



UNM2000

**Network Convergence
Management System**

Operation Guide

Version: B

Code: MN000001822

FiberHome Telecommunication Technologies Co., Ltd.

June 2016

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

Related Documentation

Document	Description
UNM2000 Network Convergence Management System Product Description	Introduces the functions, application scenarios and technical specifications of the UNM2000 Network Convergence Management System.
UNM2000 Network Convergence Management System Installation Guide (Based on Windows)	Introduces how to install the UNM2000 Network Convergence Management System on the Windows operating system.
UNM2000 Network Convergence Management System Installation Guide (Based on Linux)	Introduces how to install the UNM2000 Network Convergence Management System on the SUSE Linux operating system.
UNM2000 Network Convergence Management System Operation Guide	Introduces the operation guidelines of the UNM2000 Network Convergence Management System.

Version

Version	Description
A	Initial version.
B	Adds the new functions and operation methods of the UNM2000 R0106, R0106SP1 and R0106SP2 versions.

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

Conventions

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, first 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.



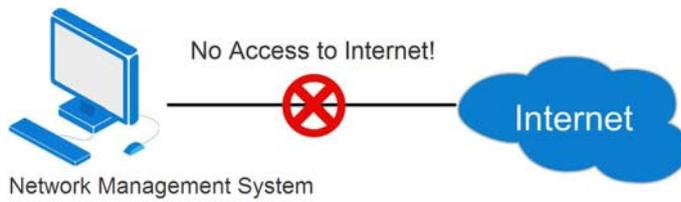
The network management computer cannot be used for purposes other than network management. Use of unidentified memory devices should be prohibited so as to avoid computer viruses.



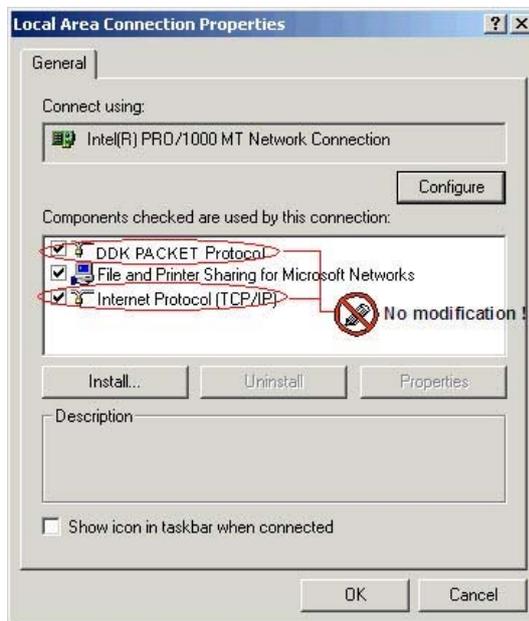
Do not delete any file in the network management system randomly or copy any irrelevant file into the network management computer.

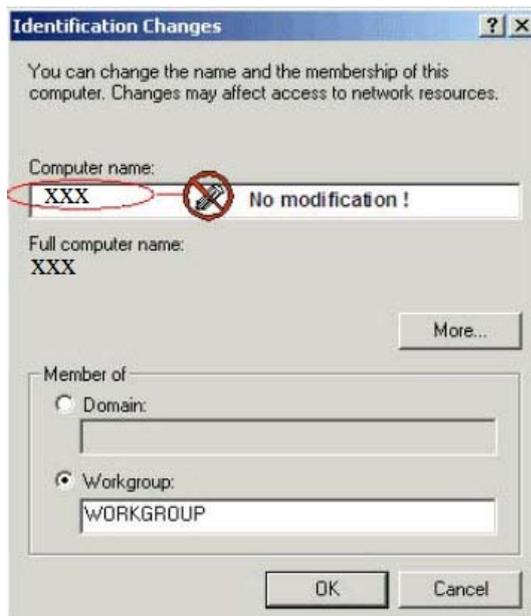
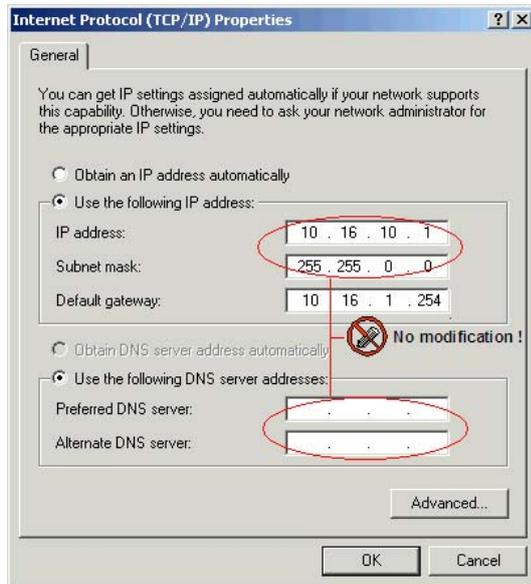


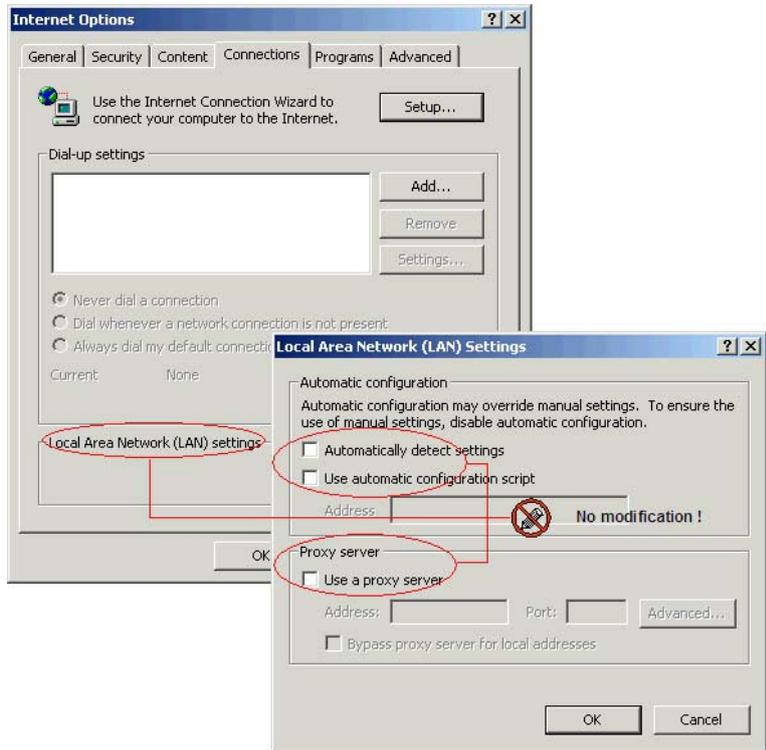
Do not visit Internet via the network management computer. Doing so may increase data flow in the net card and hence affects normal network management data transmission or results in other accidents.



- ⚠ 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
Related Documentation	I
Version	II
Intended Readers	II
Conventions	III
Operation Safety Rules.....	V
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 Logging into the UNM2000 Client End.....	5
2.1.2 Exiting the UNM2000 Client End	6
2.2 Viewing the UNM2000 Version.....	6
2.3 GUI Introduction	7
2.3.1 GUI	7
2.3.2 Shortcut Icons.....	7
2.3.3 General Shortcut Keys.....	10
2.4 Menu Description.....	11
2.4.1 System.....	11
2.4.2 View	12
2.4.3 Resource.....	14
2.4.4 Configuration	16
2.4.5 Alarm.....	16
2.4.6 Performance.....	18
2.4.7 Security	18
2.4.8 Window	19
2.4.9 Help	19
2.5 Setting System Parameters.....	20

	2.5.1	Setting the Display Style of the Browse Tree	20
	2.5.2	Setting the Time Mode	21
	2.5.3	Setting the Topology Display	22
	2.5.4	Setting Ping Parameters	24
	2.5.5	Setting the Telnet Proxy Server	25
	2.5.6	Setting the GUI Display Mode	25
2.6		Setting the FTP Server.....	26
2.7		Setting the Default Workspace	27
2.8		Basic Operations of the UNM2000	28
	2.8.1	Upgrading the License	28
	2.8.2	Modifying the Password.....	29
	2.8.3	Lock the Terminal.....	29
	2.8.4	Logging Out of the Current Account.....	30
	2.8.5	Viewing the Message Platform	31
	2.8.6	Managing Toolbars	31
	2.8.7	Creating a Custom View.....	33
3		Security Management.....	34
	3.1	User Security Concepts	35
	3.2	User Security Policy Management.....	38
	3.2.1	Setting the User Login Mode	38
	3.2.2	Setting the ACL	39
	3.2.3	Setting the Account Policy.....	40
	3.2.4	Setting the Password Policy.....	41
	3.3	Managing Network Management Users.....	42
	3.3.1	Operation Set Management	42
	3.3.2	Object Set Management	45
	3.3.3	User Group Management.....	48
	3.3.4	User Management	52
	3.4	Managing User Sessions	58
	3.4.1	Monitoring User Sessions	59
	3.4.2	Logging Out Users.....	60
	3.4.3	Sending Messages to Online Users.....	61
	3.4.4	Monitoring User Activities.....	62
	3.5	Authorization and Domain Division.....	63

4	Configuration Management.....	66
4.1	NE Communication Route Management.....	67
4.1.1	NE Management Program.....	67
4.1.2	Partition Policy Management.....	71
4.2	SNMP Parameter Template.....	73
4.2.1	Creating and Using the SNMP Parameter Template.....	73
4.2.2	Modifying / Deleting an SNMP Parameter Template.....	75
4.3	Managing Global Templates.....	76
4.3.1	Viewing the Global Template.....	76
4.3.2	Adding a Global Template.....	77
4.3.3	Modifying a Global Template.....	78
4.3.4	Binding / Unbinding a Global Template.....	80
4.3.5	Deleting a Global Template.....	81
4.4	Global Configuration Management.....	83
4.4.1	Viewing the Global Template.....	83
4.4.2	Adding the Global Configuration.....	84
4.4.3	Modifying the Global Configuration.....	84
4.4.4	Binding / Unbinding the Global Configuration.....	85
4.4.5	Deleting a Global Configuration Template.....	86
4.5	Tracing Signaling.....	87
4.6	Configuration Synchronization.....	88
4.7	Network Access Management.....	90
4.8	Home Gateway MAC Range Configuration.....	91
4.9	Pre-deploying ONUs.....	93
4.10	Pinging NEs.....	94
4.11	Telneting NEs.....	95
4.12	The Tracert Function of the UNM2000 Server.....	95
4.13	PON Configuration Transfer.....	96
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	Creating an Access NE	101
	5.3.2	Creating Other NEs.....	102
	5.3.3	Automatic Discovery of NEs.....	103
5.4		Adding Cards.....	107
	5.4.1	Adding Cards Automatically	108
	5.4.2	Adding Cards Manually	109
5.5		Creating a Virtual Connection.....	110
5.6		Editing NEs.....	111
	5.6.1	Setting NE Attributes.....	111
	5.6.2	Editing Icons	112
	5.6.3	Setting the Displayed Contents of the Icon	113
	5.6.4	Tagging NEs	113
	5.6.5	Querying a Label	114
	5.6.6	Modify NE Names in a Batch Manner	114
5.7		Editing a Fiber Connection	118
	5.7.1	Modifying the Connection Line Properties.....	119
	5.7.2	Setting the Display Mode of the Connection Line	119
5.8		Checking the Topology View	120
	5.8.1	Checking the Physical Topology View	120
	5.8.2	Viewing the Sub-topology View	121
	5.8.3	Viewing the Thumbnail.....	123
	5.8.4	Searching Objects	123
5.9		Deleting the Topology	124
	5.9.1	Deleting the Global Logical Domain.....	124
	5.9.2	Delete NEs	125
	5.9.3	Deleting the System.....	125
	5.9.4	Deleting Cards.....	126
6		Managing Access NEs.....	127
	6.1	The NE Manager GUI	128
	6.2	Configuring Local Services.....	129
	6.3	ONU Query Management	130
	6.3.1	Querying ONUs	130
	6.3.2	Viewing the ONU List.....	131
	6.3.3	ONU Query Example	133

6.4	Authorizing ONUs	134
6.4.1	Configuring the ONU Whitelist.....	134
6.4.2	Managing ONU Authentication Modes.....	135
6.4.3	Managing PON Port Authentication Modes.....	137
6.4.4	Replacing the ONU Logical Identifier.....	139
6.4.5	Viewing the Authorized ONU Information.....	139
6.5	ONU Registration Management	140
6.5.1	Querying the ONU RMS Error Information	141
6.5.2	Querying the ONU Network Access Interception Logs	141
6.6	Rule Tasks of Enabling the ONU Port.....	141
6.6.1	Viewing Rule Tasks.....	142
6.6.2	Adding a Rule Task.....	142
6.6.3	Executing Rule Tasks.....	143
6.7	Authorizing Cards	143
6.8	Synchronizing ONUs Manually.....	145
6.9	Obtaining Unauthorized ONUs	145
6.10	Authorizing ONUs Manually	147
6.11	Comparing and Synchronizing the ONU Manually	147
6.12	Querying the Card Software / Hardware Versions	148
6.13	Upgrading the Card.....	149
6.13.1	Tasks of Upgrading the System Software	150
6.13.2	Tasks of Upgrading ONUs in a Batch Manner	152
6.13.3	Batch Upgrade Task of Service Cards	155
6.14	Managing the Test Task	157
6.14.1	Managing POTS Port Internal / External Line Test Tasks..	157
6.14.2	Managing the Task of VoIP Pinging Test.....	159
6.15	Managing ONU MGC Query Tasks.....	162
6.16	Managing NE Automatic Discovery Tasks	163
6.16.1	Viewing NE Automatic Discovery Tasks.....	163
6.16.2	Adding an NE Automatic Discovery Task.....	164
7	Alarm Management	165
7.1	Basic Concepts.....	166

7.2	Setting Alarm Related Parameters	170
7.2.1	Managing Alarm Reporting Rules.....	170
7.2.2	Managing Alarm Filter Rules	172
7.2.3	Setting the Audible Alarms	176
7.2.4	Enabling / Disabling the Audio Alarm.....	177
7.2.5	Setting the Display Modes of New Alarms / Events	178
7.2.6	Setting the Alarm Color	179
7.2.7	Setting Other Items of the Local Alarms.....	180
7.2.8	Setting the Alarm Automatic Synchronization Policy	180
7.2.9	Setting the Definition of the Alarm History	181
7.2.10	Setting the Alarm Automatic Confirmation Rules.....	182
7.2.11	Converting Events to Alarms	183
7.2.12	Customizing Alarms	183
7.3	Managing Alarm / Event Templates	187
7.3.1	Alarm Template.....	187
7.3.2	Event Template	192
7.4	Synchronizing Alarms	195
7.4.1	Synchronizing Alarms Manually	195
7.4.2	Synchronizing Alarms Automatically.....	196
7.5	Monitoring Network Alarms	196
7.5.1	Viewing Current Alarms	197
7.5.2	Viewing Alarm History	199
7.5.3	Viewing Related Alarms	202
7.5.4	Viewing Alarm Details	202
7.5.5	Viewing Alarm Logs	204
7.5.6	Viewing Statistical Data of the Alarm Logs.....	206
7.5.7	Viewing Alarm Statistics.....	208
7.5.8	Querying Reported Events	210
7.5.9	Viewing the Reported Alarms	212
7.6	Handling Alarms	213
7.6.1	Confirming Alarms	214
7.6.2	Clearing Alarms Manually	215
7.6.3	Locating Alarms.....	215
7.6.4	Filtering Alarms.....	215
7.6.5	Modifying Alarm Levels	216

