according to Table 9-1 and click **OK**.

Table 9-1 Parameter Description of the **statistical system logs** Dialog Box

Parameter Name		Description	Setting Method
Basic Information	Row Statistics	Sets the items to be displayed in the row of the statistics result.	Select the items to be displayed in the drop-down menu of Row Statistics .
	Column Statistics	Sets the items to be displayed in the column of the statistics result.	Select the items to be displayed in the drop-down menu of Column Statistics .
Source		Select the query objects of the system log.	Select Source Info , click  , and then select the system to be queried in the Select Source dialog box. Description: ◆ The system logs of all users will be queried by default.
Operation Result		Query the operation record according to the operation result.	In the Operation Result group box, select one or more options. By default, all the options are selected.
Danger Level		Query the operation record according to danger level.	In the Danger Level group box, select one or more options. By default, all the options are selected.

Table 9-1 Parameter Description of the **statistical system logs** Dialog Box (Continued)

Parameter Name	Description	Setting Method
Time Range	Set the time range to query the operation logs in this time range. If no time range is set, it will query all logs.	Select Start Time or End Time and set time in the following text box.
Details contain	Filter the operation logs by querying the information in the Details contain text box.	Select Details contain and enter the fields contained in the Details contain in the text box at the right side.

3. View the result in the **Statistical System Logs** tab.

Other Operations

- ◆ GUI icon
 - ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.
 - ▶ Query: Sets the query conditions and view the query result.
 - ▶ Query According to Template: Select the existing template and query the logs that comply with the conditions.

9.4 Managing System Logs

The system logs records the automatic operations of the UNM2000, facilitating users to understand the UNM2000 running status. The following introduces how to manage the system log templates and query system logs.

9.4.1 Managing System Log Template

To query the system logs conveniently and quickly, you can set the routine system log type as the query template.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. In the main menu, select **Security** → **Search the System Logs**.
2. Click **Query** in the **System Logs** tab to bring up the **Query System Logs** dialog box.
3. Set the query conditions according to the system log query requirement, referring to Table 9-2.

Table 9-2 Parameter Description of the **Query System Logs** Dialog Box

Parameter Name	Description	Setting Method
Source	Select the query objects of the system log.	Select Source Info , click  , and then select the system to be queried in the Select Source dialog box. Description: ◆ The system logs of all users will be queried by default.
Operation Result	Query the operation record according to the operation result.	In the Operation Result group box, select one or more options. By default, all the options are selected.
Danger Level	Query the operation record according to danger level.	In the Danger Level group box, select one or more options. By default, all the options are selected.
Time Range	Set the time range to query the operation logs in this time range. If no time range is set, it will query all logs.	Select Start Time or End Time and set time in the following text box.
Details contain	Filter the operation logs by querying the information in the Details contain text box.	Select Details contain and enter the fields contained in the Details contain in the text box at the right side.

4. Click **Save as Template** to complete setting the system log query template.

Other Operations

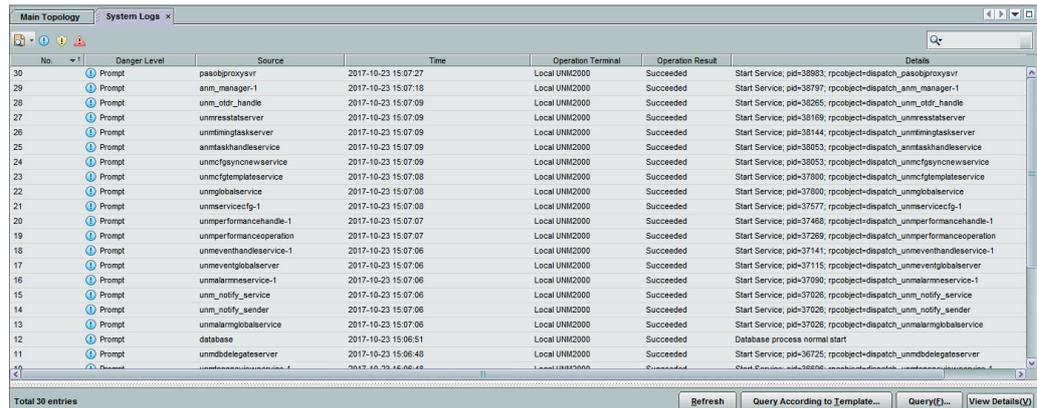
In the **System Logs** tab, right-click the item to be queried and select **Template Management** from the shortcut menu to edit or delete the existing log template.

9.4.2 Searching System Logs

The system logs records the automatic operations of the UNM2000, facilitating users to understand the UNM2000 running status.

Procedure

1. In the main menu, select **Security**→**Search the System Logs**.
2. View the query result in the **System Logs** tab. All the system logs of the current day will be queried by default.



No.	Danger Level	Source	Time	Operation Terminal	Operation Result	Details
30	Prompt	pasobjproxsvr	2017-10-23 15:07:27	Local UNM2000	Succeeded	Start Service, pid=38983, rpoject=dispatch_pasobjproxsvr
29	Prompt	anm_manager-1	2017-10-23 15:07:18	Local UNM2000	Succeeded	Start Service, pid=38797, rpoject=dispatch_anm_manager-1
28	Prompt	unm_oldr_handle	2017-10-23 15:07:09	Local UNM2000	Succeeded	Start Service, pid=38265, rpoject=dispatch_unm_oldr_handle
27	Prompt	unmreslatsvserver	2017-10-23 15:07:09	Local UNM2000	Succeeded	Start Service, pid=38169, rpoject=dispatch_unmreslatsvserver
26	Prompt	unmtrmgtaskserver	2017-10-23 15:07:09	Local UNM2000	Succeeded	Start Service, pid=38144, rpoject=dispatch_unmtrmgtaskserver
25	Prompt	unmashandservice	2017-10-23 15:07:09	Local UNM2000	Succeeded	Start Service, pid=38053, rpoject=dispatch_unmashandservice
24	Prompt	unmcfgyinciservice	2017-10-23 15:07:09	Local UNM2000	Succeeded	Start Service, pid=38053, rpoject=dispatch_unmcfgyinciservice
23	Prompt	unmcfemplateservice	2017-10-23 15:07:08	Local UNM2000	Succeeded	Start Service, pid=37800, rpoject=dispatch_unmcfemplateservice
22	Prompt	unmglobalservice	2017-10-23 15:07:08	Local UNM2000	Succeeded	Start Service, pid=37800, rpoject=dispatch_unmglobalservice
21	Prompt	unmservicecg-1	2017-10-23 15:07:08	Local UNM2000	Succeeded	Start Service, pid=37577, rpoject=dispatch_unmservicecg-1
20	Prompt	unmperformancehandle-1	2017-10-23 15:07:07	Local UNM2000	Succeeded	Start Service, pid=37468, rpoject=dispatch_unmperformancehandle-1
19	Prompt	unmperformanceoperation	2017-10-23 15:07:07	Local UNM2000	Succeeded	Start Service, pid=37268, rpoject=dispatch_unmperformanceoperation
18	Prompt	unmeventhandservice-1	2017-10-23 15:07:06	Local UNM2000	Succeeded	Start Service, pid=37141, rpoject=dispatch_unmeventhandservice-1
17	Prompt	unmeventglobalservice	2017-10-23 15:07:06	Local UNM2000	Succeeded	Start Service, pid=37115, rpoject=dispatch_unmeventglobalservice
16	Prompt	unmalarmeservice-1	2017-10-23 15:07:06	Local UNM2000	Succeeded	Start Service, pid=37090, rpoject=dispatch_unmalarmeservice-1
15	Prompt	unm_notify_service	2017-10-23 15:07:06	Local UNM2000	Succeeded	Start Service, pid=37026, rpoject=dispatch_unm_notify_service
14	Prompt	unm_notify_sender	2017-10-23 15:07:06	Local UNM2000	Succeeded	Start Service, pid=37026, rpoject=dispatch_unm_notify_sender
13	Prompt	unmalarmglobalservice	2017-10-23 15:07:06	Local UNM2000	Succeeded	Start Service, pid=37026, rpoject=dispatch_unmalarmglobalservice
12	Prompt	database	2017-10-23 15:06:51	Local UNM2000	Succeeded	Database process normal start
11	Prompt	unmdelegatesvserver	2017-10-23 15:06:48	Local UNM2000	Succeeded	Start Service, pid=36725, rpoject=dispatch_unmdelegatesvserver
10	Prompt	unmdelegatesvserver	2017-10-23 15:06:48	Local UNM2000	Succeeded	Start Service, pid=36806, rpoject=dispatch_unmdelegatesvserver

3. Double-click the selected system log in the **System Logs** tab to view the detailed information.



Note:

Click the title column of the query result to sequence the result.

Other Operations

◆ GUI icon

- ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.

- ▶ Query According to Template: Select the existing template and query the logs that comply with the conditions.
- ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing System Log Template](#).
- ▶ View / Hide Details: Displays / hides the details pane of the selected log.

◆ **Shortcut menu**

Right-click the **System Logs** dialog box to bring up the shortcut menu. The descriptions of the menu items are as follows.

- ◆ Query: Sets the query conditions and view the query result.
- ◆ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.
- ◆ Template Management: Manages the log query template. You can edit or delete the existing log template.
- ◆ Copy Cell: Copies the existing log template.
- ◆ Print: Print the queried log.
- ◆ Export All Records: Exports all the queried log records into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.
- ◆ Export Selected Record: Exports the selected log record into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.

9.5 Managing Operation Logs

The operation logs record the operation information of users, enabling you to trace and check user operations. The following introduces how to manage the operation log templates and query operation logs.

9.5.1 Managing Operation Log Templates

To query the user operations conveniently and quickly, you can set the routine operation log types as the query template.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. In the main menu, select **Security**→**Query Operation Logs**.
2. Click **Query** in the **Operation Logs** tab to bring up the **Query Operation Logs** dialog box.
3. Set the query conditions according to the operation log query requirement, referring to Table 9-3.

Table 9-3 Parameters in the **Query Operation Logs** Dialog Box

Parameter		Description	Setting Method
User Information	User-name	Select users to query their operation logs.	Select Username , click  , and select the user to be queried in the Select User dialog box. Description: <ul style="list-style-type: none"> ◆ The operation logs of all users will be queried by default. ◆ The Select User dialog box only shows the users that have logged into the UNM2000 and performed operations.
	Operation Terminal	Select the operation terminal and query operation records according to the operation terminal.	Select Operation Terminal , click  , and select the operation terminal to be queried in the Select Operation Terminal dialog box. Description: The operation logs of all operation terminals will be queried by default.
Operation Result		Query the operation record according to the operation result.	In the Operation Result group box, select one or more options. By default, all the options are selected.
Danger Level		Query the operation record according to danger level.	In the Danger Level group box, select one or more options. By default, all the options are selected.

Table 9-3 Parameters in the **Query Operation Logs** Dialog Box (Continued)

Parameter	Description	Setting Method
Start Time	Set the time range to query the operation logs in this time range. If no time range is set, it will query all logs.	Select Start Time or End Time and set time in the following text box.
Details contain	Filter the operation logs by querying the information in the Details contain text box.	Select Details contain and enter the fields contained in the Details contain in the text box at the right side.
Operation Name	Sets the operations to be queried.	Click Select under the Operation Name box and select the desired operation name from the Select Operation Name dialog box.
Operation Object	Sets the operation object to be queried.	Click Select corresponding to Operation Object . Select the name of operation to be queried in the Select Operation Object dialog box.

4. Click **Save as Template** to complete setting the operation log query template.

Other Operations

In the **Operation Logs** tab, right-click the item to be queried and select **Template Management** from the shortcut menu to edit or delete the existing log template.

9.5.2 Querying Operation Logs

The operation logs record the operation information of users, enabling you to trace and check user operations.