	7.6.6	Editing Alarm Remarks	217
	7.6.7	Exporting Alarms	217
	7.6.8	Editing Alarm Maintenance Experience	218
	7.6.9	Managing Maintenance Experience	219
	7.6.10	Exporting All Alarm Data to the FTP Service	220
7.7		Customizing the Alarm Information	221
	7.7.1	Customizing Alarm Names	221
	7.7.2	Customizing Alarm Levels	222
	7.7.3	Setting the Project Alarm Filter	224
7.8		Remote Alarm / Event Notification	226
	7.8.1	Setting Remote Communication Parameters	226
	7.8.2	Setting the Remote Notification Format of the Alarm / Event	227
	7.8.3	Setting the Remote Notification Sending Rules of the Alarm / Event	227
	7.8.4	Setting the Remote Notification Rules of the Alarm / Event	228
	7.8.5	Sending the Remote Alarm / Event Notification	229
7.9		Managing Alarm / Event Data	230
	7.9.1	Settings the Alarm / Event Overflow Save	231
	7.9.2	Settings the Manual Save of the Alarms / Events	233
7.10		Alarm Logs	235
7.11		Managing Alarm Frequency Analysis Rules	238
8		Performance Management	242
	8.1	Basic Concepts	243
	8.2	Managing Performance Query Templates	244
	8.2.1	Viewing Performance Templates	244
	8.2.2	Creating a Performance Query Profile	244
	8.2.3	Modifying a Performance Query Template	246
	8.3	Setting the Performance Collection Time	246
	8.4	Configuring the Performance Classification Switch in a Batch Manner	247
	8.5	Managing the Card Performance	249
	8.5.1	Viewing the Current Performance	249

	8.5.2	Viewing Performance History	250
	8.5.3	Viewing Comparison of Performance Data	252
	8.5.4	Viewing the Real-time Performance	253
	8.5.5	View Performance History Trend	255
8.6		Managing the Performance Collection	257
	8.6.1	Managing Performance Index Sets	257
	8.6.2	Managing Performance Threshold Sets.....	259
	8.6.3	Managing Performance Collection Task.....	262
8.7		Managing Performance Data	264
	8.7.1	Setting the Overflow Save of Performance	265
	8.7.2	Setting the Manual Save of Performance.....	266
	8.7.3	Gathering Statistics of PON Traffic	268
	8.7.4	Setting the FTP Reporting Switch.....	269
	8.7.5	Top Rank Statistics	271
9		Log Management.....	273
	9.1	Log Management Policy.....	274
	9.2	Log Types.....	275
	9.2.1	System Logs.....	275
	9.2.2	Operation Logs	276
	9.2.3	Security Logs.....	277
	9.2.4	TL1 Command Logs	278
	9.3	Log Statistics	279
	9.4	Managing System Logs	280
	9.4.1	Managing System Log Templates.....	280
	9.4.2	Querying System Logs.....	282
	9.5	Managing Operation Logs	283
	9.5.1	Managing Operation Log Templates	283
	9.5.2	Querying Operation Logs	285
	9.6	Managing Security Logs.....	288
	9.6.1	Managing Security Log Templates.....	288
	9.6.2	Querying Security Logs.....	290
	9.7	Managing TL1 Command Logs	291
	9.7.1	Managing TL1 Command Log Templates	292

	9.7.2	Querying TL1 Command Logs	293
9.8		Managing Log Data.....	294
	9.8.1	Managing the Log Forwarding Server.....	295
	9.8.2	Setting the Overflow Save of Logs.....	297
	9.8.3	Setting the Manual Save of logs	299
10		Resource Management.....	300
	10.1	Managing Resource Statistical Templates	302
		10.1.1 Viewing Resource Statistical Templates	302
		10.1.2 Customizing a Resource Statistical Template	304
	10.2	Physical Resource Statistics	306
	10.3	Resource Statistics of Other Types.....	307
	10.4	Exporting Physical Resource Statistics.....	308
	10.5	Exporting Resource Statistics of Other Types	310
	10.6	Example of Resource Statistics.....	311
	10.7	Importing the ODN NSM Information	313
	10.8	Querying Multiple ONUs	314
	10.9	Querying Cards by SN	317
	10.10	Querying the MDU Phone Number.....	318
	10.11	Querying the ONU RMS Error Information.....	320
	10.12	Querying the ONU Network Access Interception Logs	321
	10.13	Gateway Type Configuration	322
	10.14	Unauthorized ONU List	323
	10.15	Modifying ONU Names by Importing an Excel File.....	324
11		Data Synchronization and Backup.....	326
	11.1	Managing Data Synchronization Tasks.....	327
		11.1.1 Managing Software / Hardware Version Update Tasks.....	327
		11.1.2 Managing Configuration Uploading Tasks.....	327
	11.2	Data Backup.....	331
		11.2.1 Managing Software Backup Tasks.....	331
		11.2.2 Managing Configuration Export Tasks	333
		11.2.3 Managing Card Software Backup Tasks	336

11.2.4	Managing MAC Address Table Export Tasks of PON	
	Ports.....	339
12	Application Scenario	343
12.1	Alarm Management	344
12.2	Performance Management.....	347
12.3	Authorization and Domain Division.....	349
12.4	Guaranteeing Device Configuration.....	351
13	Abbreviations.....	353

Figures

Figure 1-1	Deployment of the UNM2000 in the TMN.....	2
Figure 2-1	UNM2000 Main GUI.....	7
Figure 5-1	Network Topology Creation Flow.....	99
Figure 6-1	The NE Manager GUI	128
Figure 6-2	Local Service Configuration GUI	129
Figure 10-1	Setting the MDU Phone Number Query Conditions.....	319
Figure 10-2	The Query MDU Phone Number Tab	319
Figure 10-3	Unauthorized ONU List	324

Tables

Table 1-1	Manageable Devices of the UNM2000	3
Table 2-1	Default Shortcut Icons in the Toolbar	8
Table 2-2	Other Common Shortcut Icons	9
Table 2-3	Descriptions of the General Keyboard Shortcuts.....	10
Table 2-4	Description of the Submenus under the System Menu	11
Table 2-5	Description of the Submenus under the View Menu.....	13
Table 2-6	Description of the Submenus under the Resource Menu.....	14
Table 2-7	Description of the Submenus under the Configure Menu	16
Table 2-8	Description of the Submenus under the Alarm Menu.....	17
Table 2-9	Description of the Submenus under the Performance Menu	18
Table 2-10	Sub Menus under the Security Main Menu	19
Table 2-11	Description of the Submenus under the Window Menu	19
Table 2-12	Description of the Submenus under the Help Menu	20
Table 3-1	The User Group Settings.....	51
Table 3-2	Description on User Settings	55
Table 3-3	Creating User Groups	64
Table 3-4	Creating Users.....	65
Table 4-1	Configuration Uploading / Downloading.....	89
Table 5-1	Description of the Network Topology Creation Flow	99
Table 5-2	Setting Items of Creating the Access NE	101
Table 5-3	Synchronization Mode	109
Table 5-4	Description of Parameters in the Create the Virtual Connection Dialog Box.....	110
Table 5-5	Descriptions of Settings in the Batch Modify Dialog box	117
Table 6-1	Description of the ONU Authentication Modes	136
Table 6-2	Description of PON Port Authentication Modes.....	138
Table 6-3	ONU Authorization Status	140
Table 6-4	Parameters.....	144

Table 6-5	Buttons.....	144
Table 6-6	Buttons.....	147
Table 6-7	Description on the VoIP Pinging Parameters	161
Table 7-1	Description and Handling Method of Alarms of Different Levels.....	168
Table 7-2	Access Method of Viewing Current Alarms	197
Table 7-3	Access Method of Viewing the Alarm History	200
Table 7-4	Parameter Descriptions of Project Alarm Filtering	225
Table 7-5	Descriptions of the Alarm / Event Overflow Save Task Settings.....	232
Table 7-6	Descriptions of the Alarm / Event Overflow Save Task Settings.....	234
Table 8-1	Access Method of Viewing the Performance History	251
Table 8-2	Threshold Set Parameters	261
Table 8-3	Description of the Performance Overflow Save Task Settings	266
Table 8-4	Descriptions of the Performance Manual Save Task Settings	267
Table 9-1	Description of the Parameters in the Query System Logs Dialog Box.....	281
Table 9-2	Description of the Parameters in the Query Operation Logs Dialog Box.....	284
Table 9-3	Description of the Parameters in the Query Security Logs Dialog Box.....	288
Table 9-4	Description of the Parameters in the Query TL1 Command Logs Dialog Box.....	292
Table 9-5	Description on the Settings of the Log Forwarding Server	296
Table 9-6	Descriptions of the Overflow Save Task.....	298
Table 12-1	Alarm Operation Descriptions.....	345
Table 12-2	Performance Operation Descriptions.....	348
Table 12-3	Creating User Groups	350
Table 12-4	Creating Users.....	351

1 Overview

The following introduces the product position and GUI description 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 the hierarchical network architecture and standard network interface. It is composed of business management layer (BML), service management layer (SML), network management layer (NML) and element management layer (EML). These layers comprise the layered management architecture of the TMN.

The UNM2000 manages the access devices and locates at the EML, as shown in Figure 1-1.

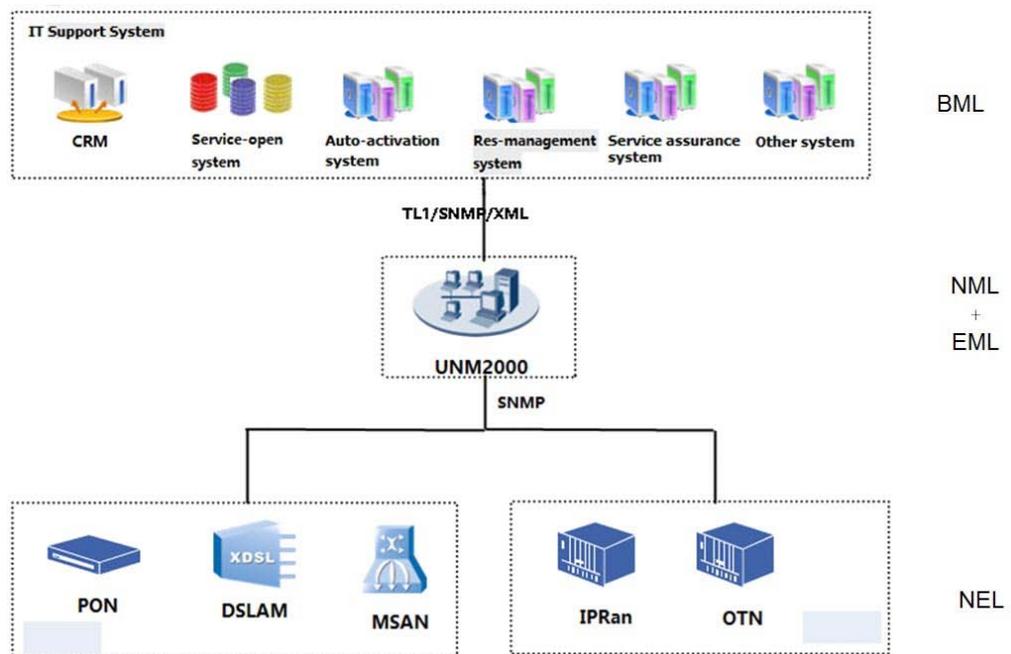


Figure 1-1 Deployment of the UNM2000 in the TMN

1.2 Manageable Device Types

The devices that can be managed by the UNM2000 are shown in Table 1-1.

Table 1-1 Manageable Devices of the UNM2000

Type	Device Model
OLT	AN5116-06B, AN5116-02, AN5116-06B, AN5516-04, AN5516-04B and AN5516-06.
ONU	AN5506-04-FG, AN5006-04-A, AN5006-04-B, AN5006-04-F, AN5506-01-A, AN5506-01-B, AN5006-01-A, AN5006-01-B, etc.
MSAN	AN5006-20, AN5006-30, AN5006-15 and AN5006-16.

2 Basic Operations of the UNM2000

The following introduces basic operations of the UNM2000, including the topics below.

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

2.1 Login / Logout

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

2.1.1 Logging into the UNM2000 Client End

You need to log into the UNM2000 system via the UNM2000 client before configuring and managing devices on the GUI of the UNM2000 client.

Prerequisite

- ◆ You have logged into the UNM2000 as the administrator.
- ◆ The UNM2000 services at the server end have been started.
- ◆ The client end communicates with the server end normally (check whether the network communication is normal by pinging the IP address of the far end).
- ◆ The client IP address is in the access control list of the UNM2000. See [Setting the ACL](#) for how to set the access control list.
- ◆ The user has been assigned a legal username and password.
- ◆ The client end of the UNM2000 is installed.

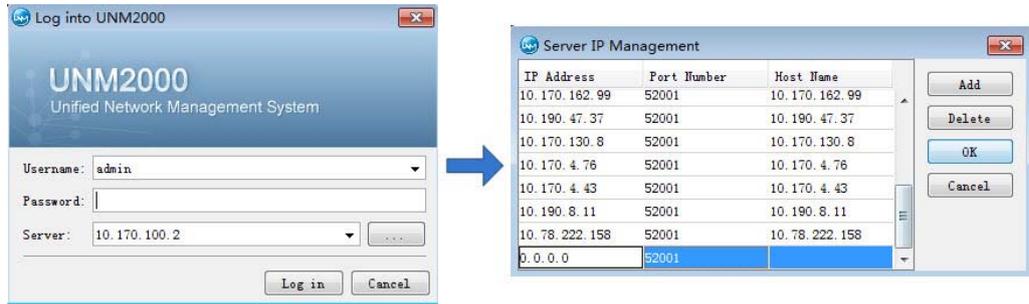
Procedure



1. Double-click the UNM2000 icon on the desktop.
2. In the **Server** drop-down list of the **UNM2000 Login** window, select the IP address of the UNM2000 server.

If the server to be logged in is not set, follow the steps below to add the server IP address.

- 1) Click  to open the **Server IP Management** dialog box, and click **Add**.
- 2) In the highlighted field, enter the **IP Address**, **Port Number** and **Host Name** of the desired UNM2000 server, and then click **OK**.



3. In the displayed **UNM2000 Login** dialog box, enter the username and password, and then click **Login**.



Note:

Upon completion of the UNM2000 installation, a default account will be given: the username is admin and the password is admin. To guarantee the UNM2000 security, please change the password immediately after login.

2.1.2 Exiting the UNM2000 Client End

Prerequisite

The UNM2000 client end runs normally.

Procedure

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

2.2 Viewing the UNM2000 Version

View the UNM2000 version information via the UNM2000 client.

Procedure

1. Log into the UNM2000 client.

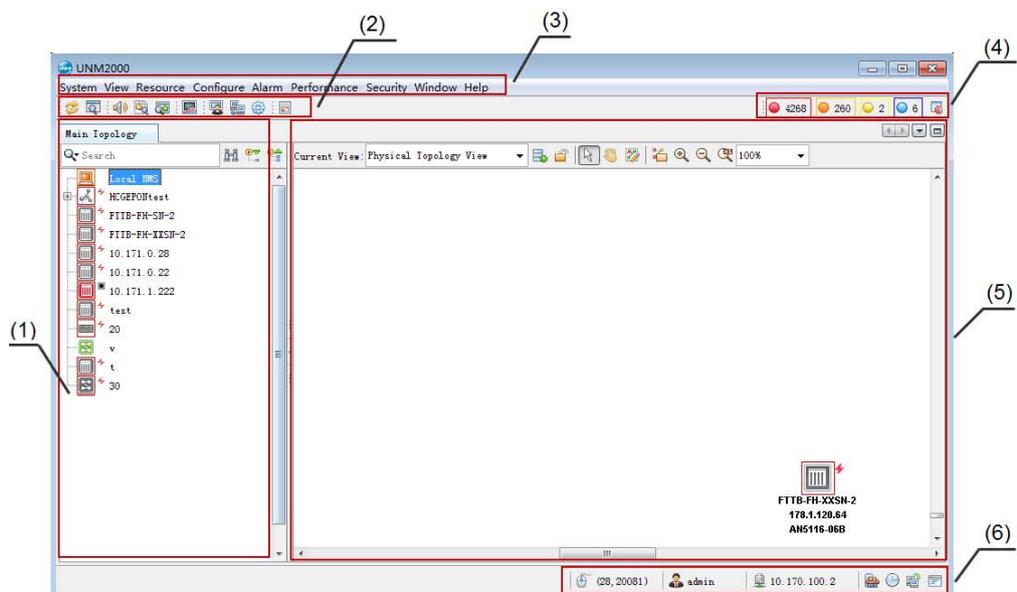
2. Select **Help**→**About UNM2000** in the main menu.
3. View the UNM2000 version in the displayed window.

2.3 GUI Introduction

The following enables you to understand the GUI of the UNM2000 and find the operation menu quickly to improve your operation efficiency.

2.3.1 GUI

The UNM2000 main GUI is composed of the object tree pane, toolbar, menu bar, etc., 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 Main GUI

2.3.2 Shortcut Icons

The following introduces the general shortcut icons in the UNM2000 GUI.

Shortcut Icons in the Toolbar

See Table 2-1 for the default shortcut icons in the toolbar.

Table 2-1 Default Shortcut Icons in the Toolbar

Classification	Icon	Name	Description
Common functional area		Refresh	Refreshes the current view.
		Searches for objects.	Searches and isolates the object.
Alarm		Alarm Prompt Tone Is On	Click the icon to switch on / off the alarm sound.
		The alarm sound prompt is turned off.	
		Current Alarm	Displays the current alarm information.
		Query Reported Events	Displays the report event information.
Performance		Performance History	Displays the historical performance information.
Others		NMS User Management	Opens the NMS User Management tab for user management.
		NE Communication Route Management	Opens the NE Communication Route Management tab for NE communication route management.
		Parameter Settings	Opens the Parameter Settings dialog box for system parameter settings.
Help		Legend	Opens the Legend pane that displays the system icons.
Alarm Statistics		Critical	Displays the quantity of critical alarms dynamically; Click this button to view the critical alarms in the Current Alarm tab.
		Major	Displays the quantity of major alarms dynamically; Click this button to view the major alarms in the Current Alarm tab.
		Minor	Displays the quantity of minor alarms dynamically; Click this button to view the minor alarms in the Current Alarm tab.

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

Classification	Icon	Name	Description
		Warning	Displays the quantity of prompt alarms dynamically; Click this button to view the prompt alarms in the Current Alarm tab.
		Display Alarm Statistics Window	Clicking this button to open the Alarm Statistics dialog box which displays all current alarm statistics.

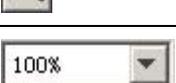
Other Common Shortcut Icons

See Table 2-2 for other common shortcut icons.

Table 2-2 Other Common Shortcut Icons

Icon	Name	Description
	Table Settings	Sets the table rows in the current GUI.
	Query by template	Queries by template or queries all.
	New	Creates a new object.
	Expand	Expands the object tree.
	Collapse	Collapses the object tree.
	Search	Open the search dialog box and enter the key word to search in the object tree.
	Quick search in the current object	Enter the key word to search in the current object+by clicking to select a search condition.
	Create a custom topology view	Creates a custom topology view and sets the view to display the concerned objects only.
	Lock / Unlock the View	Locks / unlocks the location of the NE icon in the topology view.
		
	Select	Moves NE icon freely in the topology view when the current view is unlocked.
	Move	Moves the topology view.

Table 2-2 Other Common Shortcut Icons (Continued)

Icon	Name	Description
	Edit	Edits the connection line by adding / deleting the control points.
	Aerial 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 in the original display scale.
	–	Sets the display scale of the topology view.
	Delete the custom topology view	Deletes the custom topology view.
	Modify Custom View	Modifies the basic information, node members and connection line members in the custom topology view.

2.3.3 General Shortcut Keys

See Table 2-3 for the general UNM2000 keyboard shortcuts.

Table 2-3 Descriptions of the General Keyboard Shortcuts

Shortcut	Description
F1	Opens the Help.
F5	Refreshes the current view.
Alt+Shift+Enter	Selects / Cancels the full-screen mode.
Ctrl+F	Opens the Search Object dialog box to search for NEs, logical domains or cards.
Ctrl+M	Displays the current alarms.
Ctrl+H	Views the alarm history.
Ctrl+P	Displays 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.

Table 2-3 Descriptions of the General Keyboard Shortcuts (Continued)

Shortcut	Description
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

2.4.1 System

The submenus under the **System** main menu are described in Table 2-4.

Table 2-4 Description of the Submenus under the **System** Menu

Menu	Description
Save Data	Overflow Saving When the overflow save task of historical data is set, the UNM2000 will automatically save the NMS log history data, device alarm data and performance data according to the conditions set in the task.
	Save Manually Manually saves the EMS log data, device alarm data and performance data.
Policy Task Management	Configura- tion 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 Synchroni- zation 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 MGC query.

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

Menu		Description
	Test Task	The test task includes the POTS port external / internal line task and the VoIP pinging test task.
	Statistics Export Task	Sets the statistics export task to export the performance data to an FTP server.
	Preconfig Task	Imports the Telnet command text file to perform the Batch-Download operation on the device via issuing the Telnet command and display the operation result.
Parameter Settings	Local Settings	Sets the system parameters, including the browse tree display style, the time mode, the topology display, the pinging parameters, the Telnet proxy server, and the GUI display.
	User Security Strategy	Sets the user login mode, access control list, password policy and account policy of the UNM2000.
	Alarm Settings	Sets the alarm-related parameters, including the UNM2000 client end settings (alarm sound, and processing and display mode of newly reported alarms) and the UNM2000 server settings (alarm automatic confirmation rules, automatic synchronization mode, etc.).
	Service Configuration	Sets the global FTP server.
	Performance Settings	Sets the 24-hour performance collection time of the server.
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.
Exit		Exits and closes the UNM2000 client.

2.4.2 View

The submenus under the **View** main menu are described in Table 2-5.

Table 2-5 Description of the Submenus under the **View** Menu

Menu		Description
Refresh		Refreshes the current view.
Topology View	Show NE IP and Type	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.
	Alarm Statistics	Sets whether to display  on the toolbar of the main GUI so as to view the UNM2000 and NE alarms.
	Common Function Area	Sets whether to display  on the toolbar of the main GUI.
	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.
	Help	Sets whether to display  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 system default shortcut keys on the toolbar of the main topology.
	Customize	Adds the commonly used tools onto the toolbar by customizing the toolbar.

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

Menu		Description
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.

2.4.3 Resource

The submenus under the **Resource** main menu are described in Table 2-6.

Table 2-6 Description of the Submenus under the **Resource** Menu

Menu		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.
Auto Patrol		Creates the automatic patrol conditions and executes patrol on the UNM2000, OLT, MDU and ONU according to the set patrol conditions.
Create Logical Domain		Creates a logical domain for managing NEs. The logical domain is a set of NEs.
Create NE	Create Access NE	Creates an access NE.
	Create Other NE	Creates a virtual NE.
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 the ONU names in a batch manner by exporting an Excel file.

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

Menu		Description
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		Deletes all the data of the selected network or subnet.
Searches for objects.		Searches for the object by the specified search conditions, for example, NE, logical domain or card.
Query the ONU		Searches for the ONU by the specified search conditions.
Batch Query ONU		Queries the ONUs in a batch manner by importing the specified conditions.
Query MDU Phone Number		Queries the port details by the port phone number.
Query Board by Serial Number		Queries card details by card SN.
ONU RMS Error Information Query		Queries the information of the ONU that fails to register according to specified search conditions.
ONU Network Intercept Log Query		Queries the information of the ONU that is re-authorized according to specified search conditions.
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 NE GIS information in a batch manner.
Gateway Type Config		Sets the gateway type.
Resource Statistics	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 ONU MGC services according to the preset statistical template.
	Physical Resource Statistics Export	Exports the physical resource statistics as an CSV, HTML, TXT or Excel file.
	Statistics Export of Other Types	Exports the user information statistics or service information resource statistics as an CSV, HTML, TXT or Excel file.
HGU Resource Interconnect		Manages the ONU manufacturer and device model information.
Unauthorized ONU List		Queries the unauthorized ONU list of a specified object.

2.4.4 Configuration

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

Table 2-7 Description of the Submenus under the **Configure** Menu

Menu		Description
Global Template Config	Global Profile	Configures multiple same-model NEs in the administrative domain of the entire network by using a global profile, for example, the line profile, QoS profile, port profile, service profile and bandwidth profile.
	Global Config	Completes the non-profile configurations for multiple same-model NEs in the administrative domain of the entire network, for example, the ONU card configuration, service configuration, alarm management and time management.
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 and the line card resource management system.
Signaling Tracing		Traces the signaling frame of the communication between the current IAD and the voice communication card to find the communication failure timely.
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 equipment.
Pre-deploying ONUs		Completes the configuration and deployment of the ONU service in advance to implement the automatic provisioning of the ONU service.
Home Gateway MAC Range Config		Configures and modifies the MAC addresses of home gateways in a batch manner.
PON Config Transfer		Completes the PON configuration migration.

2.4.5 Alarm

The submenus under the **Alarm** main menu are described in Table 2-8.

Table 2-8 Description of the Submenus under the **Alarm** Menu

Menu	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.
View the Reported Alarms	Sets the alarm reporting conditions to view the reported alarms of the entire network or a specified object.
Alarm Reporting Settings	Sets the alarm reporting rules according to the requirements for network maintenance.
Event to Alarm Settings	
Alarm Query Template	Quickly completes the settings of alarm browsing and alarm attributes to simplify the user setting operations.
Query Reported Event	Sets the event reporting conditions to view the reported events of the entire network or a specified object.
Event Query Template	Sets the event reporting rules according to the requirements for network maintenance.
Shield Project Alarms	Sets the alarm filter to automatically filter all the alarms and alarm clearance information reported during the project construction.
Shield Rule Of North	Sets filter rules to filter the unnecessary northbound interface alarms according to the network maintenance requirements.
Alarm Shield Rule Management	Sets filter rules to filter the alarms not focused according to the network maintenance requirements.
Alarm Flashing Shield Rule Management	Sets filter time rules for the alarms not focused according to the network maintenance requirements.
Alarm Notification Settings	Sets the information of the alarm receiver to make sure important alarms are notified to the device maintainer in a timely manner.
Alarm Maintenance Experience Management	Enters the experience information of alarm maintenance.
Customizing Alarm Names	Customizes the alarm names.
Custom Alarm Level	Customizes the alarm levels.

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

Menu		Description
Alarm Log	Query Alarm Log	Queries alarms according to the query conditions.
	Current Alarm Log Statistics	Gathers statistics of alarms according to the statistical conditions.
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.

2.4.6 Performance

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

Table 2-9 Description of the Submenus under the **Performance** Menu

Menu	Description
Performance History	Sets the query conditions to view the performance history of the entire network or a specified object.
Collection Task Management	Sets the indicator, threshold, task and time for the performance connection.
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.
Performance Query Template	Save the common performance query conditions as a template.
Performance Switch Config	Queries or configures the performance classification switch for NEs in a batch manner.
Pm FTP Switch Management	Configures the performance FTP reporting function.
Analysis of PON traffic statistics	Queries the traffic analysis data of the PON interface.
Top rank statistics	Queries the ranking data of PON traffic and device health.

2.4.7 Security

The submenus under the **Security** main menu are described in Table 2-10.

Table 2-10 Sub Menus under the **Security** Main Menu

Menu	Description
NMS User Management	Manages the users, user groups, operation sets of the UNM2000, including the security attribute settings and authority allocation.
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.
View the TL1 Command Logs	Sets the filter conditions to query the TL1 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 TL1 Command Logs	Sets the filter conditions to gather statistics of TL1 command logs.
Log Forwarding Server	Forwards the UNM2000 logs onto another server.

2.4.8 Window

The submenus under the **Window** main menu are described in Table 2-11.

Table 2-11 Description of the Submenus under the **Window** Menu

Menu	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.
Window	Opens the description for each windows.

2.4.9 Help

The submenus under the **Help** main menu are described in Table 2-12.

Table 2-12 Description of the Submenus under the **Help** Menu

Menu	Description
Legend	Opens the Legend pane to view the system legend.
License Management	Views the UNM2000 license information list, including server ID, upgrading license, etc.
About UNM2000	Views the UNM2000 version information, registration information and installed components.

2.5 Setting System Parameters

The UNM2000 system parameters include the browse tree display style, the time mode, the topology display, the pinging parameters, the Telnet proxy server, and the GUI display. The following introduces how to set and use the parameters.

2.5.1 Setting the Display Style 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

These settings take effect immediately. They are applicable to the current user at any client ends, but they are not applicable to other users.

Procedure

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



3. Set various parameters as required. During setting, users can preview the display style via the instance text.
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 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

- ◆ When you log in next time, the UNM2000 client will adopt the settings you set last time.
- ◆ The settings of the time mode are applicable to the current user at any client. However, they are not applicable to other users.



Note:

It is recommended to keep client time synchronous with the server end time to avoid data reporting error.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**Time Mode** in the left pane to open the 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.

Background Information

- ◆ The settings of the topology display mode take effect immediately.
- ◆ These settings are applicable to the current user at any client ends, but they are not applicable to other users.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**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.
- ◆ The Ping parameters of the client take effect immediately.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Local Settings**→**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.
 - ▶ When the **Consecutive Ping** option is selected, right-click the object and select **Ping** to ping the object continuously.
 - ▶ If **Forward Ping Packet via the Server** is selected, the Ping commands will be forwarded by the server.

2.5.5 Setting the Telnet Proxy Server

After setting the parameters related to the Telnet proxy server, users can use the proxy server to access the equipment.

Background Information

The settings of the Telnet proxy server take effect immediately.

Prerequisite

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

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. In the left pane, select **Local Settings**→**Telnet Proxy Server** to open the dialog box.
3. Select the **Enable Telnet Proxy Server** check box, set the proxy server information and then click **Apply** to validate the settings.

2.5.6 Setting the GUI Display Mode

Users can set the GUI display mode, including the maximum row number of a table, the display mode of name of alarms / performance / events, and whether the GUI is locked automatically.