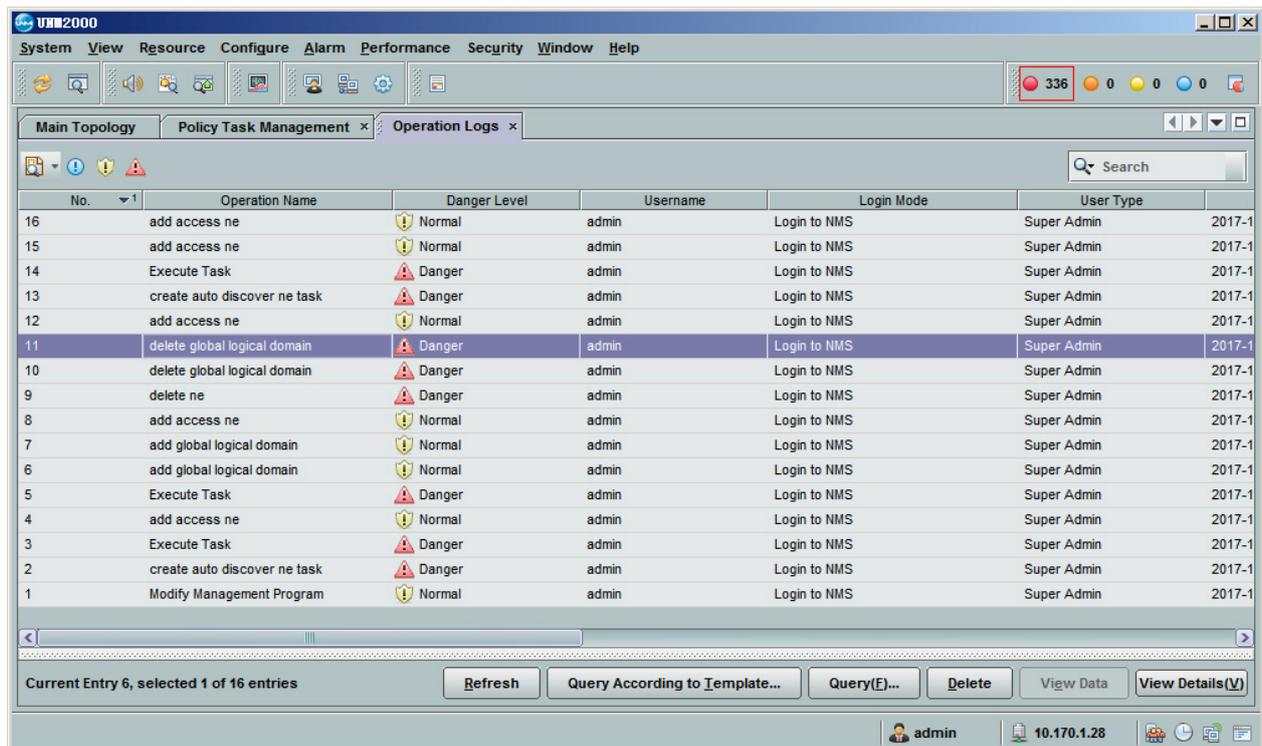
Background Information

- ◆ Filter according to username when querying operation logs. The **Unselected Value Filter** in the **Select User** dialog box only displays the usernames that has performed operations.
- ◆ The range of operation logs that users of different groups can view:

- ▶ Users in **Administrators** group can view the operation logs of all the users.
- ▶ Users in **Security Management Group** with the **Query Operation Logs** authority can view the operation logs of all users.
- ▶ The common users that have the **query operation logs** authority but belong to neither the **Security Management Group** nor the **Administrators** group can only view their own operation logs.

Procedure

1. In the main menu, select **Security**→**Query Operation Logs**.
2. View the query result in the **Operation Logs** tab. All the operation logs of the current day will be queried by default.



3. Double-click the selected operation log in the **Operation Logs** tab to view the detailed information.



Note:

Click the title column of the query result to sequence the result.

Other Operations

- ◆ GUI icon
 - ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.
 - ▶ Query According to Template: Select the existing template and query the logs that comply with the conditions.
 - ▶ Query: Sets the query conditions and view the query result. [Managing Operation Log Templates](#) shows the parameter descriptions of the query condition.
 - ▶ Delete: Deletes the selected operation log.
 - ▶ View Data: view the data information of operation records in the corresponding operation logs.



Note:

The **View Data** function is only available for viewing the operation logs of writing service configuration to device.

- ▶ View / Hide Details: Displays / hides the details pane of the selected log.
- ◆ Shortcut menu

Right-click the **Operation Logs** dialog box to bring up the shortcut menu. The descriptions of the menu items are as follows.

 - ▶ Query: Sets the query conditions and view the query result. [Managing Operation Log Templates](#) shows the parameter descriptions of the query condition.
 - ▶ View Data: view the data information of operation records in the corresponding operation logs.
 - ▶ Delete: Deletes the selected operation log.
 - ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.
 - ▶ Template Management: Manages the log query template. You can edit or delete the existing log template.
 - ▶ Copy Cell: Copies the existing log template.

- ▶ **Print:** Print the queried operation log.
- ▶ **Export All Records:** Exports all the queried log records into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.
- ▶ **Export Selected Record:** Exports the selected log record into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.

9.6 Managing Security Logs

The security logs record the information on the security operations performed by the UNM2000. Querying security logs regularly helps ensuring the security of the network management system effectively. The following introduces how to manage security log templates and query the security logs.

9.6.1 Managing Security Log Template

To query the UNM2000 security logs conveniently and quickly, you can set the routine security log type as the query template.

Prerequisite

You have the authority of **Security Admin Group** or higher authority.

Procedure

1. In the main menu, select **Security**→**Query Security Logs**.
2. Click **Query** in the **Security Logs** tab to bring up the **Query Security Logs** dialog box.
3. Set the query conditions according to the security log query requirement, referring to Table 9-4.

Table 9-4 Parameter Description of the **Query Security Logs** Dialog Box

Parameter Name		Description	Setting Method
User Information	User-name	Select users to query their security logs.	Select Username , click  , and select the user to be queried in the Select User dialog box. Description: <ul style="list-style-type: none"> ◆ The security logs of all users will be queried by default. ◆ The Select User dialog box only shows the users that have logged into the UNM2000.
	Operation Terminal	Select the operation terminal. Query security records according to the operation terminal.	Select Operation Terminal , click  , and select the operation terminal to be queried in the Select Operation Terminal dialog box. Description: The security logs of all operation terminals will be queried by default.
Operation Result		Query the operation record according to the security result.	In the Operation Result group box, select one or more options. By default, all the options are selected.
Danger Level		Query the security record according to danger level.	In the Danger Level group box, select one or more options. By default, all the options are selected.
Start Time		Set the time range to query the security operation logs in this time range. If no time range is set, it will query all logs.	Select Start Time or End Time and set time in the following text box.
Details contain		Filters the security logs by querying the information in the Details contain text box.	Select Details contain and enter the fields contained in the Details contain in the text box at the right side.

Table 9-4 Parameter Description of the **Query Security Logs** Dialog Box (Continued)

Parameter Name	Description	Setting Method
Select Security Event	Sets the security event to be queried.	Click Select corresponding to Select Security Event . Select the name of operation to be queried in the Select Security Event dialog box.
Select the operation object.	Sets the operation object to be queried.	Click Select corresponding to Select Operation Object . Select the name of operation to be queried in the Select Operation Object dialog box.

4. Click **Save as Template** to complete setting the security log query template.

Other Operations

In the **Security Logs** tab, right-click the item to be queried and select **Template Management** from the shortcut menu to edit or delete the existing log template.

9.6.2 Querying Security Logs

The security logs record the information on the security operations performed by the UNM2000. Querying security logs regularly helps ensuring the security of the network management system effectively.

Background Information

The user with the **Query Security Logs** authority can view the security logs of all users.

Procedure

1. In the main menu, select **Security**→**Query Security Logs**.
2. In the **Security Logs** tab, view the query result. The system displays the security logs of the current day by default.

No.	Security Event	Danger Level	Username	Login Mode	User Type	Operation Time	Operation Terminal
12	user login	Normal	admin	Login to NMS	Super Admin	2017-10-23 15:32:06	10.32.150.5
11	user exit	Normal	admin	Login to NMS	Super Admin	2017-10-23 15:31:56	10.32.150.5
10	user login	Normal	admin	Login to NMS	Super Admin	2017-10-23 15:24:18	10.32.150.5
9	user exit	Normal	admin	Login to NMS	Super Admin	2017-10-23 15:21:51	10.32.150.5
8	user login	Normal	admin	Login to NMS	Super Admin	2017-10-23 15:19:37	10.32.150.5
7	user exit	Normal	vpjason	Login to NMS	Ordinary User	2017-10-23 15:08:58	10.18.157.30
6	user exit	Normal	t-jcao	Login to NMS	Ordinary User	2017-10-23 15:08:58	10.30.17.193
5	user exit	Normal	t-hpdamo	Login to NMS	Super Admin	2017-10-23 15:08:58	10.4.18.243
4	user exit	Normal	recdelgado	Login to NMS	Ordinary User	2017-10-23 15:08:58	10.18.157.31
3	user exit	Normal	tpjcsde	Login to NMS	Ordinary User	2017-10-23 15:00:55	10.25.66.23
2	user login	Normal	admin	Login to NMS	Super Admin	2017-10-23 15:08:44	10.175.160.79
1	user login	Normal	admin	Login to NMS	Super Admin	2017-10-23 15:07:53	10.168.17.33

- In the **Security Logs** tab, double-click the desired security log to view the log details.



Note:

Click the title column of the query result to sequence the result.

Other Operations

- ◆ GUI icon
 - ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.
 - ▶ Query According to Template: Select the existing template and query the logs that comply with the conditions.
 - ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing Security Log Template](#).
 - ▶ View / Hide Details: Displays / hides the details pane of the selected log.
- ◆ Shortcut menus

Right-click the **Security Logs** dialog box to bring up the shortcut menu. The descriptions of the menu items are as follows.

- ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing Security Log Template](#).
- ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.
- ▶ Template management: Manages the log query templates or edits / deletes the existing log query template. See [Managing Security Log Template](#).

- ▶ Copy Cell: Copies the existing log template.
- ▶ Print: Print the queried log.
- ▶ Export All Records: Exports all the queried log records into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.
- ▶ Export Selected Record: Exports the selected log record into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.

9.7 Managing Northbound Interface Command Logs

The northbound interface command logs record the operations performed on the device by the UNM2000 users on the UNM2000 client end via the northbound interface commands. You can view the northbound command logs to understand the northbound interface command operations received by the device and obtain the device running information.

9.7.1 Managing TL1 Command Log Templates

To conveniently and quickly query the TL1 commands accepted and executed by the NEs, you can set the most concerned TL1 commands as a query template.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. In the main menu, select **Security**→**Query Northbound Interface Command Logs**.
2. In the lower left corner of the **View the TL1 Command Logs** window, select **TL1 Command Logs** tab and click **Query** to open the **Query TL1 Command Log** dialog box.
3. Set the query conditions as needed, referring to Table 9-5.

Table 9-5 Description of the Parameters in the **Query TL1 Command Logs** Dialog Box

Parameter Name	Description	Setting Method
Operation Result	Query the operation record according to the operation result.	In the Operation Result group box, select one or more options. By default, all the options are selected.
Start Time	Set the time range to query the security operation logs in this time range. If no time range is set, it will query all logs.	Select Start Time or End Time and set time in the following text box.
Details contain	Filters the operation logs by the information entered in the Details contain textbox.	Select Details contain and enter the fields contained in the Details contain in the text box at the right side.
Select Operation Name	Selects the operation commands to be queried.	Click Select under the Operation Name box and select the desired operation name from the Select Operation Name dialog box.
Select the operation object.	Sets the operation object to be queried.	Click Select corresponding to Operation Object . Select the name of operation to be queried in the Select Operation Object dialog box.

- Click **Save as Template** to open the **Save as Template** dialog box. Enter the **Template Name** and **Remark**, and click **OK**.

9.7.2 Querying TL1 Command Logs

The TL1 command logs record the operations performed on the device by the UNM2000 users on the UNM2000 client end via the TL1 commands. You can view the TL1 command logs to understand the operations performed on the device by the UNM2000 users via the TL1 commands and obtain the device running information.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. In the main menu, select **Security**→**Query Northbound Interface Command Logs**.
2. In the lower left corner of the **View the TL1 Command Logs** window, select **TL1 Command Logs** tab to view the query result. The system queries all the TL1 command logs of the current day.
3. Double-click a TL1 command log to view the details of the TL1 command log.



Note:

Click the title column of the query result to sequence the result.

Other Operations

◆ GUI icon

- ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.
- ▶ Query According to Template: Select the existing template and query the logs that comply with the conditions.
- ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing TL1 Command Log Templates](#).
- ▶ View / Hide Details: Displays / hides the details pane of the selected log.

◆ Shortcut menus

Right-click the **TL1 Logs** dialog box to bring up the shortcut menu. The descriptions of the menu items are as follows.

- ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing TL1 Command Log Templates](#).
- ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.

- ▶ **Template management:** Manages the log query templates or edits / deletes the existing log query template. See [Managing TL1 Command Log Templates](#).
- ▶ **Copy:** Select to copy the cell or row and edit or delete the existing log template.
- ▶ **Print:** Print the queried log.
- ▶ **Export All Records:** Exports all the queried log records into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.
- ▶ **Export Selected Record:** Exports the selected log record into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.