Background Information

- ◆ The display settings take effect immediately.
- ◆ The alarm color settings are applicable for all users at any client.

Procedure

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

- Set the parameters and click **Apply** to apply the settings.

2.6 Setting the FTP Server

Set the FTP server and related parameters to implement the data transmission between the UNM2000 client end and the server end.

Background Information

The FTP 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 FTP server are shown in the following table.

Module Name	Implementation	Related Function
Policy task	Implements the task customization via the FTP 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 FTP 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 and PON port MAC address table.
Save Data	Releases the database space and saves the data onto the FTP 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 authorities of **Operator Group** or higher authorities.

Procedure

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

FTP Server Setting					
Set Global FTP Server					
Host Name	Host IP	Username	Password	Port Number	Path
10.170.100.2	IPv4:10.170.100.2	1	●	21	./
aasas	IPv4:0.0.0.0			21	./sljfls/
ww	IPv4:1.0.0.1	1	●	214	./

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

Other Operations

For the FTP server already set, you can delete it if it is no longer used or test it before use.

- ◆ Select the FTP server not needed and click **Delete** to delete it.
- ◆ Select the desired FTP server and click **Test FTP** to test whether the FTP 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.

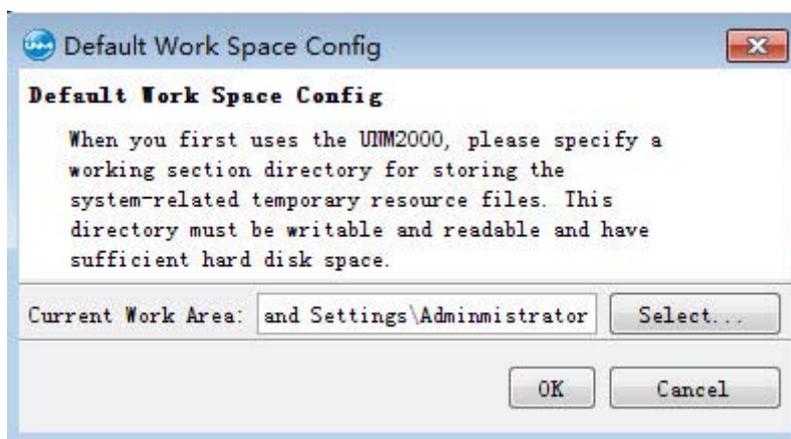


Note:

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

Procedure

1. Select **System**→**Default Work Section Settings** in the main menu to open the **Default work space set** dialog box.



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

2.8 Basic Operations of the UNM2000

2.8.1 Upgrading the License

The UNM2000 license file is used for controlling the functions and management capability of the UNM2000. You cannot log into the UNM2000 client without the license file. The following introduces how to renew the UNM2000 license.

Prerequisite

- ◆ You have logged into the UNM2000 as the admin user.
- ◆ The user has obtained the UNM2000 license.

Procedures

1. Back up the original License.

Create a folder named **backup** under **D:\unm2000\platform\etc\license** and copy the original license file **unm2000_license.lic** to this folder.

2. Renew the License.
 - 1) Select **Help**→**License management** in the main menu.
 - 2) In the **License information** dialog box that appears, click **Update license**.
 - 3) In the **Open** dialog box, select the corresponding license and click **Open**.
 - 4) In the **License comparison** dialog box, check the control items of both the old and the new licenses and click **Confirm License update**.
 - 5) Click **Yes** in the displayed alert box.
 - 6) Click **Close** in the **License Information** dialog box.
3. After updating the license file, restart the UNM2000 client. The client will reload the control items according to the updated license.

2.8.2 Modifying the Password

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

Procedure

1. Select **System**→**Modify Password** in the main menu.
2. In the displayed **Modify Password** dialog box, set **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 Lock 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** in the main menu to open the **The window is locked** dialog box.

- ▶ Locking the terminal automatically.

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

2.8.4 Logging Out of the Current Account

Different UNM2000 users have different operation authorities. The user can perform operations of different levels by logging out of the current account and logging in again with another account.

Procedure

1. Select **System**→**Log off** from the main menu.
2. Click **Yes** in the alert box that appears to lock out of the current account.
3. In the **UNM2000 Login** dialog box that appears, select the server you want to log in and enter the username and password. Click **Enter**.



2.8.5 Viewing the Message Platform

You can view the prompts and operation echo information that influence the running of the UNM2000 on the message platform.

Procedure

1. Select **View**→**Message Platform** from the main menu to open the **Message Platform** pane.



2.8.6 Managing Toolbars

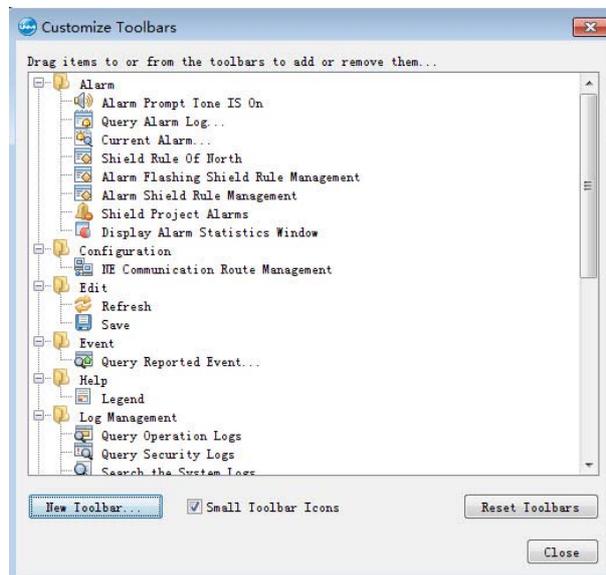
You can set which toolbars and their corresponding shortcut menus are displayed for quick operations to improve the operation efficiency.

Procedure

1. Select **View**→**Toolbars** in the main menu.
2. In the **Toolbars** menu, click the function modules to be displayed in the main topology.
3. The selected function module will be added with a tick (√) in front of it and it will appear in the toolbar of the main view.

Other Operations

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



2. Click **New Toolbar**, enter the name for the new toolbar in the displayed **New Toolbar** dialog box and then click **OK**.
3. The user can drag an item in or out of the toolbar to add or delete the corresponding shortcut icon as needed.
4. After completing the settings, click **Close**.

In the following figure, the **Topo** functional module is added to the toolbar. Drag the **Create Custom Views** shortcut icon to the **Topo** function module in the **Customize Toolbars** dialog box.



2.8.7 Creating a Custom View

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

- ◆ One user can create up to five custom views.
- ◆ A user can only see the custom views created by himself / herself.

Prerequisite

You have the authorities of Operator Group or higher authorities.

Procedure

1. On the toolbar of the **Main topology** 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** to open the **Select Object** dialog box. Then select the NEs to be displayed in the custom view and click **OK**.
4. Select **Link Member**→**Select** to open the **Select Object** dialog box. Then select the NE fiber connections to be displayed in the custom view and click **OK**.
5. In the **Create Custom View** dialog box, click **OK**.
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 Network Management Users
- Managing User Sessions
- Authorization and Domain Division

3.1 User Security Concepts

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

Managed Entities

- ◆ Object set: Indicates a set of managed objects. Dividing the managed objects into object sets facilitates the allocation of authorities for managing NEs. The object set only includes the physical objects (exclusive of logical objects) with the smallest granularity being cards.
- ◆ Operation set: Indicates a set of operations. Dividing the operations into operation sets facilitates the management of user authorities. 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 authorities 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 do not 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 authorities. The UNM2000 supports creating user groups to manage the users of the same authorities in a same group. The users in a same group have the same authorities 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 admin group, inspector group, the operator group and the maintainer group.

- ▶ Administrators: The **Administrators** group is unique. It cannot be created nor deleted. The Administrators group has the administrative domains of all objects in the entire network and all the operation authorities except the security management authority. Its administrative domains and operation authorities cannot be modified.
- ▶ Security Admin Group: This group is unique. It cannot be created nor deleted. The Security Admin Group has the administrative domains of all objects in the entire network and the authorities related to security management authority.
- ▶ Inspector group: This group has the default authorities of **Inspector Operation Sets**. The users in this group can only query and gather statistics, having no authorities to perform the creation and configuration operations.
- ▶ Operator group: This group has the default authorities of **Operator Operation Set**. Apart from the basic authorities of the inspector group, the users in this group can perform the creation, modification and deletion operations in the UNM2000, but having no authorities related to security management.
- ▶ Maintainer group: This group has the default authorities of **Maintainer Operation Set**. Apart from the authorities 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 authorities. When a user is added into a user group, the user is assigned with the operation authorities associated with the user group.
 - ▶ A user can be added into multiple user groups. In this case, the authorities of a user are the union of its basic authorities and the authorities of the user groups that the user belongs to. There are two ways to assign authorities to users:
 - Divide the user to the user group and the user can thus have the authorities of the user group.
 - Give the user directly 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. The authorities of admin cannot be modified and the admin user cannot be added to other user group.

Authority 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 of the UNM2000 is implemented through the administrative domain and operation authorities. The operation authorities are divided into different functional domains through the authority division function and the NEs are divided into different network domains through the domain division function. Assigning the UNM2000 users with the authority combination of different functional domains and network domains effectively controls user management authorities.

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 authorities within this sub-domain and can create the object set, operation set, user group, users based on such domain authorities. 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 authorities 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 contents:

- ◆ Setting the user login mode
- ◆ Setting the ACL
- ◆ 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 ACL

By setting the ACL, the operator can set the UNM2000 users to log in only via the client end with the set IP address or network segment, so as to ensure the network security.

Background Information

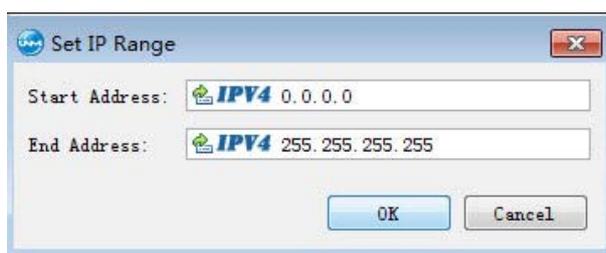
The access control list set by a user is only applicable to the user.

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. Select **User Security Strategy**→**Access Control List** in the left pane to open the **Access Control List** dialog box.
3. Click **Add** and open the **Set IP Range** dialog box.



4. Set the **Start address** and **End address**. After completing the settings, click **OK**. Then the added IP address range appears in the ACL.



Note:

Click  to switch between the IPv4 and IPv6.

5. Click **Apply** to apply the settings.

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 parameters in **Common Policy** and **Advanced Policy** tabs, and then click **Apply** to apply the settings.

Other Operations

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

3.3 Managing Network Management Users

The following introduces the operations of creating, modifying, and deleting network management users and assigning the authorities for them.

3.3.1 Operation Set Management

The operation set is the set of operations of a certain type. Via the operation set management, users can assign and manage the operations on the equipment.

- ◆ 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 authorities 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

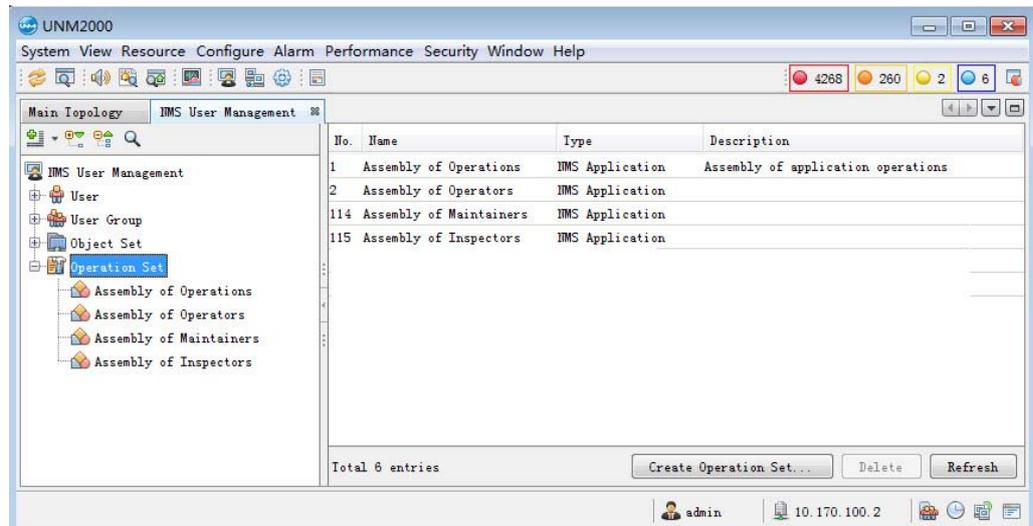
The security administrator can view specific operations included in an operation set to check whether the authorities in the operation set meet the requirements.

Prerequisite

You have logged into the UNM2000 as a user belonging to the **Security Admin Group**.

Procedure

1. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
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 **Refresh**, **Delete**, **copy cell (K)**, **Print**, or **Export**.
- ◆ Select the corresponding operation set in the left pane, and modify the information items in the right pane. After completing the modification, click **Apply**.



Note:

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

3.3.1.2 Adding an Operation Set

The operation set is the set of operations of a certain type. Via the operation set management, users can assign and manage the operations on the equipment. When the current operation set cannot meet the requirements, users can create a new operation set.

Prerequisite

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

Procedure

1. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
2. Select one of the following access methods to open the **Create Operation Set** dialog box.

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

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



Note:

Click **Copy Members from Operational 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

Double-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. Users 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 authorities 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

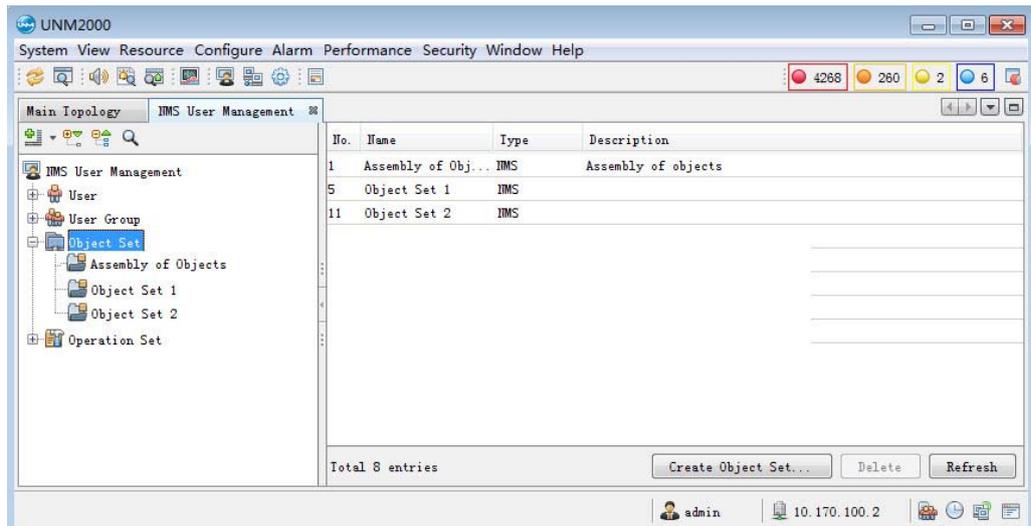
The security administrator can view the objects included in the object set to check whether the objects in the object set meet the requirements.

Prerequisite

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

Procedure

1. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
2. Click **Object Set** 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 **Refresh**, **Delete**, **copy cell (K)**, **Print**, or **Export**.
- ◆ Select the corresponding object set in the left pane, and modify the information items in the right pane. After completing the modification, click **Apply**.



Note:

Users 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, users can create a new object set.

Prerequisite

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

Procedure

1. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
2. Select one of the following access methods to open the **Create Object Set** dialog box.

No.	Access Method
1	Select NMS User Management in the left pane and click Create Object Set in the right pane.
2	Select 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 operation 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

Double-click an added object set to view the information related to the object set in the right pane.

3.3.3 User Group Management

The user group is the set of the network management users with the same management authorities. For the users to be granted with the same authorities, 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 authorities, quickly allocating the authorities 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 authorities assigned to the user group.
- ◆ Only the users in **Security Admin Group** and **Domain Security Admin Group** can manage user groups.



Caution:

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

3.3.3.1 Viewing User Groups

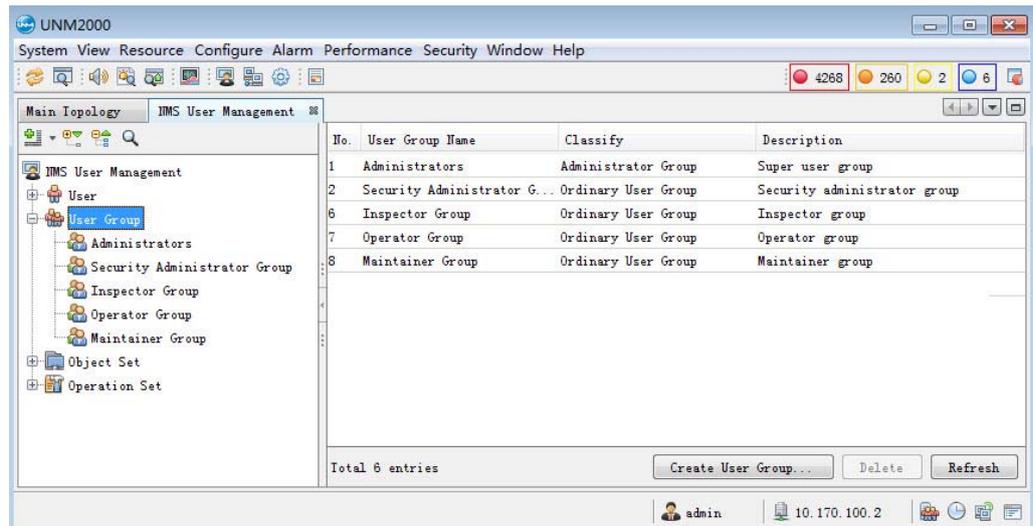
The security administrator can view the administrative domains of the user groups to check which objects are managed by the user group.

Prerequisite

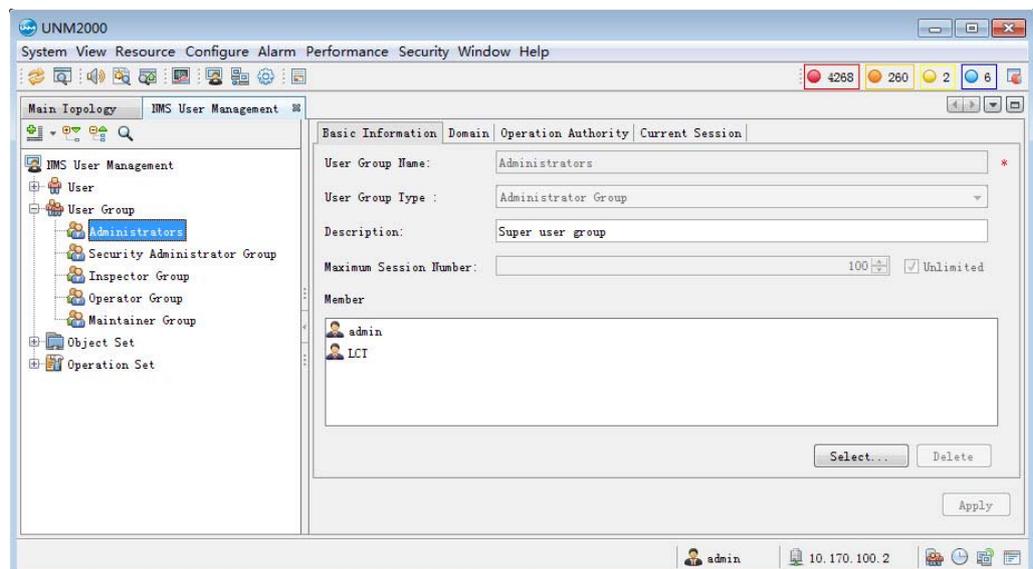
You have the authorities of **Security Admin Group**.

Procedure

1. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
2. Click **User Group** or **+** before **User Group** in the left pane and then view the existing user groups in the right pane or the expanded list of **User Group** in the left pane.



3. Double-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 **Refresh**, **Delete**, **copy cell (K)**, **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 authorities for users.

Prerequisite

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

Procedure

1. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
2. Select one of the following access methods to open the **New User** dialog box.

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

No.	Access Method
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. According to Table 3-1, 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"> ◆ Sub Domain Security Administrator Group: The administrative domain of this group is assigned by the security administrator. This group only has the application authorities of security management and its authorities cannot be modified. ◆ Ordinary User Group: The administrative domain and operation authorities of the users in this group are assigned by the security administrator or sub domain security administrator.
	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, No limit .
	Member	Sets the members of the user group via the Select... and Delete buttons.

Table 3-1 The User Group Settings (Continued)

Parameter	Description
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.
Operational 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.

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

Subsequent Operation

Double-click an added user group to view the information related to the user group in the right pane.

3.3.4 User Management

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

3.3.4.1 Viewing Users

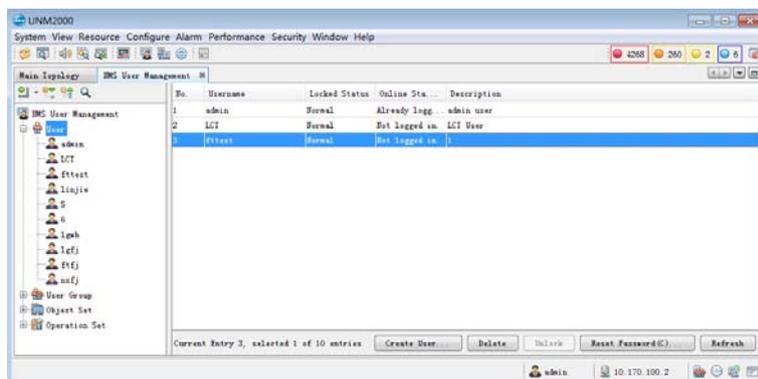
You can query the number and additional information of the UNM2000 users for convenient user management.

Prerequisite

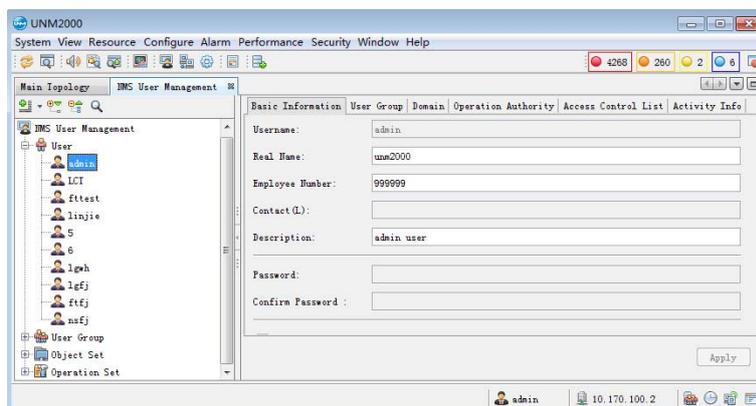
You have the authorities of **Security Admin Group** or higher authorities.

Procedure

1. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
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. Double-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 (C)**, **Clone**, **Refresh**, **Print...**, **Copy Cell (K)**, 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 authorities so as to allocate the accounts to users of different responsibilities.

Background Information

The UNM2000 provides a default superuser named **admin**. The authorities of admin cannot be modified and the admin user cannot be added to other user group.

Prerequisite

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

Procedure

1. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
2. Select one of the following access methods to open the **New User** dialog box.

No.	Access Method
1	Select NMS User Management in the left pane and click Create User in the right pane.
2	Select NMS User Management in the left pane, right-click in the right pane and select Create User from the shortcut menu.
3	Click User in the left pane and click Create User 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. According to Table 3-2, set the user parameters in the **Create user** dialog box.

Table 3-2 Description on 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	The brief description of the user account, used to identify different users.
	Password	Sets the user password, which must comply with the password policies. For the settings of the password policies, see Setting the Password Policy .
	Confirm the password	Type the user password again.
Basic Information	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.

Table 3-2 Description on User Settings (Continued)

Parameter		Description
	Password Valid Days	<p>Sets the number of the valid days of the password.</p> <ul style="list-style-type: none"> ◆ Select “Valid days of using system password: 180”, and the valid days number is 180. ◆ Select User Define (L) to set the number of days. Value range: 0 to 999 (days) (0 indicates that the password is always valid)
User Group		Sets the user group of the user.
Domain		<p>Sets the management domain of the user.</p> <p>The objects of the management domain are arranged in parallel in the tree topology of the equipment sets, the global logical domains, and the object groups. The valid management domain is the sum of the selected equipment sets, global logical domains, and object groups.</p>
Operation Authority		<p>Sets the operation authority of the user.</p> <p>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.</p>
Access Control List		<p>Sets the ACLs of the user.</p> <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 ACL. ◆ Select Use the following assigned ACL (B) to set the range of IP addresses logged in by the user account.



Note:

Click **Copy permission from users...**, set the user in the **Select user** dialog box, and directly copy the management domain and operation authority of the corresponding user. This can improve the setting efficiency.

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

Subsequent Operation

Double-click an added user 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 belonging to the Security Admin Group or the 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) In the main menu, select **Security**→**NMS User Management** to open the **NMS User Management** tab.
 - 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 Re-setting 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. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
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 User Sessions

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

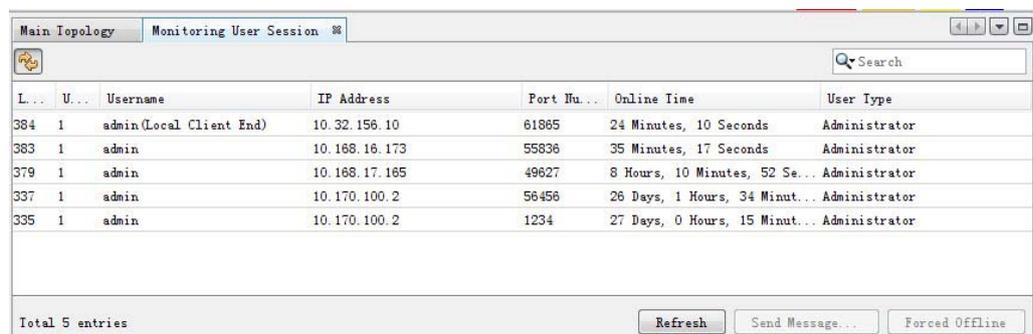
- ◆ Session: The connection set up between the client end and the server.
- ◆ When the user login mode is set to **Multi-User Mode**, one user account can log in multiple client ends at the same time. You can specify the maximum number of concurrent online users using a same account. For details, see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

Prerequisite

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

Procedure

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



The screenshot shows a software interface with a tab titled "Monitoring User Session". Below the tab is a search bar and a table with the following columns: L..., U..., Username, IP Address, Port Nu..., Online Time, and User Type. The table contains five rows of session data. At the bottom of the interface, there are buttons for "Refresh", "Send Message...", and "Forced Offline", along with a status indicator "Total 5 entries".

L...	U...	Username	IP Address	Port Nu...	Online Time	User Type
384	1	admin(Local Client End)	10.32.156.10	61865	24 Minutes, 10 Seconds	Administrator
383	1	admin	10.168.16.173	55836	35 Minutes, 17 Seconds	Administrator
379	1	admin	10.168.17.165	49627	8 Hours, 10 Minutes, 52 Se...	Administrator
337	1	admin	10.170.100.2	56456	26 Days, 1 Hours, 34 Minut...	Administrator
335	1	admin	10.170.100.2	1234	27 Days, 0 Hours, 15 Minut...	Administrator

Other Operations

Right-click in the tab and click **Refresh**, **Copy Cell**, **Print** or **Export** from the shortcut menu.

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**→**Monitoring User Session**.
2. In the **Monitor User Session** tab, view the information of the online user.

L...	U...	Username	IP Address	Port Nu...	Online Time	User Type
384	1	admin(Local Client End)	10.32.156.10	61865	24 Minutes, 10 Seconds	Administrator
383	1	admin	10.168.16.173	55836	35 Minutes, 17 Seconds	Administrator
379	1	admin	10.168.17.165	49627	8 Hours, 10 Minutes, 52 Se...	Administrator
337	1	admin	10.170.100.2	56456	26 Days, 1 Hours, 34 Minut...	Administrator
335	1	admin	10.170.100.2	1234	27 Days, 0 Hours, 15 Minut...	Administrator

Total 5 entries

Refresh Send Message... Forced Offline

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

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

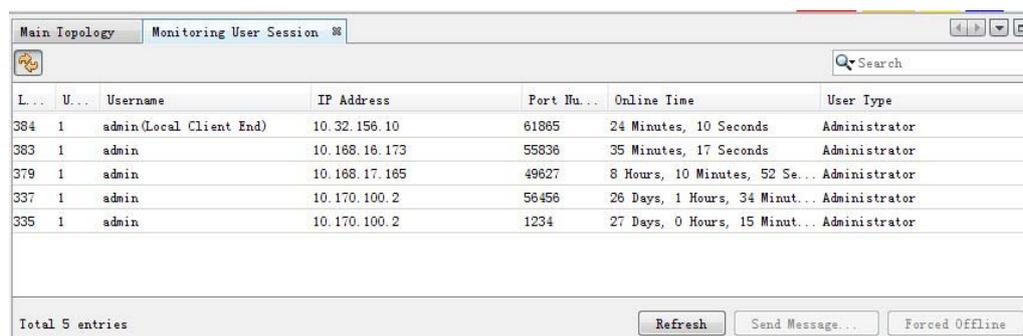
- ◆ Session: The connection set up between the client end and the server.
- ◆ When the user login mode is set to **Multi-User Mode**, one user account can log in multiple client ends at the same time. You can specify the maximum number of concurrent online users using a same account. For details, see [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 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**→**Monitoring User Session**.
2. In the **Monitor User Session** tab, view the information of the online user.