9.7.3 Querying the Web Service Command Log Template

To conveniently and quickly query the Web service commands accepted and executed by the NEs, you can set the most concerned Web service commands as a query template.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. In the main menu, select **Security**→**Query Northbound Interface Command Logs**.
2. In the lower left corner of the **View the TL1 Command Logs** window, select **Web Service Command Logs** tab and click **Query** to open the **Query Web Service Command Log** dialog box.
3. Set the query conditions as needed. See Table 9-6.

Table 9-6 Description of the Parameters in the **Query Web Service Command Log** Dialog Box

Parameter	Description	Setting Method
Operation Result	Query the operation record according to the operation result.	In the Operation Result group box, select one or more options. By default, all the options are selected.
Start Time	Set the time range to query the security operation logs in this time range. If no time range is set, it will query all logs.	Select Lastest Time or Time Ronger and set time.
OLT IP	Set the IP address of the OLT in the Web service command log.	Set it manually.
ONU MAC/SN	Set the MAC address or SN of the ONU in the Web service command log.	Set it manually.
HG MAC	Set the MAC address of the card home gateway of the ONU in the Web service command log.	Set it manually.
Failure reason	Query the operation records according to the operation failure.	Set it manually.
Details contain	Filters the operation logs by the information entered in the Details contain textbox.	Select Details contain and enter the fields contained in the Details contain in the text box at the right side.
Select Operation Name	Selects the operation commands to be queried.	Click Select under the Operation Name box and select the desired operation name from the Select Operation Name dialog box.
Select the operation object.	Sets the operation object to be queried.	Click Select corresponding to Operation Object . Select the name of operation to be queried in the Select Operation Object dialog box.

- Click **Save as Template** to open the **Save as Template** dialog box. Enter the **Template Name** and **Remark**, and click **OK**.

9.7.4 Querying the Web Service Command Logs

The Web service command logs record the operations performed on the device by the UNM2000 users on the UNM2000 client end via the Web service commands. You can view the Web service command logs to understand the operations performed on the device by the UNM2000 users via the Web Service commands and obtain the device running information.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. In the main menu, select **Security**→**Query Northbound Interface Command Logs**.
2. In the lower left corner of the **View the TL1 Command Logs** window, select **Web Service Command Logs** tab to view the query result. The system queries all the Web service command logs of the current day.
3. Double-click a Web service command log to view the details of the Web service command log.



Note:

Click the title column of the query result to sequence the result.

Other Operations

- ◆ GUI icon
 - ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.
 - ▶ Query According to Template: Select the existing template and query the logs that comply with the conditions.
 - ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Querying the Web Service Command Log Template](#).
 - ▶ View / Hide Details: Displays / hides the details pane of the selected log.

◆ Shortcut menus

Right-click the **Web Service Command Logs** dialog box to bring up the shortcut menu. The descriptions of the menu items are as follows.

- ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Querying the Web Service Command Log Template](#).
- ▶ Refresh: Obtains the latest data from the database at the server end and displays them in the client end.
- ▶ Template management: Manages the log query templates or edits / deletes the existing log query template. See [Querying the Web Service Command Log Template](#).
- ▶ Copy: Select to copy the cell or row and edit or delete the existing log template.
- ▶ Print: Print the queried log.
- ▶ Export All Records: Exports all the queried log records into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.
- ▶ Export Selected Record: Exports the selected log record into the selected directory in format of TXT, Excel, CSV, XML, PDF or HTML.

9.8 Managing Log Data

By saving logs, you can clear the unnecessary logs manually or on a regular basis to avoid that the logs occupy too many resources. By exporting the logs as files, you can view logs or locate failures.

9.8.1 Managing the Log Forwarding Server

By setting the log forwarding server, you can forward the logs of the UNM2000 to other servers.

9.8.1.1 Viewing the Syslog Forwarding Server

Check whether the preset Syslog forwarding server meets the requirement.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **Security**→**System Log Forwarding Server Management** from the main menu to open the **System Log Forwarding Server Management** tab, and view the information of the existing Syslog forwarding server.

Other Operations

Click the button below or the right-click the corresponding entry to select **Modify**, **Stop / Enable**, **Delete**, **Refresh**, **Copy Cell**, **Print** or **Export**.

9.8.1.2 Adding A Syslog Forwarding Server

You can add a new Syslog forwarding server if the existing server cannot meet the requirement.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **Security**→**System Log Forwarding Server Management** from the main menu to open the **System Log Forwarding Server Management** tab.
2. Right-click in the blank area of the **System Log Forwarding Server Management** tab and select **Add** to open the **System Log Forwarding Server Settings** dialog box.
3. Set the parameters of the Syslog forwarding server, referring to Table 9-7.

Table 9-7 Description of the Syslog Forwarding Server

Parameter		Description
Server Information	Server IP	Sets the IP address of the Syslog forwarding server.
	Server Port	Sets the port of the Syslog forwarding server.

Table 9-7 Description of the Syslog Forwarding Server (Continued)

Parameter		Description
Syslog Information	Log Type	Sets the type of log to be forwarded, including: <ul style="list-style-type: none"> ◆ System Logs ◆ Security Logs ◆ Operation Logs ◆ NE Logs ◆ TL1 Logs ◆ Current Alarm Logs
	Log Level	Sets the level of logs to be forwarded, including: <ul style="list-style-type: none"> ◆ EMERG: the system is unavailable. ◆ ALERT: the event should be handled in a timely manner. ◆ CRIT: critical event. ◆ ERR: error event. ◆ WARNING: warning event. ◆ NOTICE: common but important event. ◆ INFO: useful information. ◆ DEBUG: debugging information.
	Facility Level	Sets the facility level to be forwarded, consistent with the setting on the Syslog forwarding server side. including: <ul style="list-style-type: none"> ◆ KERN: kernel log information. ◆ USER: random user log information. ◆ MAIL: mail system log information. ◆ DAEMON: system daemon process log information. ◆ AUTH: security management log information. ◆ SYSLOG: Syslog forwarding server log information. ◆ LPR: printer log information. ◆ NEWS: news service log information. ◆ UUCP: UUCP system log information. ◆ CRON: log information of the system daemon process CRON. ◆ AUTHPRIV: private security management log information. ◆ DAEMON: system daemon process log information. ◆ LOCAL0 to 7: reserve for local.
	protocol type	Sets the transmission protocol type, including TCP and UDP, which should be consistent with the setting of the Syslog forwarding server.
Other Information	Character String Filtering	Sets the character string, and the logs comply with the character string filtering conditions will be forwarded.
	Comment	Sets the remark information.
Enable		Sets whether to enable the current settings.

4. Click **OK** to add a new Syslog forwarding server.

9.8.2 Setting the Log Overflow Saving

Set the saving task of the log overflow. The UNM2000 regularly checks whether the log data history (operation logs, TL1 logs, system logs, NE logs and security logs) of the database meets the pre-set conditions. If the overflow saving conditions are met, the UNM2000 saves the log data automatically. The saved log data history will be deleted from the database.

Background Information

The UNM2000 provides the default overflow saving tasks of history data, which cannot be deleted. You can modify the overflow saving conditions of the corresponding task as needed.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

The procedures of setting log overflow saving are similar. The following takes setting operation log overflow saving as an example.

1. Select **System**→**Save Data** to open the **Save the Data** tab.
2. Select **Save History Data**→**Overflow Saving**→**Save Operation Log Overflow** from the left pane to view the existing saving task of operation log overflow.
3. Select any one access method from the table below to open the **Attribute** dialog box of the corresponding saving task of alarm history overflow.

No.	Access Method
1	Double-click the corresponding overflow saving task in the right pane.
2	Right-click the corresponding overflow saving task in the right pane and select Attribute .
3	In the left pane, click  on the left side of Overflow Saving , and right-click the corresponding overflow saving task to select Attribute .

4. Set the attribute of the overflow saving task, referring to Table 9-8.

Table 9-8 Description of the Overflow Saving Task Parameters

Parameter		Description
Basic Information	Task Name	The name of the overflow saving task, which cannot be edited by users.
	Enable	Select it to enable the task.
	Task Type	Sets the execution cycle of the task. The default value is Every 2 days .
	Execution Time	Sets the execution time of the task.
	Start Time	Sets the start time of the task.
	End Time	Sets the end time of the task.
Extended information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the data history that meets the overflow saving conditions into files. You can convert the data history into CSV files and save them into the sever harddisk or into the FTP server. ◆ Select Delete Directly to delete the data history that meets the overflow saving conditions directly.
	Overflow Limit	If the data history exceeds the maximum saving entry number or exceeds the record threshold, a pre-set proportion of the database will be saved.
	Capacity Limit	The data history that exceeds the reserving days of the database will be saved during the saving task.

5. Click **OK**.
6. Select the corresponding overflow saving task in the left pane and click **Execute Now** in the upper right pane. View the execution result in the bottom right pane.

9.8.3 Setting Manual Log Saving

To prevent insufficient space, the UNM2000 supports saving operation logs, system logs, NE logs, security logs and TL1 logs manually

Background Information

The UNM2000 provides the default manual saving tasks of log data, which cannot be deleted. You can modify the parameters of the corresponding saving task as needed.



Note:

The name of the manually saved file can be marked with the saving time. You can turn on the switch to mark the saving time in the name of the saved file by modifying the background configuration file. For specific operations, contact the FiberHome technical engineer. The procedures for setting manual saving of logs are the similar. The following uses the operation logs as an example to introduce how to set the manual saving.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **System** → **Save Data** from the main menu to open the **Save Data** tab.
2. Select **Save History Data** → **Save Manually** → **Save Operation Log** from the left pane to view the existing manual saving task of operation log.
3. Select any one access method from the table below to open the **Attribute** dialog box of the corresponding manual saving task of data history.

No.	Access Method
1	Double-click the corresponding manual saving task in the right pane.
2	Right-click the corresponding manual saving task in the right pane and select Attribute .
3	In the left pane, click  on the left side of Save Manually , and right-click the corresponding manual saving task to select Attribute .

4. Modify the parameters of the corresponding task in the **Attribute** dialog box according to requirement and click **OK**.

5. Select the corresponding manual saving task in the left pane and click **Execute Now** in the upper right pane. View the execution result in the bottom right pane.

10 Resource Management

Resource management manages the physical asset information and important logical configuration of all the devices in the network. The UNM2000 provides the unified query and statistics functions for the resources in the network. You can understand the usage of various resources in the network timely via the resource management.

The UNM2000 supports statistics and statistical result export for the following resources:

- ◆ Physical resources: Include NE resources, card resources, port resources, ONU resources, ONU port resources and MDU port resources.
- ◆ Other types: Include ONU users, local end VLANs, NE MGC services, ONU MGC services, device types, PON device capability, ONU WAN connection service, ONU out-of-service timing length and management VLAN.

- Managing Resource Statistics Template
- Physical Resource Statistics
- Resource Statistics of Other Types
- Exporting Physical Resource Statistics
- Exporting Resource Statistics of Other Types
- Example of Resource Statistics
- Importing the ODN NSM Information
- Querying Multiple ONUs
- Query Board By Serial Number
- Querying the MDU Phone Number
- ONU RMS Error Information Query

- Querying the ONU Network Access Interception Logs
- Importing GIS Data in a Batch Manner
- Gateway Type Config
- Unauthorized ONU List
- Modify ONU Names by Importing EXCEL

10.1 Managing Resource Statistics Template

This chapter introduces how to query and create the resource statistics template.

10.1.1 Viewing Resource Statistical Templates

You can view the resource statistical templates already set and saved. If a template meets your requirements for querying resources of the same conditions, you can use the template directly without the need to set the conditions. This section introduces how to view the resource statistical templates already customized in the UNM2000.



Note:

The name of the manually saved file can be marked with the saving time. You can turn on the switch to mark the saving time in the name of the saved file by modifying the background configuration file. For specific operations, contact the FiberHome technical engineer. The following introduces how to query the NE resource statistical template. The procedures for querying other templates are similar with the only difference in the access method.

Prerequisite

You have the authority of **Inspector Group** or higher authority.

Procedure

1. Select **Resource**→**Resource Statistics** in the main menu to display the **Resource Statistics** tab.
2. In the navigation tree in left pane, select **Resource Statistics**→**Physical Resource Statistics**→**NE Resource Statistics**.
3. Select the NE information list in the **Statistics Template** drop-down list.
4. Click **Custom** next to **Statistics Template** to open the **Custom Template** dialog box to view the existing statistical templates.