L...	U...	Username	IP Address	Port Nu...	Online Time	User Type
384	1	admin(Local Client End)	10.32.156.10	61865	24 Minutes, 10 Seconds	Administrator
383	1	admin	10.168.16.173	55836	35 Minutes, 17 Seconds	Administrator
379	1	admin	10.168.17.165	49627	8 Hours, 10 Minutes, 52 Se...	Administrator
337	1	admin	10.170.100.2	56456	26 Days, 1 Hours, 34 Minut...	Administrator
335	1	admin	10.170.100.2	1234	27 Days, 0 Hours, 15 Minut...	Administrator

Total 5 entries

Refresh Send Message... Forced Offline

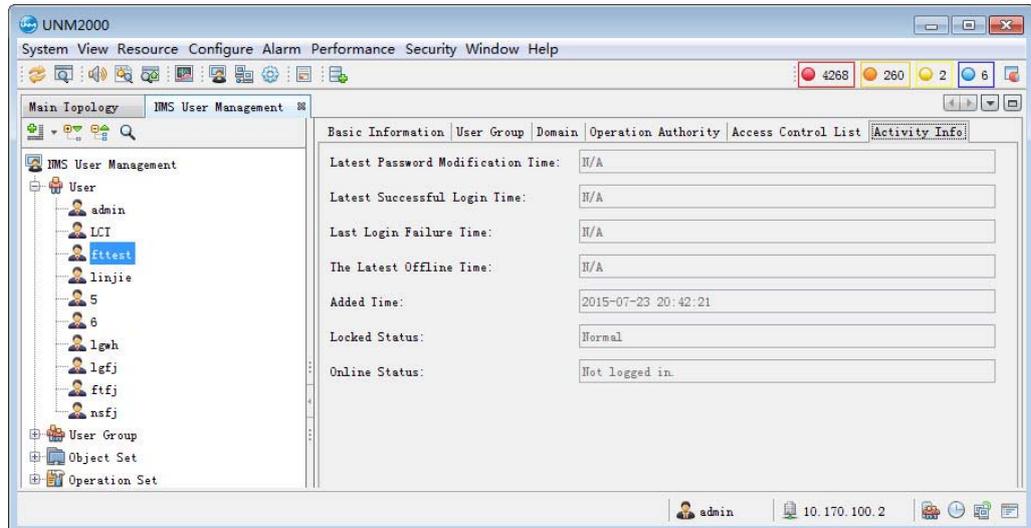
3. Right-click the corresponding user session, and select **Send Message** from the shortcut menu.
4. Type the message contents in the **Send message** dialog box, and then click **OK**.

3.4.4 Monitoring User Activities

Monitor the user action information, so as to prevent illegal operations of users.

Procedure

1. In the main menu, select **Security**→**NMS User Management** to access the **NMS User Management** tab.
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 authorities for users in two areas as example to introduce how to create user accounts and assign authorities.

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 authorities respectively.

Procedures

1. Create object sets.

According to area division, create object set A and object set B. Add the devices of Area A and Area B to the members of object set A and object set B.

Refer to [Creating an Object Set](#) to create the object sets.

2. Create operation sets.

Use 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 specific operations of creating the operation set, see [Adding an Operation Set](#).

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
Supervisor 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

Refer to [Creating User Groups](#) for specific steps of creating the 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.
- ▶ According to the working shifts of the staff, set the login time ranges.
- ▶ Set the users' user groups. If six user groups A, B, C, D, E, and F are to be created, refer to Table 3-4. After being assigned with a user group, the user will be authorized with the management domain and operational authorities 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 and limit the IP address range accessible to the user.

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
- Managing Global Templates
- Global Configuration Management
- Tracing Signaling
- Configuration Synchronization
- Network Access Management
- Home Gateway MAC Range Configuration
- Pre-deploying ONUs
- Pinging NEs
- Telneting NEs
- The Tracert Function of the UNM2000 Server
- PON Configuration Transfer

4.1 NE Communication Route Management

By using the NE communication routing function, you can create the NE management program, manage NEs based on partitions, and manage the pre-configured NEs. The following introduces the operations for managing NE communication routes.

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 Manager Services

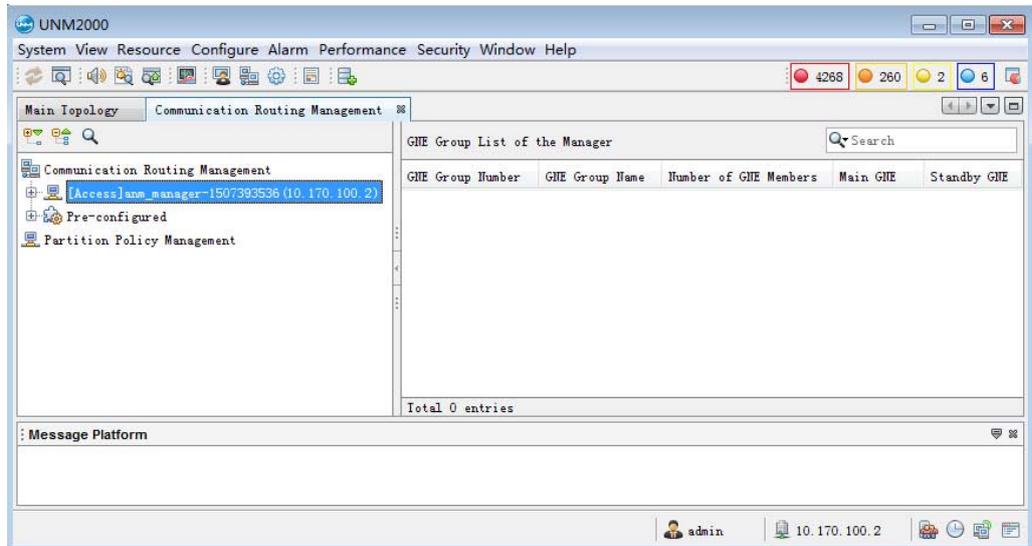
Correct configuration of the NE management program is the prerequisite to ensure normal communication between the UNM2000 and the NEs.

Prerequisite

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

Procedure

1. Select **Configure**→**NE Communication Route Management** to open the **Communication Routing 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.

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

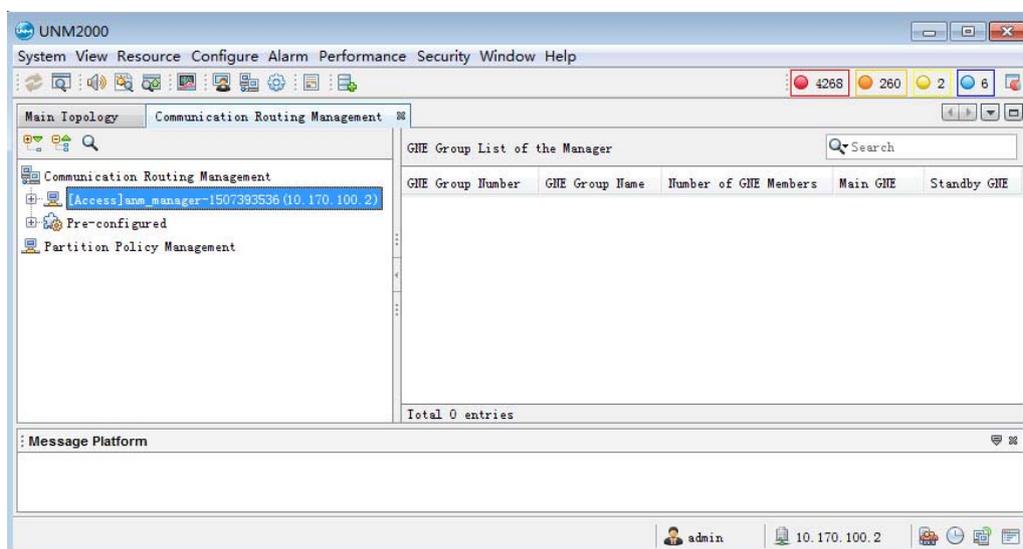
In case of network resource adjustment and that changes are made to the management program that the NE belongs to, you can delete the management program and then create one or directly modify the management program to meet your requirement.

Prerequisite

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

Procedure

1. Select **Configure**→**NE Communication Route Management** to open the **Communication Routing Management** tab.



2. Delete a management program: In the left pane of the **Communication Routing Management** dialog box, right-click the management program and select **Delete the Manager** from the shortcut menu and then click **OK** in the displayed dialog box.
3. Modify a management program: In the left pane of the **Communication Routing Management** dialog box, right-click the management program and select **Manager Property** from the shortcut menu to open the **Manager Properties** dialog box. Then modify the parameters as needed and click **OK**.

Other Operations

1. In the left pane of the **Communication Routing Management** dialog box, click **Pass-through** before the management program. The right pane displays the pass-through NEs 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

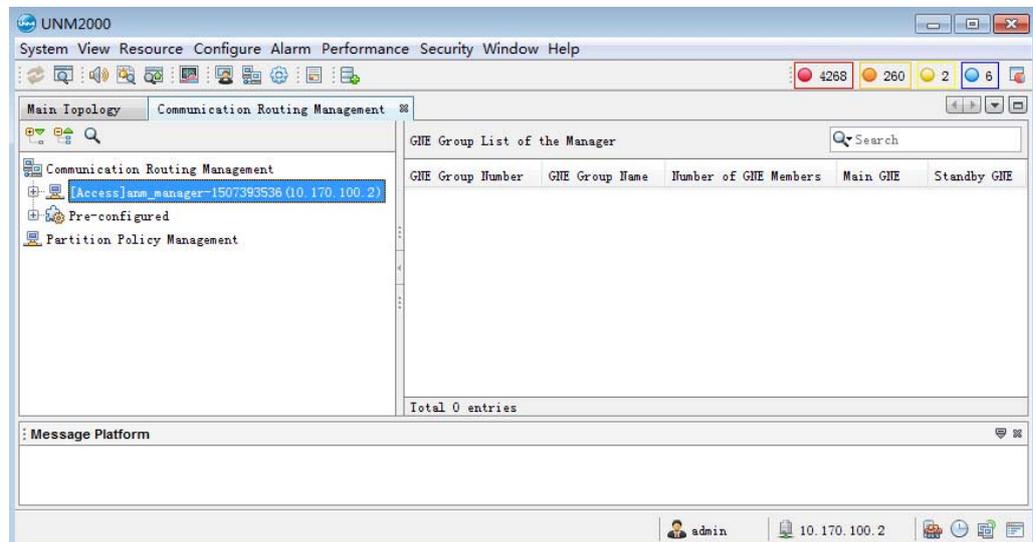
The NEs in the **Pre-configured** communication NE list are those without management program.

Prerequisite

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

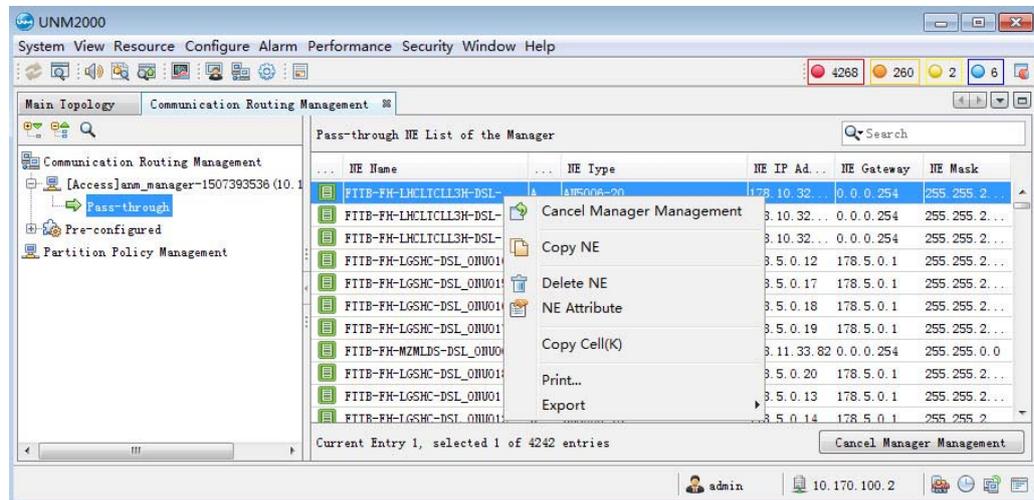
Procedure

1. Select **Configure** → **NE Communication Route Management** to open the **Communication Routing Management** tab.



2. In the left pane of the **Communication Routing Management** dialog box, click → **Pass-through** before the management program.

- 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

- Right-click a certain NE in the pre-configured common NE list and select **Select the Manager** from the shortcut menu, or click a certain NE in the pre-configured common NE list and click the **Select the Manager** button to select a management program for the NE again.
- 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.

Prerequisite

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

Procedure

- Select **Configure**→**NE Communication Route Management** to open the **Communication Routing 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 (N)**, **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 authorities of **Operator Group** or higher authorities.

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 NE during the creation, the NE will use the default SNMP parameter template **default**.

Procedure

1. In the main menu, select **Configure**→**SNMP Parameter Template** to open the **SNMP Parameter Template Management** tab.

Template Name	Alias	SNMP Version	SNMP Subjec...	Read the Co...	Write the C...	Retry Times	Timeout
default		snmp v2c		adsl	adsl	0	30000

SNMP Parameter Template

Template Name: Alias Name:

SNMP Version: SNMP Subject Name:

Read the Community Name: Write Community Name:

Number of Retries: Timeout Interval (ms):

2. Set various parameters in the **SNMP Parameter Template** pane at the bottom of the tab, and click **Create**. The detailed information of the newly created SNMP parameter template appears in the template list above.
3. Right-click a 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**. After the binding is performed, 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 **Attribute Page** 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.

The screenshot shows the 'Attribute Page' dialog box with the following fields and values:

Basic Information	
NE Type*	AN5116-06B
NE Name*	FIIB-FH-XXSN-2
NE IP Address	178.1.120.64
NE Mask	255.255.254.0
NE Gateway	178.1.120.1
Alias Name	
NE SN	
Manufacturer Name	Fiberhome
Remark	sz_693114087
Username	
Password	
longitude	0.02472
latitude	-0.87338
Communication Info	
Manager	ann_manager-1507393536 (10.17...
SNMP Parameter Template*	default
	default
	1

SNMP Parameter Template*
SNMP Parameter Template (required)

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 authorities of **Operator Group** or higher authorities.

Background Information

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

Procedure

1. In the main menu, select **Configure** → **SNMP Parameter Template** to open the **SNMP Parameter Template Management** tab.

Template Name	Alias	SIMP Version	SIMP Subject...	Read the Co...	Write the C...	Retry Times	Timeout
default		snmp v2c		adsl	adsl	0	30000

SIMP Parameter Template

Template Name: Alias Name:

SIMP Version: SIMP Subject Name:

Read the Community Name: Write Community Name:

Number of Retries: Timeout Interval (ms):

2. In the upper pane of the **SNMP Parameter Template Management** dialog box, select the desired SNMP parameter template.
 - 1) Modify the parameter settings in the **SNMP Parameter Template** pane at the lower part and then click **Create**.
 - 2) Click **Delete** to delete the SNMP parameter template.



Note:

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

4.3 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.

4.3.1 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 authorities of **Operator Group** or higher authorities.

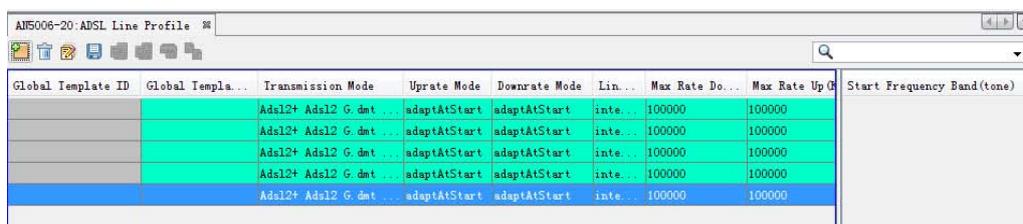


Note:

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 Config** 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 **ASDL Line Profile** tab.



Global Template ID	Global Templa...	Transmission Mode	Uprate Mode	Downrate Mode	Lin...	Max Rate Do...	Max Rate Up O	Start Frequency Band(tone)
		Adsl2+ Adsl2 G. dmt ...	adaptAtStart	adaptAtStart	inte...	100000	100000	
		Adsl2+ Adsl2 G. dmt ...	adaptAtStart	adaptAtStart	inte...	100000	100000	
		Adsl2+ Adsl2 G. dmt ...	adaptAtStart	adaptAtStart	inte...	100000	100000	
		Adsl2+ Adsl2 G. dmt ...	adaptAtStart	adaptAtStart	inte...	100000	100000	
		Adsl2+ Adsl2 G. dmt ...	adaptAtStart	adaptAtStart	inte...	100000	100000	

- 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**, **Modify**, **Compare Templates**, **Bind to System Card / Port**, etc.

4.3.2 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 authorities of **Operator Group** or higher authorities.



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

- Select **Configure**→**Global Template Config** from the main menu to open the **Global Template Management** tab.
- 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, type the number of templates to be added and then 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**.

Global Template ID	Global Template Name	Packet Type	Enable/Disable	Speed(kbit/s)
1		broadcast	enable	64
		multicast	disable	
		unknown	disable	

4.3.3 Modifying a Global Template

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

Background Information

- ◆ If you only modify the parameter settings of the template with the template name unchanged, the UNM2000 will automatically update the parameter settings of the template. If the template is bound with a device, the template parameter settings on the device are inconsistent with those in the UNM2000. To ensure the consistency of the template parameter settings on the device and in the UNM2000, see [Binding / Unbinding a Global Template](#).
- ◆ If you modify the name of the template, the UNM2000 will create a template with the new name and the old template will be deleted from the UNM2000. If the template is bound with a device, the template on the device will lose the reference relationship with the template in the UNM2000.

Prerequisite

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

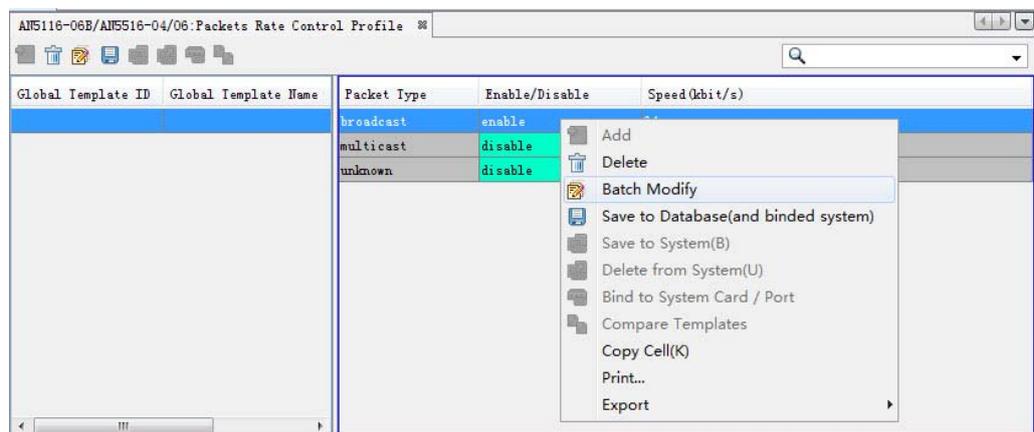


Note:

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 Config** 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. Right-click the desired template and select **Batch Modify** to open the **Batch Modify** dialog box.



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

Modify in a batch manner

Select	Number	Column Name	Type
<input type="checkbox"/>	1	Packet Type	*Uneditable
<input type="checkbox"/>	2	Enable/Disable	Radio Drop-Down Box
<input type="checkbox"/>	3	Speed (kbit/s)	Positive Integer

Configuration Item

Initial: Repeat:

Step:

Modify the Selected Rows

Reset OK Cancel Apply

4.3.4 Binding / Unbinding a Global Template

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 authorities of **Operator Group** or higher authorities.



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 Config** 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 the template and click  or select **Save to System** from the shortcut menu to open the **Select Object** dialog box. Select the system to be bound and click the **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 desired device and click **OK**.

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**.

4.3.5 Deleting a Global Template

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

Prerequisite

- ◆ You have the authorities of **Operator Group** or higher authorities.
- ◆ 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 Config** from the main menu to open the **Global Template Management** tab.
2. Select **ADSL Line Profile** in the left pane to open the **ASDL Line Profile** tab.

Global Template ID	Global Templa...	Transmission Mode	Uprate Mode	Downrate Mode	Lin...	Max Rate Do...	Max Rate Up G	Start Frequency Band(tone)
		Adsl2+ Adsl2 G. dmt ...	adaptAtStart	adaptAtStart	inte...	100000	100000	
		Adsl2+ Adsl2 G. dmt ...	adaptAtStart	adaptAtStart	inte...	100000	100000	
		Adsl2+ Adsl2 G. dmt ...	adaptAtStart	adaptAtStart	inte...	100000	100000	
		Adsl2+ Adsl2 G. dmt ...	adaptAtStart	adaptAtStart	inte...	100000	100000	

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**.

Global Template ID	Global Template Name	Transmission Mode	Uprate Mode	Downrate Mode	Line Type	Max Rate Down(Kbit/s)	Max Rate Up	Start Frequen
		Adsl2+ Adsl2 G. d...	adaptAtStart	adaptAtStart	interleave	100000	100000	
		Adsl2+ Adsl2 G. d...	adaptAtStart	adaptAtStart	interleave	100000	100000	
		Adsl2+ Adsl2 G. d...	adaptAtStart	adaptAtStart	interleave	100000	100000	
		Adsl2+ Adsl2 G. d...	adaptAtStart	adaptAtStart	interleave	100000	100000	

Configure the Selection Range

Select Range

All

Select Line

Current Row

OK Cancel

4.4 Global Configuration Management

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.

4.4.1 Viewing the Global Template

The user 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 authorities of **Operator Group** or higher authorities.



Note:

The following uses the **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 Config** 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, displaying the existing voice VLAN data.

Global Configuration ID	Global Configuration Name	VoIP Vlan Type	Service NAME	Svlan Tpid	Svlan Id	Svlan Cos	Cvlan Tpid	Cvlan Id	Cvlan Cos
2		signal vlan		33024	5	33024			
		RIP vlan		33024	5	33024			

4.4.2 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 authorities of **Operator Group** or higher authorities.



Note:

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

Procedure

1. Select **Configure**→**Global Template Config** from the main menu to open the **Global Template Management** tab.
2. In the left pane, select **Global Config**→**Service Configure**→**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 automatically generates the **Global Configuration ID**.

4.4.3 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 authorities of **Operator Group** or higher authorities.



Note:

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

Procedure

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

4.4.4 Binding / Unbinding the Global Configuration

Bind the global configuration with a device so that the parameter settings of the device are consistent with those set in the global configuration in the UNM2000.

Prerequisite

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



Note:

The following uses the **IGMP Mode** under **Service Configure** 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 Config** from the main menu to open the **Global Template Management** tab.
2. In the left pane, select **Global Config**→**Service Configure**→**IGMP Mode** to open the **IGMP Mode** tab.
3. Select the desired configuration and click  or select **Save Configuration to Device** from the shortcut menu. In the displayed **Please select card** dialog box, select the NE to which the configuration is to be issued and click **OK**.
4. The **Select Port** dialog box appears. Select a desired port and click **OK**.

4.4.5 Deleting a Global Configuration Template

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

Prerequisite

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



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 Config** 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. 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 Tracing Signaling

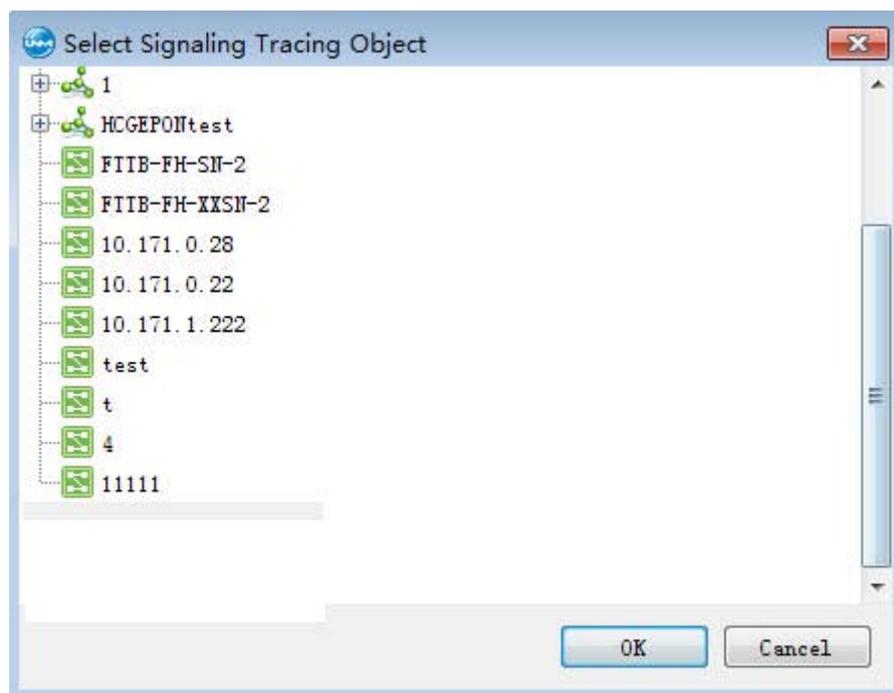
Tracing the signaling is used to trace the signaling frame of the communication between the current IAD and the voice communication card, so as to find the communication faults in a timely manner.

Background Information

This function is available only to the FTTH type ONUs and the FTTB type ONUs that support the voice service.

Procedure

1. In the main menu, select **Configure**→**Signaling Trace** to open the **Select Signaling Tracing Object** dialog box.



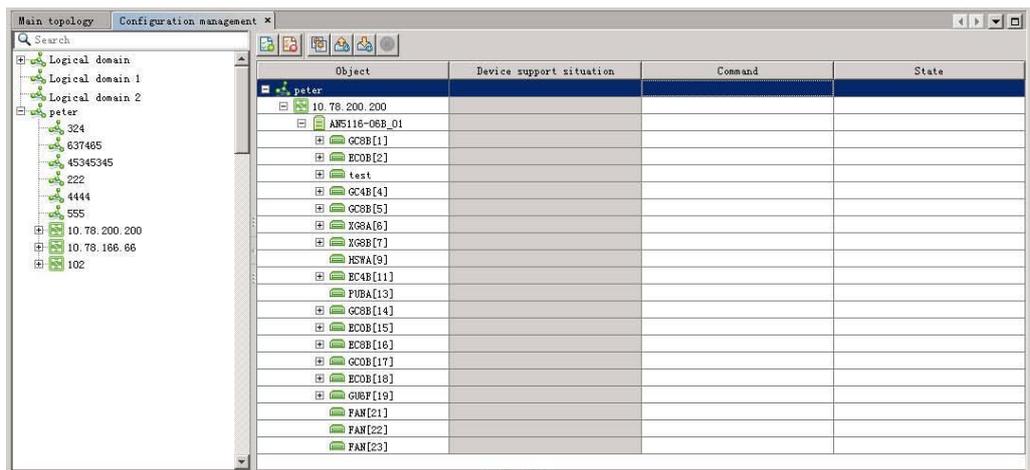
2. Select the signaling tracing object in the left pane and click **New** to add one row in the right pane. Then set **IP address**, **Four-layer source port number**, and **4 Level Destination Port Number**.
3. Click **OK** to open the **Signal Trace** tab.
4. Click **Start** to perform tracing signaling.

4.6 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. Click **Configure**→**Configuration Synchronization** in the main menu to open the **Synchronize the Configuration** tab.
2. Right-click the objects to be compared and select **Add Selected and Sub-items** from the shortcut menu. The selected objects will be added to the right comparison zone.



3. Select the objects to be compared in the comparison zone, and click  to compare the configuration.

Object	Device support situation	Command	State
AN5116-06B_01		Compare configuration	Executing
GC8B [1]		Compare configuration	Executing
GC8B [2]		Compare configuration	Executing
GC4B [3]		Compare configuration	Executing
EC8B [4]		Compare configuration	Executing
GC8B [5]		Compare configuration	Executing
EC4B [7]		Compare configuration	Executing
GC4B [8]		Compare configuration	Executing
MSWA [10]		Compare configuration	Executing
GC8B [11]		Compare configuration	Executing
EC8B [12]		Compare configuration	Executing
PUBA [13]		Compare configuration	Executing
EC0B [14]		Compare configuration	Executing
EC4B [15]		Compare configuration	Executing
XG8A [16]		Compare configuration	Executing
GC4B [17]		Compare configuration	Executing
GU4E [19]		Compare configuration	Executing
HU1A [20]		Compare configuration	Executing
FAN [21]		Compare configuration	Executing
FAN [22]		Compare configuration	Executing
FAN [23]		Compare configuration	Executing
HCU-OLT [801]		Compare configuration	Executing



Note:

The comparison results displayed in the **Status** column are described as follows:

- ◆ Completed: The configuration data are consistent.
- ◆ Inconsistent: The configuration data are inconsistent.
- ◆ Failure / Command timeout: Communication error between the UNM2000 and the device.

Subsequent Operation

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

Table 4-1 Configuration Uploading / Downloading

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

The result of configuration uploading is as shown in the figure.

Object	Device support situation	Command	State
[-] peter			Executing
[-] 10.78.200.200			Executing
[-] ANS116-06B_01		Upload configuration	Executing
[-] GCBB[1]		Upload configuration	Executing
[-] ECOB[2]		Upload configuration	Executing
[-] test		Upload configuration	Executing
[-] GC4B[4]		Upload configuration	Executing
[-] GCBB[5]		Upload configuration	Executing
[-] XGSA[6]		Upload configuration	Executing
[-] XGSE[7]		Upload configuration	Executing
[-] HSWA[9]		Upload configuration	Executing
[-] EC4B[11]		Upload configuration	Executing
[-] PUBA[13]		Upload configuration	Executing
[-] GCBB[14]		Upload configuration	Executing
[-] ECOB[15]		Upload configuration	Executing
[-] ECOB[16]		Upload configuration	Executing
[-] GCOB[17]		Upload configuration	Executing
[-] ECOB[18]		Upload configuration	Executing
[-] GUBF[19]		Upload configuration	Executing
[-] FAN[21]		Upload configuration	Executing
[-] FAN[22]		Upload configuration	Executing
[-] FAN[23]		Upload configuration	Executing

4.7 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.

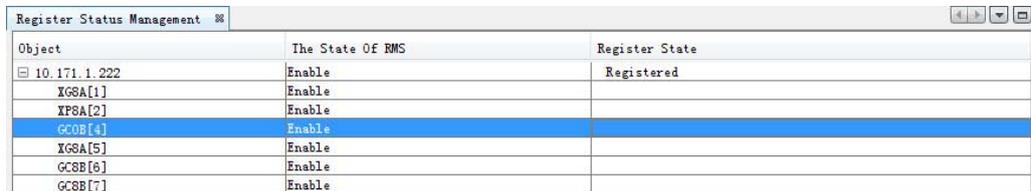
Prerequisite

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

Procedure

1. Select **Configure**→**Network Access Status Management** to open the **Network Access Status Management** tab.
2. Select the desired object in the object tree and select the **Query Status (Q)** 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 (M)** / **Send the Selected Line Card RMS Connection Status (C)** button to enable the interconnection with the resource management system.