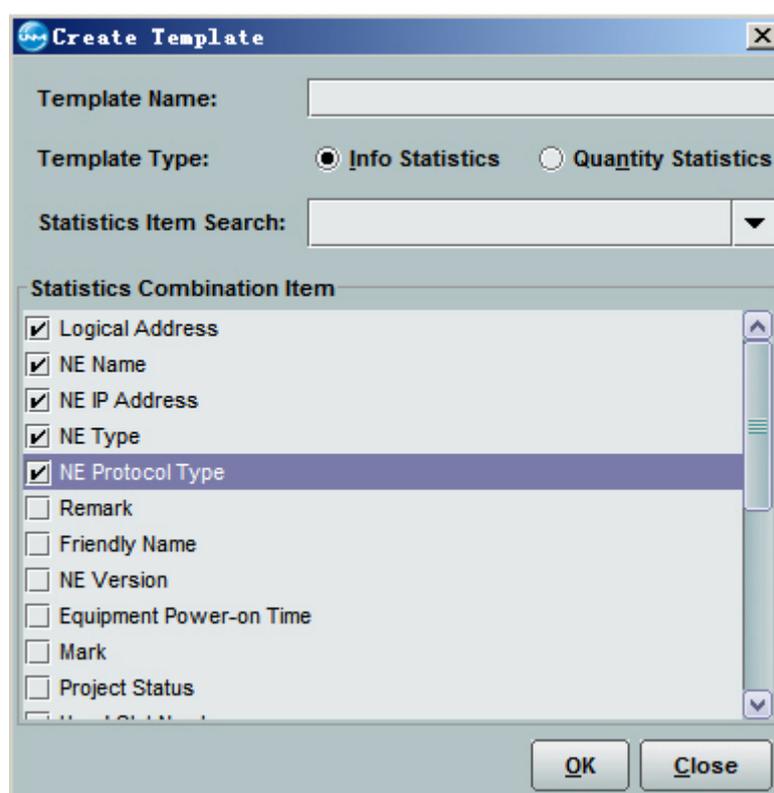
**Note:**

The NE information list and slot usage information list are the system default templates, which cannot be modified or deleted.

Other Operations

When the statistical items set in the template do not meet the requirements for resource statistics, you can modify the created template. The NE information list and slot usage information list are the system default templates and cannot be modified.

1. Select the desired template entry, click **Modify** to open the **Modify the Template** dialog box.



2. Modify the statistical items as needed and click **OK**.

10.1.2 Customizing a Resource Statistical Template

When the existing resource statistical templates in the UNM2000 do not meet the requirements for resource query, you can customize resource statistical templates according to your needs. The following introduces how to customize resource statistical templates in the UNM2000.



Note:

The following uses the NE resource statistical template as an example. You can follow the same procedures to customize other templates with the only difference in the access method.



Caution:

For **PON Device Capability Statistics**, only the default template can be used and no new one can be created.

Prerequisite

You have the authority of **Inspector Group** or higher authority.

Procedure

1. Select **Resource**→**Resource Statistics** in the main menu to display the **Resource Statistics** tab.
2. In the navigation tree in left pane, select **Resource Statistics**→**Physical Resource Statistics**→**NE Resource Statistics**.
3. Select the ONU information list in the **Statistics Template** drop-down list.
4. Click **Custom** next to **Statistics Template** to open the **Custom Template** dialog box to view the existing statistical templates.
5. In the **Custom Template** dialog box, click **Create** to open the **Create Template** dialog box.

6. Set **Template Name**, **Template Type** and **Statistics Combination Item**, and then click **OK**. The added template appears in the **Custom Template** dialog box.
7. Close the **Custom Template** dialog box and the added template appears in the **Statistics Template** drop-down list.

10.2 Physical Resource Statistics

You can understand the NEs, cards, ports, ONUs, ONU ports, MDU ports and other physical resources in the network through the physical resource statistics.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

The procedures for collecting statistics of various physical resources are similar. The following introduces how to collect statistics of NE information list.

1. Select **Resource**→**Resource Statistics** in the main menu to display the **Resource Statistics** tab.
2. In the navigation tree in left pane, select **Resource Statistics**→**Physical Resource Statistics**→**NE Resource Statistics**.
3. Select the ONU information list in the **Statistics Template** drop-down list.
4. Click **Statistics Range** to open the **Select Object** dialog box.
5. Select the desired object or use the search function to select the object quickly. Then click **OK** to view the statistical result.

Logical Address	NE Name	NE IP Address	NE Type	Slot Address	Card Name	Card Type	Card Port Number	Card Port Name	Card Port
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	2	PON2	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	8	PON8	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	1	PON1	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	2	PON2	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	2	PON2	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	7	PON7	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	6	PON6	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	4	PON4	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	6	PON6	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	3	PON3	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	2	PON2	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	3	PON3	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	1	PON1	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	4	PON4	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	3	PON3	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	3	PON3	PON_PORT

Other Operations

Right-click an entry in the statistical result and select **Copy Cell**, **Print** or **Export** from the shortcut menu.

10.3 Resource Statistics of Other Types

Resource statistics of other types include ONU users, local end VLANs, NE MGC services, ONU MGC services, device types, PON device capability, ONU WAN connection service, ONU out-of-service timing length and management VLAN.



Note:

As the procedures for gathering statistics of resources of other types are similar, the following uses the ONU user statistics as an example.

Prerequisite

You have the authority of **Inspector Group** or higher authority.

Procedure

1. Select **Resource** → **Resource Statistics** in the main menu to display the **Resource Statistics** tab.
2. In the left navigation tree, select **Resource Statistics** → **Other Type Resource** → **ONU User Statistics**.

3. Select the ONU information list in the **Statistics Template** drop-down list.
4. Click **Statistics Range** to open the **Select Object** dialog box.
5. Select the desired object or use the search function to select the object quickly. Then click **OK** to view the statistical result.

Logical Address	NE Name	NE IP Address	NE Type	Slot Address	Card Name	Card Type	Card Port Number	Card Port Name	Card Port
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	2	PON2	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	8	PON8	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	1	PON1	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	2	PON2	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	2	PON2	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	7	PON7	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	6	PON6	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	4	PON4	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	6	PON6	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	3	PON3	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	2	PON2	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	3	PON3	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	1	PON1	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	4	PON4	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	5	PON5	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	3	PON3	PON_PORT
GMM134217733.Alabang134217739	ALAFEOL002	10.226.67.194	ANS116-06B	1	GC8B(1)	GC8B	3	PON3	PON_PORT

Other Operations

Right-click an entry in the statistical result and select **Copy Cell**, **Print** or **Export** from the shortcut menu.

10.4 Exporting Physical Resource Statistics

You can export the physical resource statistics to the preset FTP server.



Note:

The procedures of exporting physical resource statistics are similar. In the following the NE resource statistics are exported as an example.

Background Information

The physical resources that can be exported include NE resources, card resources, port resources, ONU resources, ONU port resources and MDU port resources.

Prerequisite

- ◆ The statistical template is set. See [Customizing a Resource Statistical Template](#).
- ◆ The FTP server is set. See [Setting the XFTP Server](#).
- ◆ You have the authority of **Inspector Group** or higher authority.

Procedure

1. Select **Resource**→**Resource Statistics** in the main menu to display the **Resource Statistics** tab.
2. In the left navigation tree, select **Export Statistics**→**Physical Resource Statistics Export**→**Physical Resource Statistics Export** to view the existing export tasks.
3. Execute the following operations as needed.
 - ▶ If the existing task has met the requirements, run the task at the scheduled time; or click **Execute now**, or select **Execute now** from the shortcut menu to start the task.



Note:

The task will automatically run at the scheduled time and the user can obtain the exported statistical information file from the FTP server when the execution result displays **Successful**.

- ▶ If the existing task has not met the requirements, → Step 4.
4. Create a physical resource statistics task.
 - 1) Right-click in a blank area of the GUI and select **Create** from the shortcut menu to open the **Create NE Resource Statistics Export** dialog box.
 - 2) Set the parameters in the **Basic information**, **Object source** and **Extend information** tabs and then click **OK**. The created task appears on the GUI.
 - 3) Select a task and click **Execute Now** or select **Execute Now** from the shortcut menu to execute the task immediately.

Other Operations

Right-click an entry in the statistical result and select the corresponding shortcut menu item to delete, print or export the entry or view the attribute.

10.5 Exporting Resource Statistics of Other Types

You can export statistical information of resources like the ONU users, local end VLANs, NE MGC services, ONU MGC services, device types, ONU WAN connection services, ONU out-of-service time length and management VLAN as needed.



Note:

The procedures of exporting resource statistics of other types are similar. In the following the ONU user statistics are exported as an example.

Prerequisite

- ◆ The statistical template is set. See [Customizing a Resource Statistical Template](#).
- ◆ The FTP server is set. See [Setting the XFTP Server](#).
- ◆ You have the authority of **Inspector Group** or higher authority.

Procedure

1. Select **Resource**→**Resource Statistics** in the main menu to display the **Resource Statistics** tab.
2. In the left navigation tree, select **Export Statistics**→**Statistics Export of Other Types**→**ONU User Statistics Export** to view the existing export tasks.
3. Execute the following operations as needed.
 - ▶ If the existing task has met the requirements, run the task at the scheduled time; or click **Execute now**, or select **Execute now** from the shortcut menu to start the task.



Note:

The task will automatically run at the scheduled time and the user can obtain the exported statistical information file from the FTP server when the execution result displays **Successful**.

- ▶ If the existing task has not met the requirements, → Step 4.
4. Add an ONU user statistical task.
 - 1) Right-click in a blank area of the GUI and select **Create** from the shortcut menu to open the **Create ONU User Statistics Export** dialog box.
 - 2) Set the parameters in the **Basic information**, **Object source** and **Extend information** tabs and then click **OK**. The created task appears on the GUI.
 - 3) Select a task and click **Execute Now** or select **Execute Now** from the shortcut menu to execute the task immediately.

Other Operations

Right-click an entry in the statistical result and select the corresponding shortcut menu item to delete, print or export the entry or view the attribute.

10.6 Example of Resource Statistics

The resource statistics of the UNM2000 manages the physical asset information and important logical configuration of all the devices in the network.

The UNM2000 provides the unified query and statistics functions for the resources in the network. You can understand the resource usage in the network timely via the resource management.



Note:

Considering the users' use preferences, the UNM2000 supports up to 20 thousand data entries and the excessive data will not be displayed. You can export the statistical resources to view all data.

Viewing the Port Usage of the ONU Under a Specified NE

1. Select **Resource**→**Resource Statistics** from the main menu.
 2. Select **Physical Resource Statistics**→**ONU Port Resource Statistics**.
 3. Click **Custom**→**Create** to open the **Create Template** dialog box. Enter the template name, select the template type and the ONU port information entries to be collected, and then click **OK** to create the statistical template.
-



Note:

Template type description:

- ◆ Info statistics: Collects the statistics on basic attributes of the statistical objects.
 - ◆ Quantity statistics: Collects the quantities of the types of the statistical objects.
-

4. Click **Statistics Range**, select the statistical object and click **OK**.

Viewing the Quantity of ONUs of the Specified NE

1. Select **Resource**→**Resource Statistics** from the main menu.
 2. Select **Physical Resource Statistics**→**ONU Resource Statistics**.
 3. Click **Custom**→**Create** to open the **Create Template** dialog box. Enter the template name, select the template type and the ONU port information entries to be collected, and then click **OK** to create the statistical template.
-



Note:

Template type description:

- ◆ Info statistics: Collects the statistics on basic attributes of the statistical objects.
 - ◆ Quantity statistics: Collects the quantities of the types of the statistical objects.
-

4. Click **Statistics Range**, select the statistical object and click **OK**.

Viewing the VLAN Information

1. Select **Resource**→**Resource Statistics** from the main menu.
2. Select **Other Type Statistics**→**Local VLAN Statistics**.
3. Click **Custom**→**Create** to open the **Create Template** dialog box. Enter the template name, select the template type and the VLAN information entries to be collected, and then click **OK** to create the statistical template.
4. Click **Statistics Range**, select the statistical object and click **OK**.

10.7 Importing the ODN NSM Information

Manual creation of ODN view is inefficient and may cause errors. By importing the ODN NMS information, you can quickly establish the ODN network view. After the information is imported, the relationship among NEs (OLT PON port, splitter and ONU) is displayed in the topology. This improves the operation and maintenance efficiency.

Background Information

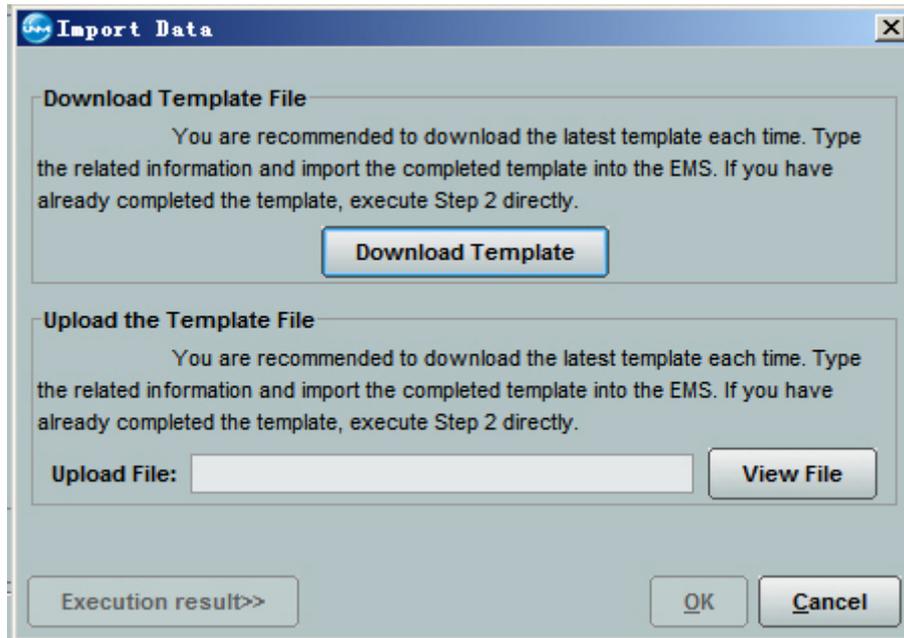
The ODN provides optical transmission channel between the OLT and ONU.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Resource**→**Import ODN NSM Information** from the main menu.
2. Click **Open File** in the lower right corner to bring up the **Import Data** dialog box.



3. Click **Download Template** to save the ODN imported information template to the local computer and then complete the information according the actual project requirement.



Note:

The items marked with * in the template file are required. Please enter the items correctly; otherwise, the file may be failed to be imported.

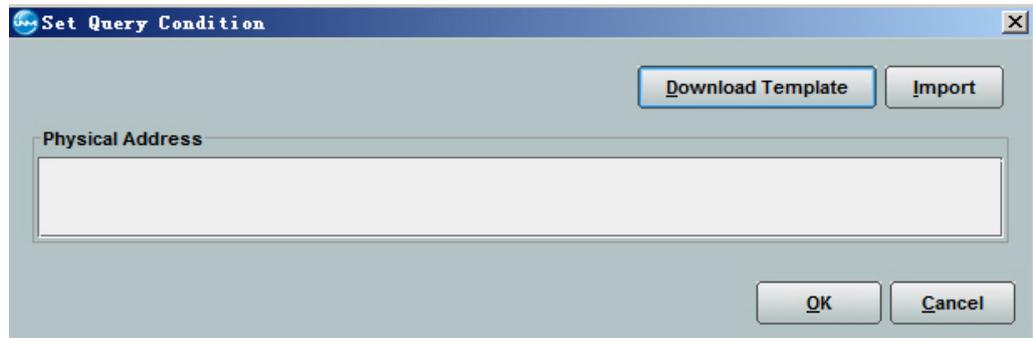
4. Click **Browse File**, select the ODN information file preset and click **OK** to import the data.

10.8 Querying Multiple ONUs

After importing the ONU physical ID table, you can search for the corresponding ONU information (ONU basic information, online status and port VLAN information) according to the ONU physical ID, and deauthorize them in a batch manner.

Procedure

1. On the UNM2000 main menu, select **Resource**→**Batch Query ONU** to open the **Set Query Condition** dialog box.



2. In the **Set Query Condition** dialog box, click **Download Template** to download the ONU physical ID template.
3. Enter the desired ONU physical ID in the ONU physical ID template table.

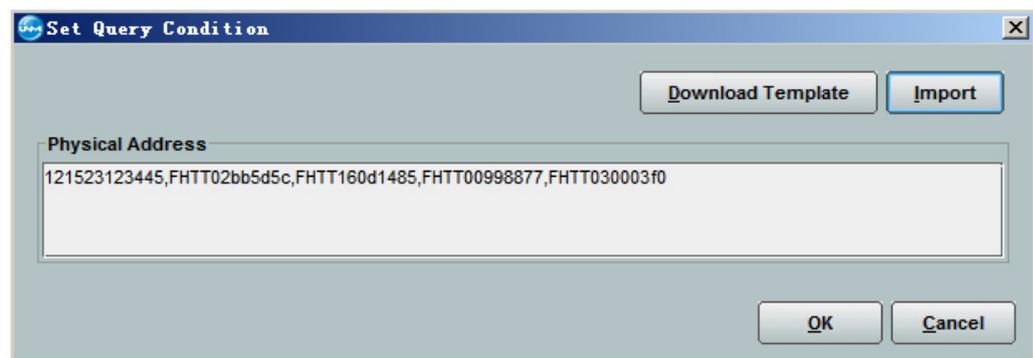


Note:

The ONU physical ID types and value range are described as follows:

- ◆ Physical SN: The first four digits are a ASCII character string (case-sensitive) and the last 8 digits should range from 0 to 9 or a to f (lower-case letters).
- ◆ MAC address: It consists of digits ranging from 0 to 9 or a to f (lower-case letters).

4. In the **Set Query Condition** dialog box, click **Import** to import the ONU physical ID template with physical IDs entered.



5. In the **Set Query Condition** dialog box, click **OK**. The **Batch Query ONU** tab displays the query result.

Device Name	OLT IP	ONU Type	Slot Number	PON Number	ONU Number	Physical Address	Online Status	ONU Public IP	Port Name
PON[1]-HG260[2]	10.171.0.22	HG260	13	1	2	FHTT160d1485	Offline		LAN1
PON[1]-HG260[2]	10.171.0.22	HG260	13	1	2	FHTT160d1485	Offline		iTV
PON[1]-HG260[2]	10.171.0.22	HG260	13	1	2	FHTT160d1485	Offline		LAN3
PON[1]-HG260[2]	10.171.0.22	HG260	13	1	2	FHTT160d1485	Offline		LAN4
PON[1]-HG260[2]	10.171.0.22	HG260	13	1	2	FHTT160d1485	Offline		VOP1
PON[1]-HG260[2]	10.171.0.22	HG260	13	1	2	FHTT160d1485	Offline		VOIP2

10.9 Query Board By Serial Number

You can query the name and management IP of the OLT where the card belongs and the slot number where the card locates according to the serial number of the card. The query range can be all the OLT devices in the network.

Prerequisite

The serial number of the card is obtained.

Procedure

1. Select **Resource** → **Query Board by Serial Number** from the UNM2000 main menu.
2. In the **Set Query Conditions** dialog box, enter the serial number of the card and select one or more OLT device(s).



Note:

- ◆ If you select **Full Field Matching**, enter a complete serial number of the card.
- ◆ If you deselect **Full Field Matching**, fuzzy query is supported.

3. Click **OK**. The **Query Board by Serial Number** tab displays the query result.

NE Logic Address	NE Name	NE IP Address	Slot No	Board Type	Board Name	Serial Number
GMM134217733-Balara	BLRFEOL001	10.251.80.34	15	GC8B	GC8B(15)	12090200037
GMM134217733-Balara	BLRFEOL001	10.251.80.34	16	GC8B	GC8B(16)	120910150114
GMM134217733-Balara	BLRFEOL001	10.251.80.34	17	GC8B	GC8B(17)	121006310187
GMM134217733-North Marikina	MNRFEOL001	10.251.80.94	17	GC8B	GC8B(17)	120910150253
GMM134217733-South Taguig	SOTFEOL001	10.251.80.98	14	GC8B	GC8B(14)	150602960149
GMM134217733-South Taguig	SOTFEOL001	10.251.80.98	15	GC8B	GC8B(15)	150602960196
GMM134217733-South Taguig	SOTFEOL001	10.251.80.98	16	GC0B	GC0B(16)	121147450162
GMM134217733-South Taguig	SOTFEOL001	10.251.80.98	17	GC0B	GC0B(17)	121148490054
GMM134217733-Caanta	CAIFEOL001	10.251.80.86	15	GC8B	GC8B(15)	120910150211
GMM134217733-Caanta	CAIFEOL001	10.251.80.86	16	GC8B	GC8B(16)	120910150285
GMM134217733-Caanta	CAIFEOL001	10.251.80.86	17	GC8B	GC8B(17)	121031450155
GMM134217733-Valenzuela	VALFEOL001	10.251.87.66	11	GC8B	GC8B(11)	120910150143
GMM134217733-Valenzuela	VALFEOL001	10.251.87.66	12	GC8B	GC8B(12)	120910150250
GMM134217733-Valenzuela	VALFEOL001	10.251.87.66	13	GC8B	GC8B(13)	120910150280
GMM134217733-Valenzuela	VALFEOL001	10.251.87.66	14	GC8B	GC8B(14)	121009800056
GMM134217733-Valenzuela	VALFEOL001	10.251.87.66	15	GC8B	GC8B(15)	121031450089
GMM134217733-Valenzuela	VALFEOL001	10.251.87.66	16	GC8B	GC8B(16)	150603480150

10.10 Querying the MDU Phone Number

With the **Query MDU Phone Number** function, you can navigate to the corresponding card and port according to the telephone number of the port. At

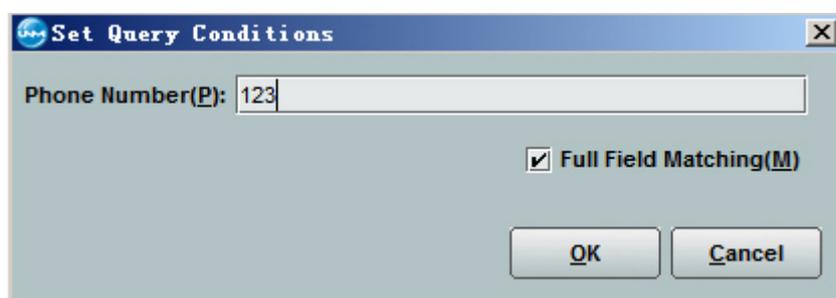
present, this function only supports querying the SIP voice port of the AN5006-20 and AN5006-30.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Resource**→**Query MDU Phone Number** from the UNM2000 main menu.
2. In the **Set Query Conditions** dialog box, enter the **Phone Number**.



Note:

- ◆ If you select **Full Field Matching**, enter a complete phone number.
 - ◆ If you deselect **Full Field Matching**, fuzzy query is supported.
-

3. Click **OK**. The **Query MDU Phone Number** tab displays the query result.

10.11 ONU RMS Error Information Query

You can filter and query the failure information of the ONU RMS and print / export the content in the failure information table.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. In the UNM2000 main menu, select **Resource**→**ONU RMS Error Information Query** to open the **Query ONU RMS Error Information** dialog box.
2. In the **Query ONU RMS Error Information** dialog box, set **Basic Information** and **Advanced Information**.
3. Click **OK**. The **ONU RMS Error Information** tab displays the failure details.

Other Operations

In the **ONU RMS Error Information** tab, right-click an entry and select **Print** or **Export**.

10.12 Querying the ONU Network Access Interception Logs

You can query the ONU network access interception logs through the UNM2000 and print / export the log content.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. On the UNM2000 main menu, select **Resource**→**ONU Network Intercept Log Query** to open the **ONU Network Intercept Log Query** dialog box.
2. In the **ONU Network Intercept Log Query** dialog box, set **Basic Information** and **Advanced Information**.
3. Click **OK**. The **ONU Network Intercept Log Query** tab displays the log information.

Other Operations

In the **ONU Network Intercept Log Query** tab, right-click an entry and select **Print** or **Export**.

10.13 Importing GIS Data in a Batch Manner

You can modify the coordinate of an NE by importing into Excel, improving the configuration efficiency.

Prerequisite

- ◆ You have obtained the NE coordinate data.
- ◆ You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Resource**→**GIS Batch Import** from the main menu.
2. Click **Download Template** to save the Excel template into the designated directory on the UNM2000 client end.
3. Enter the Longitude and Latitude of the NE in the Excel and save it.
4. Click **Import** to bring up the **Open** dialog box.
5. Select the saved Excel file and click **Open**.
6. Click **OK** to import the data into the UNM2000.

10.14 Gateway Type Config

You can configure the gateway types, actual models and manufacturer names of ONU devices of different manufacturers through the UNM2000 so that the gateway types of the ONU devices can be identified when the resource management system delivers the network access configuration of enterprise gateway.

Prerequisite

You have the authority of **Operator Group** or higher authority.

Procedure

1. On the UNM2000 main menu, select **Resource**→**Gateway Type Config** to open the **Gateway Type Config** dialog box.
2. In the **Gateway Type Config** dialog box, click **Add** to open the **Add** dialog box.

3. In the **Add** dialog box, enter the **ONU Vendor** and **ONU Realno** and select the gateway type.
4. Click **Yes** to save the gateway type configuration into the database.

10.15 Unauthorized ONU List

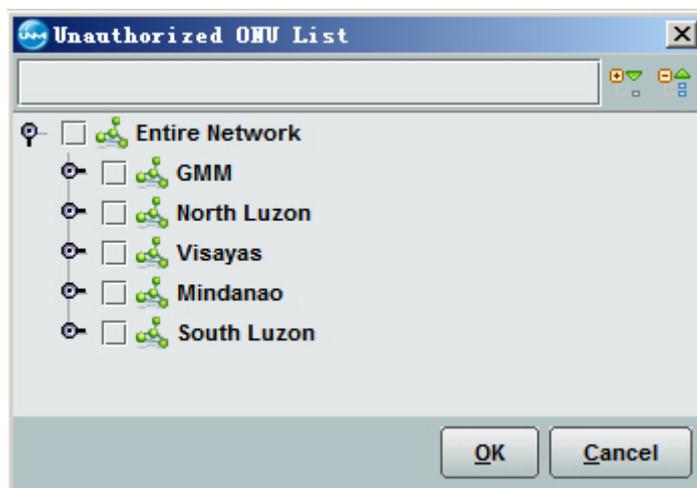
You can obtain the information of all unauthorized ONUs under one or more OLT device(s) through the UNM2000. The information of unauthorized ONUs includes system IP address, slot number, PON port number, ONU type, physical address, physical password, logical ID and logical password.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **Resource**→**Unauthorized OUN List** to open the **Unauthorized OUN List** tab.
2. In the **Unauthorized ONU List** tab, select the object.



3. Click **OK** to query the unauthorized ONU list.

System Name	IP of System	Slot Number	PON Number	ONU Type	Physical Address	Physical password	Logical ID	Logic password
NEANS116-06B_10.171.0.16	10.171.0.16	13	8	AN5006-20	FHTT002928e8			

10.16 Modify ONU Names by Importing EXCEL

You can modify the ONU name by importing into Excel, improving the configuration efficiency.

Prerequisite

- ◆ The ONU name has been planned.
- ◆ You have the authority of **Operator Group** or higher authority.

Procedure

1. Select **Resource**→**Modify ONU Names by Importing EXCEL** in the main menu.
2. Click **Open File** to bring up the **Import Data** dialog box.
3. Click **Download Template** to save the Excel template into the designated directory on the UNM2000 client end.
4. Enter the planned information in the Excel and save it.
5. Click **View File** to open the **Save** dialog box.
6. Select the configured Excel file and click **Save**.
7. Click **Confirm** to import the data into the UNM2000.

11 Data Synchronization and Backup

When the NEs are managed by multiple UNM2000 systems and the NE configuration is modified by one UNM2000 system, the data in other UNM2000 systems are inconsistent with NE data. To ensure consistency of the Network data and NE data and data security, the UNM2000 provides the data synchronization and backup functions.

Managing Data Synchronization Task

Backing Up Data

11.1 Managing Data Synchronization Task

Data synchronization indicates synchronizing the device data with the UNM2000 data. Managing the data synchronization tasks including managing the software / hardware version upgrade tasks, configuration upload tasks and automatic discovery of NEs.

11.1.1 Managing Software / Hardware Version Upgrade Tasks

The software and hardware version upgrade indicates upgrading the software and hardware versions to the UNM2000 database.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Data Synchronization**→**Software&Hardware Version Update Task** to view the existing software and hardware version upgrade tasks.
3. Do as follows:
 - ▶ If the existing tasks can meet the requirements, right-click a task and select **Execute Now**, or select the task and click **Execute Now** at the lower right corner of the tab to execute the software / hardware version upgrade task.
 - ▶ Right-click the task to **Delete**, or view / modify **Attribute**.
4. Click a task in the left pane to view the object information, status and failure reason of the task.

11.1.2 Managing Configuration Upload Tasks

Due to NE maintenance or upgrade / downgrade requirements, you can back up the NE data to the UNM2000 server, client or the third-party FTP server to avoid damage or loss of NE data caused by upgrade / downgrade or unexpected reason.

The configuration upload tasks are used to synchronize the device configuration to the UNM2000 database to ensure consistency of the UNM2000 data and the device data.

11.1.2.1 Viewing Configuration Upload Tasks

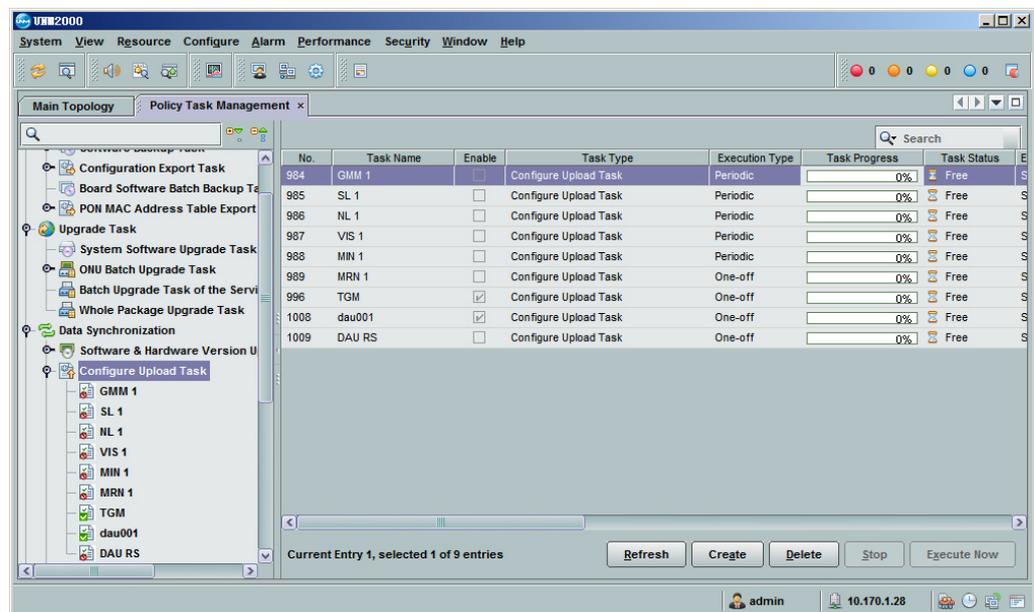
By viewing the configuration upload tasks, you can confirm whether the time of uploading the device configuration to the UNM2000 database and the execution object meet the requirements for data synchronization.

Prerequisite

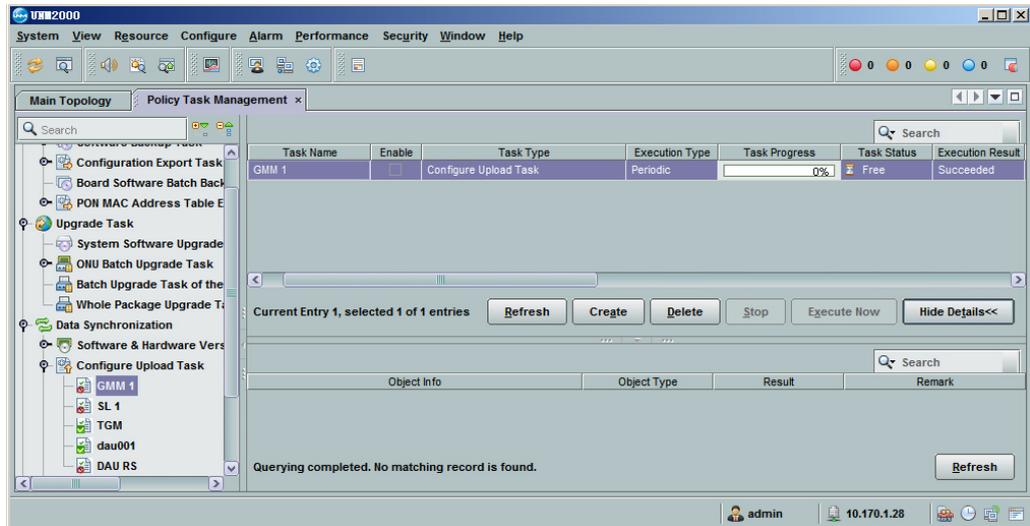
You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Data Synchronization**→**Configuration Upload Task** in the left pane to view the existing configuration upload tasks.



3. In the right pane, right-click a task entry and select **View** to query the object information and status of the task.



Other Operations

In the right pane, right-click the task entry to **Delete**, **Disable**, or view or modify **Attribute**.

11.1.2.2 Creating a Configuration Upload Task

If the existing configuration upload task fails to meet the data synchronization requirement, you can create new configuration upload tasks as required.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Right-click **Configuration Upload Task** in the left pane or right-click in the right pane and select **Create** to open the dialog box.
3. Set the parameters in the **Basic information** and **Object source** tabs as required, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

4. Click a task in the left pane to view the object information and status of the task.

11.1.2.3 Executing Configuration Upload Tasks

You can execute the configuration upload tasks to synchronize the device configuration to the UNM2000 database so as to ensure security and correctness of the UNM2000 data.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Data Synchronization**→**Configuration Upload Task** in the left pane to view the existing configuration upload tasks.

Task Name	Enable	Task Type	Execution Type	Task Progress	Task Status	Execution Result
GMM 1	<input type="checkbox"/>	Configure Upload Task	Periodic	0%	Free	Succeeded
SL 1	<input type="checkbox"/>	Configure Upload Task	Periodic	0%	Free	Succeeded
NL 1	<input type="checkbox"/>	Configure Upload Task	Periodic	0%	Free	Succeeded
VIS 1	<input type="checkbox"/>	Configure Upload Task	Periodic	0%	Free	Succeeded
MIN 1	<input type="checkbox"/>	Configure Upload Task	Periodic	0%	Free	Succeeded
MRN 1	<input type="checkbox"/>	Configure Upload Task	One-off	0%	Free	Succeeded
TGM	<input checked="" type="checkbox"/>	Configure Upload Task	One-off	0%	Free	Succeeded
dau001	<input checked="" type="checkbox"/>	Configure Upload Task	One-off	0%	Free	Succeeded
DAU RS	<input type="checkbox"/>	Configure Upload Task	One-off	0%	Free	Succeeded

3. In the right pane, right-click a task entry and select **View** to query the **Object Info** and **Status** of the task so as to confirm whether the configuration upload task meet the requirements.
4. Right-click a task and select **Execute Now**, or select the task and click **Execute Now** at the lower right corner of the tab to execute the configuration upload task.

11.2 Backing Up Data

To ensure security of the NE data, you can back up the NE data so that you can restore the data when the severe failure occurs in the network. You can manage the configuration backup tasks, including managing software backup task and configuration export tasks.

11.2.1 Managing Software Backup Tasks

The following introduces how to view, create and execute the software backup tasks.

11.2.1.1 Viewing Software Backup Tasks

The following introduces how to view software backup tasks.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Configuration Backup**→**Software Backup Task** in the left pane to view the existing software backup tasks.
3. In the right pane, right-click a task entry and select **View** to query the object information and status of the task.

Other Operations

In the right pane, right-click the task entry to **Delete**, **Disable**, or view or modify **Attribute**.

11.2.1.2 Creating Software Backup Task

If the existing software backup task fails to meet the backup requirement, you can create new tasks as required.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Right-click **Software Backup Task** in the left pane or right-click in the right pane and select **Create** to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

4. Click a task in the left pane to view the object information and status of the task.

11.2.1.3 Executing Software Backup Tasks

The following introduces how to execute software backup tasks.

Prerequisite

- ◆ The FTP server is configured. See [Setting the XFTP Server](#).

- ◆ The service for transmitting files between the client and the server is running normally.
- ◆ You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Configuration Backup**→**Software Backup Task** in the left pane to view the existing software backup tasks.
3. In the right pane, right-click a task entry and select **View** to query the **Object Info** and **Status** of the task so as to confirm whether the software backup task meet the requirements.
4. Right-click a task and select **Execute Now**, or select the task and click **Execute Now** at the lower right corner of the tab to execute the software backup task.

11.2.2 Managing Configuration Export Tasks

This section introduces how to view the data export task information, and how to create a new task and execute operations.

11.2.2.1 Viewing Configuration Export Tasks

By viewing configuration export tasks, you can confirm whether the exported data need to be saved externally.

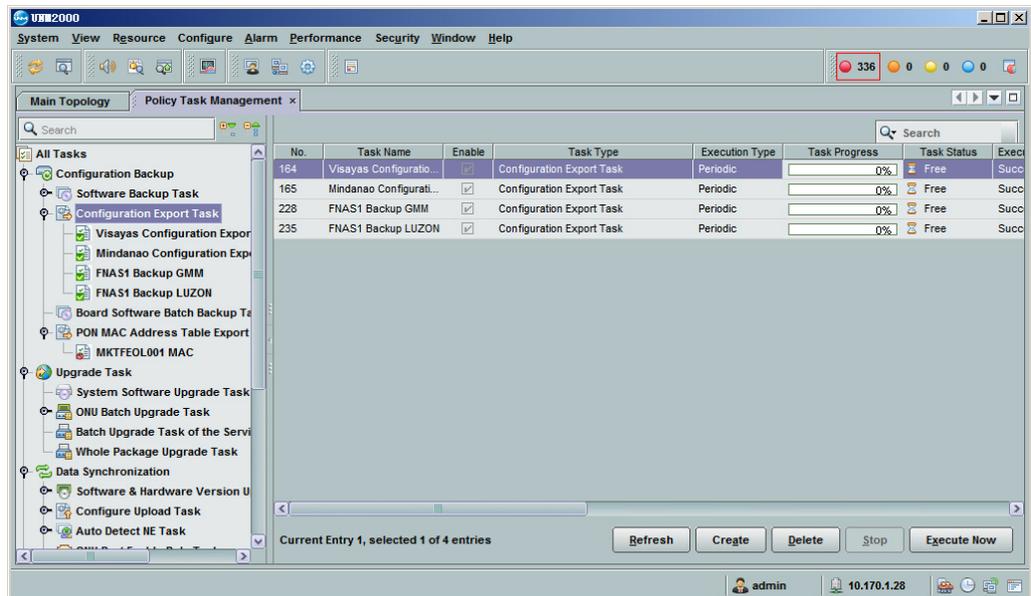
Prerequisite

You have the authority of **Supervisor Group** or higher authority.

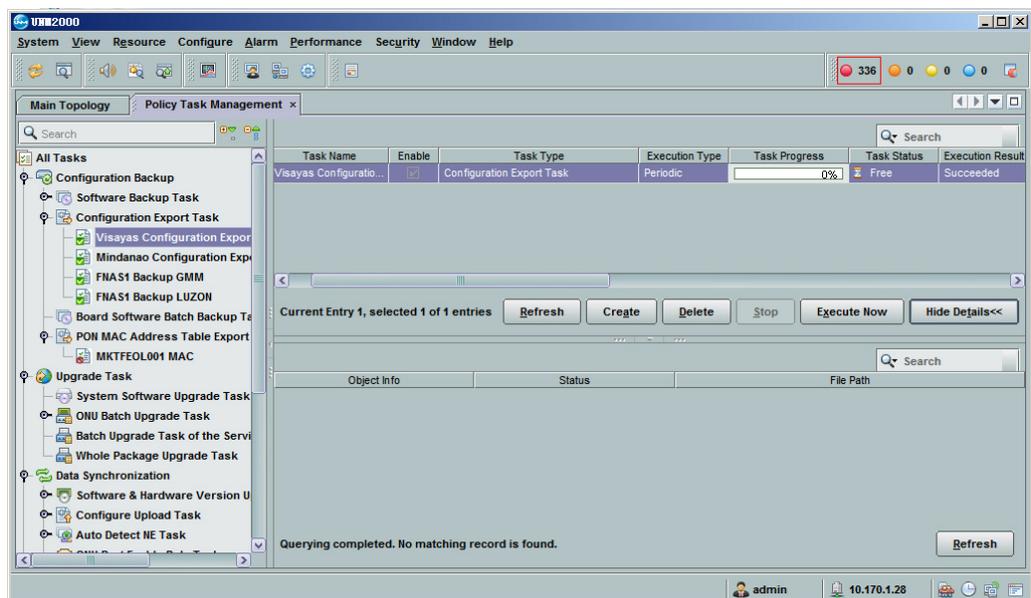
Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.

2. Select **Configuration Backup**→**Configuration Export Task** in the left pane to view the existing configuration export tasks.



3. In the right pane, right-click a task entry and select **View** to query the object information and status of the task.



Other Operations

In the right pane, right-click the task entry to **Delete**, **Disable**, or view or modify **Attribute**.

11.2.2.2 Creating a Configuration Export Task

If the existing configuration export task fails to meet the backup requirement, you can create new configuration export tasks as required.

Prerequisite

You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Right-click **Configuration Export Task** in the left pane or right-click in the right pane and select **Create** to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

4. Click a task in the left pane to view the object information and status of the task.

11.2.2.3 Managing Configuration Export Tasks

The following introduces how to execute the configuration export tasks.

Prerequisite

- ◆ The FTP server is configured. See [Setting the XFTP Server](#).
- ◆ The service for transmitting files between the client and the server is running normally.
- ◆ You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Configuration Backup**→**Configuration Export Task** in the left pane to view the existing configuration export tasks.
3. In the right pane, right-click a task entry and select **View** to query the **Object Info** and **Status** of the task so as to confirm whether the configuration export task meet the requirements.
4. Right-click a task and select **Execute Now**, or select the task and click **Execute Now** at the lower right corner of the tab to export the configuration.

11.2.3 Managing Card Software Backup Tasks

The following introduces how to view, create and execute the card software backup tasks.

11.2.3.1 Viewing the Software Batch Backup Tasks

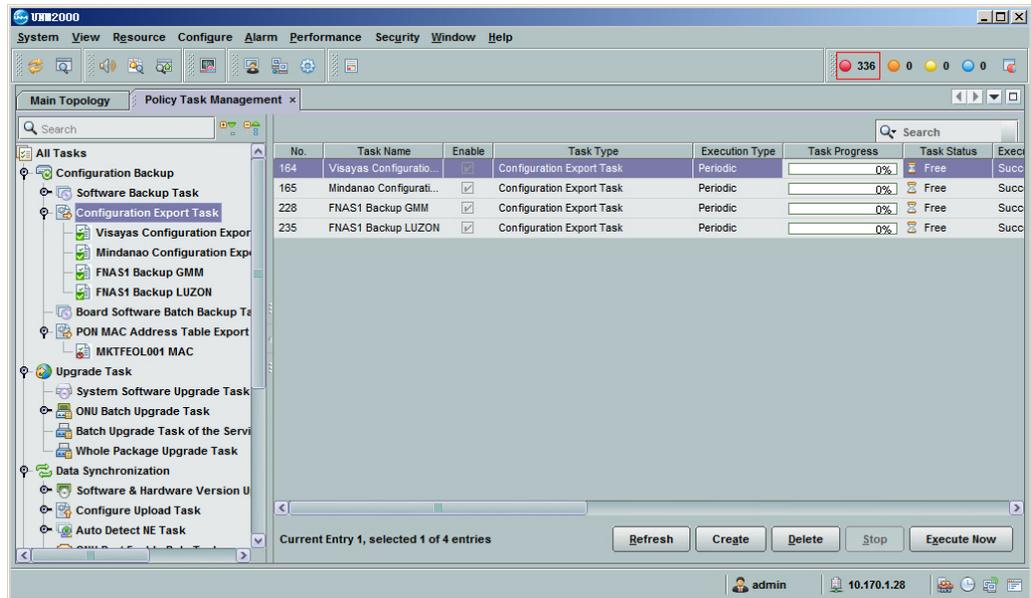
By viewing software backup tasks, you can confirm whether it is needed to add or delete software backup tasks.

Prerequisite

You have the authority of **Supervisor Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Configuration Backup**→**Board Software Batch Backup Task** in the left pane to view the existing configuration export tasks.



3. In the right pane, right-click a task entry and select **View** to query the object information and status of the task.

Other Operations

In the right pane, right-click the task entry to **Delete**, **Disable**, or view or modify **Attribute**.

11.2.3.2 Creating Software Backup Task

If the existing software backup task fails to meet the backup requirement, you can create new tasks as required.

Prerequisite

You have the authority of **Inspector Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** from the main menu to open the **Policy Task Management** tab.
2. Select **Configuration Backup**→**Board Software Batch Backup Task** in the left pane.

- In the right pane, click **Create** to open the **Create Board Software Batch Backup Task** dialog box.

- Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

- Click a task in the left pane to view the object information and status of the task.

11.2.3.3 Executing Software Backup Tasks

The following introduces how to execute software backup tasks.

Prerequisite

- ◆ The FTP server is configured. See [Setting the XFTP Server](#).
- ◆ The service for transmitting files between the client and the server is running normally.
- ◆ You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Configuration Backup**→**Board Software Batch Backup Task** in the left pane to view the existing tasks.
3. In the right pane, right-click a task entry and select **View** to query the **Object Info** and **Status** of the task so as to confirm whether the configuration export task meet the requirements.
4. Right-click a task and select **Execute Now**, or select the task and click **Execute Now** at the lower right corner of the tab to export the configuration.

11.2.4 Export Tasks of MAC Address Table

The export task of MAC address table support exporting the MAC address table of the PON port or OLT, which can be set by the MAC address type. The following mainly introduces how to view, create and execute the export tasks of MAC address table.

11.2.4.1 Viewing Export Tasks of MAC Address Table

By viewing the export tasks of MAC Address Table, you can confirm whether it is needed to add or delete the export tasks of MAC address table.

Prerequisite

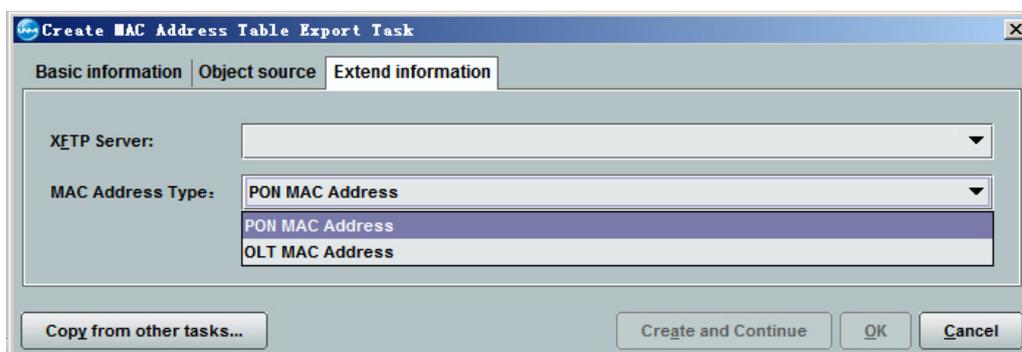
You have the authority of **Inspector Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Configuration Backup**→**MAC Address Table Export Task** in the left pane to view the existing configuration export tasks.
3. In the right pane, right-click a task entry and select **View** to query the object information and status of the task.

Other Operations

In the right pane, right-click a task entry and select **Attribute** to view the MAC address type of the task.



11.2.4.2 Adding an Export Task of MAC Address Table

If the existing task fails to meet the backup requirement, you can create new export tasks of MAC address table.

Prerequisite

You have the authority of **Inspector Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** from the main menu to open the **Policy Task Management** tab.
2. Select **Configuration Backup**→**MAC Address Table Export Task** in the left pane.
3. Click **Create** in the right pane to open the dialog box.

4. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required, and click **OK**. The new task appears in the task list.



Note:

Click **Copy from other tasks** to copy all settings except **Task Name** from other templates. This improves the setting efficiency.

5. Click a task in the left pane to view the object information and status of the task.

11.2.4.3 Executing Export Tasks of MAC Address Table

The following introduces how to execute the export task of MAC address table.

Prerequisite

- ◆ The FTP server is configured. See [Setting the XFTP Server](#).
- ◆ The service for transmitting files between the client and the server is running normally.
- ◆ You have the authority of **Maintainer Group** or higher authority.

Procedure

1. Select **System**→**Policy Task Management** in the main menu to open the **Policy Task Management** window.
2. Select **Configuration Backup**→**MAC Address Table Export Task** in the left pane to view the existing tasks.
3. In the right pane, right-click a task entry and select **View** to query the **Object Info** and **Status** of the task so as to confirm whether the configuration export task meet the requirements.
4. Right-click a task and select **Execute Now**, or select the task and click **Execute Now** at the lower right corner of the tab to export the configuration.

12 Application Scenarios

The following introduces the common application scenarios of the UNM2000.

- Alarm Management
- Performance Management
- Authorization and Domain Division
- Guaranteeing Device Configuration

12.1 Alarm Management

Alarm management module performs real-time monitoring on the faults and abnormalities generated during the equipment operation and provides detailed information and analysis of the alarm, so as to help users to isolate the faults and handle them quickly.

Background Information

The UNM2000 classifies the alarms into the current alarms and the alarm history according to the alarm statuses.

- ◆ Current alarm: the alarm data saved in the current alarm database of the UNM2000.

The alarm frequently generated by the same object will be displayed as one entry in the current alarm list, and the frequency column shows the generation times of the alarm. You can view the alarm log to query all the alarm records.

- ◆ Alarm history: the current alarms that have been confirmed and cleared will be added into the alarm history after a preset period.

The alarm history will be saved into the alarm history database from the current alarm database. See [Setting the Definition of the Alarm History](#) regarding how to set the delay time for transferring the current alarms to the alarm history.

Alarm Operation Description

The UNM2000 provides abundant alarm management functions. The user can refer to Table 12-1 and choose the corresponding function to monitor and handle the alarms.

Table 12-1 Alarm Operation Description

Operation	Description	Related Function
Preset alarm parameters	Set the alarm parameters, including alarm sound, alarm automatic synchronization policy and alarm history definition.	For setting the alarm parameters, see Setting Alarm Related Parameters .
Monitor alarms	Monitor the alarms to obtain the alarm information.	For viewing the current alarms, see Viewing current alarms .

Table 12-1 Alarm Operation Description (Continued)

Operation	Description	Related Function
		For viewing the alarm history, see Viewing Alarm History .
		For viewing reported alarms, see Viewing Reported Alarms .
		For viewing alarm logs, see View alarm logs..
		For viewing statistics of alarm logs, see Viewing the Alarm Log Statistics .
		For viewing alarm statistics, see Viewing Alarm Statistics .
	To obtain accurate alarm information, synchronize the alarms to make the alarms displayed in the UNM2000 consistent with device alarms.	For synchronizing alarms, see Synchronizing Alarms .
	Customize the alarm names or levels according to the maintenance requirements for convenient management and efficient alarm monitoring.	For customizing alarm names, see Custom Alarm Name .
		For customizing alarm levels, see Custom Alarm Level .
	To make sure the related staff are notified timely upon occurrence of failures, you need to set the alarm notification mode in advance, including the alarm sound, alarm reporting rules and remote notification rules.	For managing remote alarm notification, see Alarm / Event Remote Notification .
		For enabling / disabling alarm alert sound, see Enabling / Disabling the Audio Alarm .
For setting the alarm reporting rule, see Viewing Alarm Reporting Rules .		
Collect failure information and analyze the failure reason.	Collects failure information by viewing alarm details, locating alarms and viewing alarm-related operations and then analyzes the failure reason.	For viewing the alarm details, see Viewing Alarm Details .
		For locating the alarms, see Locating Alarms .
		For viewing related alarms, see Viewing Related Alarms .
		For outputting alarm information, see Exporting the Alarm Information .
		View root / derivative alarms.

Table 12-1 Alarm Operation Description (Continued)

Operation	Description	Related Function
Eliminate failures	Eliminate the failures that trigger the alarms according to the related manuals and alarm details.	For viewing the alarm details, see Viewing Alarm Details .
Handle alarms	After a failure is eliminated, the corresponding alarms will be cleared automatically. If the alarms cannot be cleared automatically, you can remove them manually.	For clearing the alarms manually, see Clearing Alarms Manually .
	When the device is maintained, tested or commissioned, there will be a relatively great number of reported alarms. For those alarms that do not required to be focused, you can set the alarm shield to shield the alarms matching the conditions.	For filtering alarms, see Shielding Alarms .
		For managing alarm shield rules, see Viewing Alarm Filter Rules .
		For setting project alarm shield, see Setting the Project Alarm Filtering .
Confirm alarms	When an alarm is confirmed, this alarm is processed.	For confirming alarms, see Confirming Alarms .
Confirm and clear alarms	Confirm and clear alarms at the same time, and save the alarm to the alarm database.	For confirming and clearing alarms, see Confirming and Clearing Alarms .
Record alarm maintenance experience	When the failure is processed, you can record the alarm maintenance experience to the alarm database.	For editing the alarm maintenance experience, see Editing Alarm Maintenance Experience .
		For managing the alarm maintenance experience, see Managing Maintenance Experience .
Save alarm history	Save the alarm history to improve the NE running efficiency.	For managing history data saving, see Managing the Alarm / Event Data .

12.2 Performance Management

The following introduces performance management function, helping you effectively understand the service running status in a specified period of time.

Background Information

The performance data include the current performance data, real-time performance data and performance history data.

- ◆ **Current performance:** Indicates the current 15-minute performance and the performance of the latest sixteen 15-minute time intervals. The current performance data are not saved in the database.
- ◆ **Real-time Performance:** Indicates the performance data collected and displayed in real time. The collection period can be 10 seconds or 30 seconds; the collection interval can be 15 minutes, 30 minutes, one hour, or 24 hours. The performance data will not saved in the database.
- ◆ **Performance history:** Indicates the performance data collected according to the performance collection task and saved into the database.

Performance Operation Description

The UNM2000 provides abundant performance management functions. You can refer to Table 12-2 and choose the corresponding performance function to effectively monitor the running status of the NE service.

Table 12-2 Performance Operation Description

Operation	Description	Related Function
Enable the NE performance classification switch	As there are many performance indexes with great amount of performance data, the UNM2000 disables the performance classification switch of the device by default. Therefore, you need to enable the performance classification switch before querying the NE performance data.	-
Manage performance collection	Collect performance data or monitor performance quality through the performance collection task.	For managing performance collection tasks, see Managing Performance Collection Tasks .
	By managing performance indicator sets, you can quickly set the collection indicator of the performance collection task.	For managing performance indicator set, see Managing Performance Indicator Sets .
	You can monitor the performance data by setting the performance threshold. If the performance data exceeds the preset threshold value, the threshold crossing alarm will be generated.	For managing performance threshold set, see Managing Performance Threshold Sets .

Table 12-2 Performance Operation Description (Continued)

Operation	Description	Related Function
Monitor performance data	Obtain performance data by monitoring performance.	For viewing the current performance, see Viewing the Current Performance .
		For viewing the real-time performance, see Viewing Real-time Performance .
		For viewing the performance history, see Viewing Performance History .
		For viewing the performance history trend, see View Performance History Trend .
		For viewing the performance comparison, see Viewing the Performance Comparison .
Save performance history data	Save the performance history data to improve the NE running efficiency.	For managing history data saving, see Managing Performance Data .

12.3 Authorization and Domain Division

The following takes assigning authority for users in two areas as example to introduce how to create user accounts and assign authority.

Scenario Description

The devices in Area A and Area B are managed by UNM2000 for uniform supervision. The device in Area A is monitored, operated and maintained by working staff in Area A and the device in Area B is monitored, operated and maintained by working staff in Area B. Therefore, the working staff in Area A and Area B should be allocated with user accounts and authority respectively.

Procedure

1. Create object sets.

Create object set A and object set B according to the area division. Add the devices of Area A and Area B to the members of object set A and object set B.

For creating object sets, see [Creating an Object Set](#).

2. Create operation sets.

Adopt the default operation sets according to the users' responsibilities.

- ▶ The working staff responsible for monitoring: the application supervisor set and the network supervisor set.
- ▶ The working staff responsible for operation: the application operator set and the network operator set.
- ▶ The working staff responsible for maintenance: the application maintainer set and the network maintainer set.

For creating operation sets, see [Creating Operation Groups](#).

3. Create user groups.

According to the users' responsibilities, it is required to create six user groups, as shown in Table 12-3.

Table 12-3 Creating User Groups

User Group Name	User Group Type	Management Domain	Operation Authority
Inspector Group A	Common user group	Object Group A	Application supervisor set and network supervisor set
Operator Group A	Common user group	Object Group A	Application operator set and network operator set
Maintainer Group A	Common user group	Object Group A	Application maintainer set and network maintainer set
Inspector Group B	Common user group	Object Group B	Application supervisor set and network supervisor set
Operator Group B	Common user group	Object Group B	Application operator set and network operator set
Maintainer Group B	Common user group	Object Group B	Application maintainer set and network maintainer set

For details of creating user groups, see [Creating User Groups](#).

4. Create users.

- ▶ Create the user's basic information. Set the username and password. For security, select **Modify Password on Next Login** or set the valid days of the password.
- ▶ Set the login time ranges according to the working shifts of the staff.
- ▶ Set the users' user groups. If six user groups A, B, C, D, E, and F are to be created, as shown in Table 12-4. After being assigned with a user group,

the user will be authorized with the management domain and operational authority of the user group.

Table 12-4 Creating Users

User	User Group
A	Inspector Group A
B	Operator Group A
C	Maintainer Group A
D	Inspector Group B
E	Operator Group B
F	Maintainer Group B

- ▶ Set the access control list to restrict users' login IP address to the specified ones.

For details of creating user groups, see [Creating Users](#).

After completing the above configurations, provide the user accounts for the corresponding staff.

12.4 Guaranteeing Device Configuration

To avoid that unexpected events, such as device failure, communication interruption between the UNM2000 and the device and power failure, influence the service recovery, the UNM2000 provides some functions for guaranteeing the device configuration.

Backing Up Configuration

- ◆ When you need to compare whether the device configuration is the same as that in the UNM2000 database, you can configure the synchronization operation to view whether each configuration is the same. If not, you can manually synchronize the device configuration to the UNM2000 database or synchronize the configuration in the UNM2000 database to the device. For specific operations, see [Configuration Synchronization](#).

- ◆ To avoid device failures, you can set the execution period as needed so that the device configuration will be automatically uploaded to the UNM2000 database on a regular basis, which is convenient for restoring the configuration after the device failure is eliminated. For specific operations, see [Managing Configuration Upload Tasks](#).
- ◆ To avoid that the device and the UNM2000 server become faulty at the same time, you can set the execution period so that the device configuration will be automatically exported and saved to another FTP server on a regular basis to ensure that the device configuration will not be lost. For specific operations, see [Managing Configuration Export Tasks](#).

Backing Up Software

To avoid upgrade failure of device software, you can set the execution period as need so that the device configuration will be automatically exported and saved to another FTP server on a regular basis, which is convenient for quickly restoring the device software. For specific operations, see [Managing Software Backup Tasks](#).

Appendix A Abbreviations

BML	Business Management Layer
BMS	Business Management System
CORBA	Common Object Request Broker Architecture
CPU	Central Processing Unit
DCC	Data Communication Channel
DCN	Data Communication Network
DDN	Digital Data Network
EML	Element Management Layer
EMS	Element Management System
EPON	Ethernet Passive Optical Network
GPON	Gigabit-Capable Passive Optical Network
FTP	File Transfer Protocol
GE	Gigabit Ethernet
GNE	Gate Network Element
GUI	Graphic User Interface
IP	Internet Protocol
ITU-T	International Telecommunication Union- Telecommunication Standardization Sector
NE	Network Element
NEL	Network Element Level
NML	Network Management Layer
NMS	Network Management System
OLT	Optical Line Terminal
ONT	Optical Network Terminal
ONU	Optical Network Unit
RMS	Resources Management System
SML	Service Management Layer
SMS	Service Management System
TCP	Transfer Control Protocol
TL1	Transaction Language 1
TMN	Telecommunications Management Network

UDP	User Datagram Protocol
UPS	Uninterrupted Power System

Product Documentation Customer Satisfaction Survey

Thank you for reading and using the product documentation provided by FiberHome. Please take a moment to complete this survey. Your answers will help us to improve the documentation and better suit your needs. Your responses will be confidential and given serious consideration. The personal information requested is used for no other purposes than to respond to your feedback.

Name	
Phone Number	
Email Address	
Company	

To help us better understand your needs, please focus your answers on a single documentation or a complete documentation set.

Documentation Name	
Code and Version	

Usage of the product documentation:

1. How often do you use the documentation?

Frequently Rarely Never Other (please specify) _____

2. When do you use the documentation?

in starting up a project in installing the product in daily maintenance in trouble shooting Other (please specify) _____

3. What is the percentage of the operations on the product for which you can get instruction from the documentation?

100% 80% 50% 0% Other (please specify) _____

4. Are you satisfied with the promptness with which we update the documentation?

Satisfied Unsatisfied (your advice) _____

5. Which documentation form do you prefer?

Print edition Electronic edition Other (please specify) _____

Quality of the product documentation:

1. Is the information organized and presented clearly?

Very Somewhat Not at all (your advice) _____

2. How do you like the language style of the documentation?

Good Normal Poor (please specify) _____

3. Are any contents in the documentation inconsistent with the product?

4. Is the information complete in the documentation?

Yes

No (Please specify) _____

5. Are the product working principles and the relevant technologies covered in the documentation sufficient for you to get known and use the product?

Yes

No (Please specify) _____

6. Can you successfully implement a task following the operation steps given in the documentation?

Yes (Please give an example) _____

No (Please specify the reason) _____

7. Which parts of the documentation are you satisfied with?

8. Which parts of the documentation are you unsatisfied with?Why?

9. What is your opinion on the Figures in the documentation?

Beautiful Unbeautiful (your advice) _____

Practical Unpractical (your advice) _____

10. What is your opinion on the layout of the documentation?

Beautiful Unbeautiful (your advice) _____

11. Thinking of the documentations you have ever read offered by other companies, how would you compare our documentation to them?

Product documentations from other companies:_____

Satisfied (please specify) _____

Unsatisfied (please specify) _____

12. Additional comments about our documentation or suggestions on how we can improve:

Thank you for your assistance. Please fax or send the completed survey to us at the contact information included in the documentation. If you have any questions or concerns about this survey please email at edit@fiberhome.com