- Select the system / card to be registered and click the **Initiate Registration / Initiate Registration of the Selected Line Cards** button. After the registration succeeds, the status is as shown in the following figure.



Object	The State Of RMS	Register State
10.171.1.222	Enable	Registered
IGSA[1]	Enable	
IPSA[2]	Enable	
GCOB[4]	Enable	
IGSA[5]	Enable	
GCBB[6]	Enable	
GCBB[7]	Enable	

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

4.8 Home Gateway MAC Range Configuration

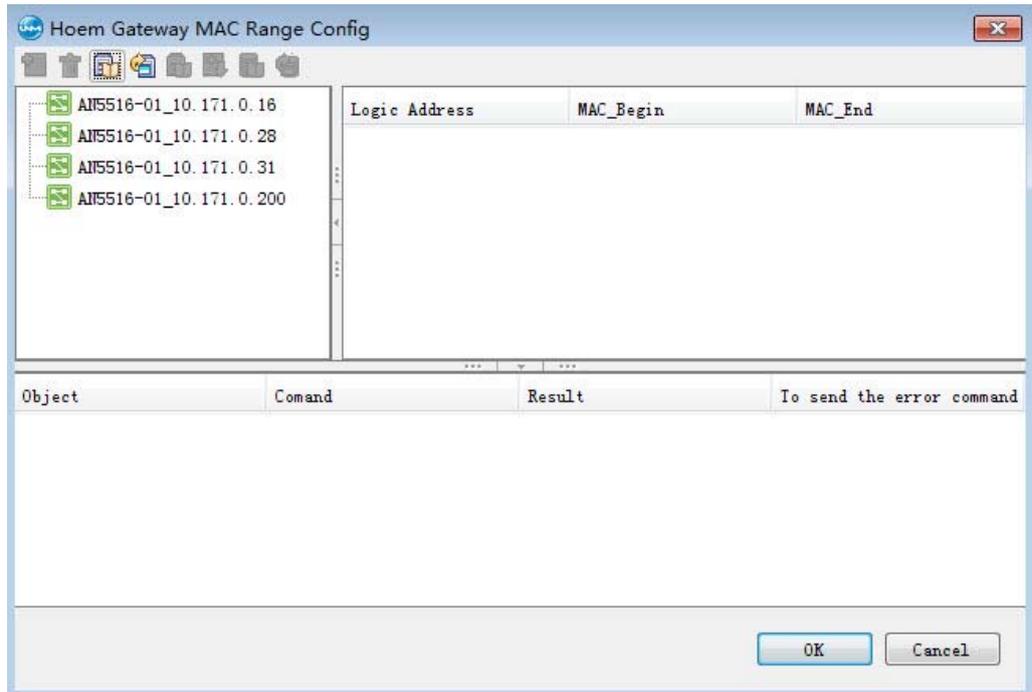
The UNM2000 enables you to configure the home gateways in a batch manner, which effectively lowers the heavy workload of configuring the NEs one by one.

Prerequisite

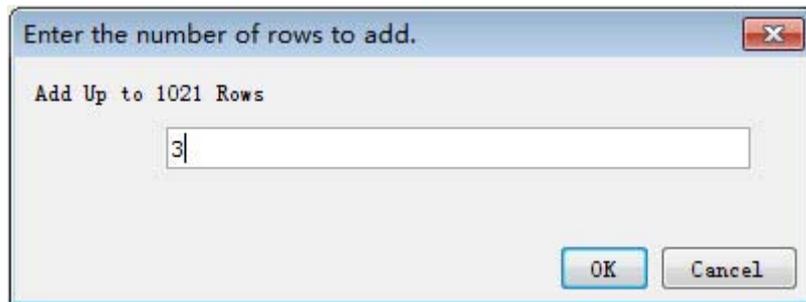
You have the authorities of **Operator Group** or higher authorities.

Procedure

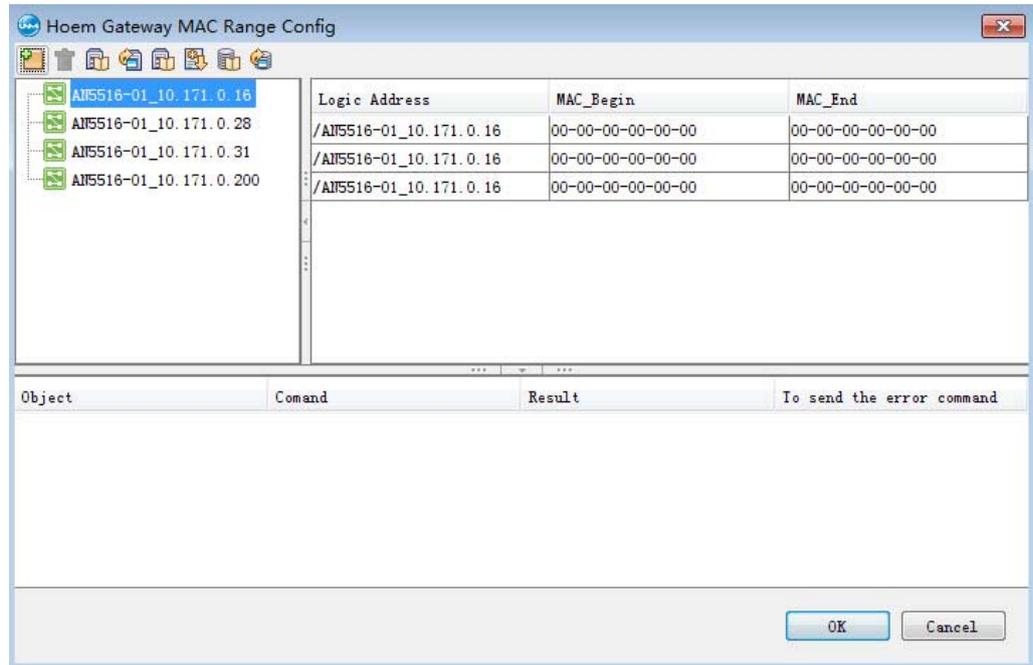
- On the UNM2000 main menu, select **Configure**→**Home Gateway MAC Range Configure** to open the **Home Gateway MAC Range Configure** dialog box.



2. In the left pane of the dialog box, select the desired NE and click  to enter the number of entries to be added.



3. Configure the start MAC address of the home gateways in a batch manner according to the planning data.



4. Select the configured multiple home gateway entries and click  to deliver them to the device.

4.9 Pre-deploying ONUs

In some network deployment, there are a great number of remote ONUs far away from the equipment room of the central office and dispersed. However, the UNM2000 enables you to implement pre-deployment of NEs and their corresponding services via importing a table. This achieves offline batch-configuration and plug-and-play of ONUs.

Prerequisite

- ◆ You have understood the deployment planning and service configuration planning of the network devices.
- ◆ You have the authorities of **Operator Group** or higher authorities.
- ◆ The OLT device has been added to the UNM2000.

Procedure

1. In the main menu of the UNM2000, select **Configure**→**Pre-deploy ONUs** to open the **Pre-deploy ONU Configuration** dialog box.
2. Click the  button to download the template and save it to the local computer.
3. Complete the ONU parameter settings according to the examples in the downloaded template.
4. In the **Pre-deploy ONU Configuration** dialog box, click  to import the parameter configuration file into the UNM2000.
5. The **Pre-deploy ONU Configuration** dialog box displays the imported parameter configuration information. You can click the tab at the bottom of the dialog box to view the corresponding configuration entries.

Subsequent Operation

1. When the ONU is provisioned, select the corresponding configuration entry and click  to deliver the pre-deployment parameters to the ONU so as to complete the service data configuration.

Other Operations

- ◆ Click  to export the configuration data in the UNM2000 to the local client end as a configuration template.
- ◆ Click  to add configuration data entries in the current configuration tab.
- ◆ Click  to delete the selected configuration data entries.
- ◆ Click  to query the existing pre-deployed configuration data.

4.10 Pinging NEs

Ping operations are used to check the communication between the NE and the network management system.

Procedure

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

4.11 Telneting NEs

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. See [Setting the Telnet Proxy Server](#) for the Telnet proxy server settings.

Procedures

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.

4.12 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.

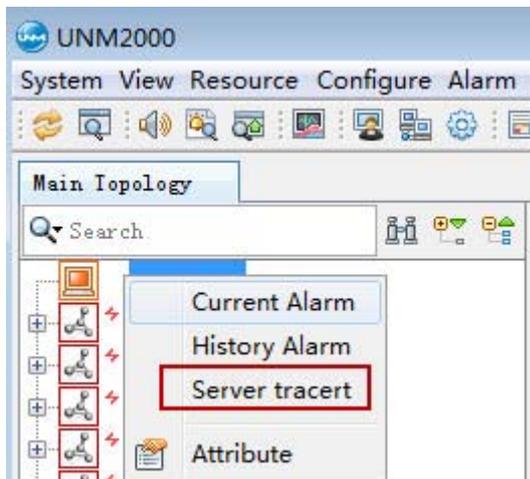
The command is **Tracert** on Windows OS and it is **Traceroute** on UNIX OS.

Prerequisite

- ◆ The authority of the Tracert function is configured in the authority and domain division management. Only the user who has the corresponding authority can 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 **Object Tree** pane of the UNM2000 main topology, right-click **Local NMS** and select **Server tracert**, as shown below:



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, as shown below:



4.13 PON Configuration Transfer

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

Prerequisite

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

Procedure

1. Select **Config**→**PON Config Transfer** from the main menu to open **PON Config Transfer** dialog box.



2. Set the parameters, such as IP addresses of the source and sink OLTs.
3. Click **Execute**.
4. Click **OK** 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 reflect the network connection status and operating status of the equipment. Users 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 Virtual Connection
- Editing NEs
- Editing a Fiber Connection
- Checking 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.

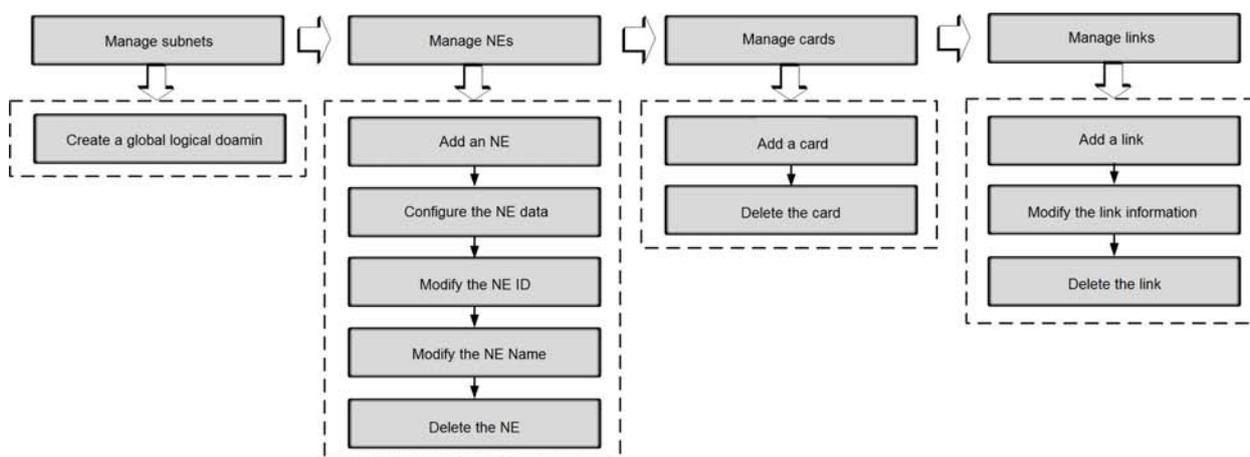


Figure 5-1 Network Topology Creation Flow

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 flow for creating the network topology is as shown in Table 5-1

Table 5-1 Description of the Network Topology Creation Flow

Procedures	Operation	Description
Manage the subnet	Creating a Global Logical Domain	For convenient management of NEs, you can place the topological objects in the same area or of the same attribute into a same logical domain.
Manage the NE	Creating an 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 a 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)

Procedures	Operation	Description
	Modify the NE name	You can modify the NE name as needed. 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 of the NE is required, you can delete the card from the NE panel.
Manage the link	Creating a Link	You can create links, fibers / cables as well as virtual fibers.
	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 authorities of **Operator Group** or higher authorities.

Procedure

1. In the main menu, select **Resource**→**Create Logical Domain** to open the **Create Logical Domain** dialog box.
2. Set the parameters, among which **Logical Domain Name** is required and others 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 Creating an Access NE

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

Prerequisite

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

Procedure

1. Right-click the logical domain, and select **Create NE**→**Create Access NE**, or click the logical domain and select **Resource**→**Create NE**→**Create Access NE** in the main menu to open the **Create Access NE** dialog box.
2. Configure the parameters according to Table 5-2.

Table 5-2 Setting Items of Creating the Access NE

Setting Item	Description	Remark
NE Type	The type of the NE.	Required.
Default Shelf Type	After the NE type is selected, the corresponding subrack (shelf) type will be determined by the system.	

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

Setting Item	Description	Remark
NE Name	The name of the NE for identification.	
NE IP Address	The IP address of the NE.	
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.	Optional.
Manufacturer Name		
Remark		
Username		
Password		
Longitude	The longitude and latitude of the physical area to which the device locates, convenient for locating.	
Latitude		
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 profile used for the communication between the UNM2000 server and various NEs. Generally select the default template.	-

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

5.3.2 Creating Other NEs

To display the topological relationship between the NEs that can be directly managed and the NEs that cannot be directly managed in the topograph, you need to create virtual NEs (representing the NEs that cannot be directly managed) to implement unified management of the NEs in the entire network.

Background Information

Virtual NE

- ◆ The virtual NE is the abstract concept of the NEs that cannot be directly managed by the UNM2000. In case the NEs managed by other EMS instead of the UNM2000 exist in the network and paths are created between these NEs and the NEs managed by the UNM2000, you can create virtual NEs in the UNM2000 to present their topological relationship in the topograph.
- ◆ Different from the actual NEs, the virtual NEs has no restriction on hardware device and therefore they can be used to represent any unknown devices.
- ◆ The procedure of creating or deleting a virtual NE is similar to that of creating or deleting an actual NE.

Prerequisite

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

Procedure

1. Right-click the logical domain and select **Create NE**→**Create Other NE**, or click the logical domain and select **Resource**→**Create NE**→**Create Other NE** in the main menu to open the **Create a Virtual NE** dialog box.
2. Set the NE type of the virtual NE to **VIRTUAL_NE**, and configure other parameters as required.
3. After configuring the parameters, click **OK**. The created virtual NE appears in the logical domain or main topology.

5.3.3 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.

5.3.3.1 Viewing NE Automatic Discovery Tasks

You can view the existing NE automatic discovery tasks to check whether they meet the requirements for network development.

Prerequisite

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

Procedure

- Select one of the following access methods to open the **Policy Task Management** tab to view the existing NE automatic discovery tasks.
 - In the main menu, select **Resource**→**Auto NE Discovery**.
 - In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window. In the left pane, select **Data Synchronization**→**Auto Detect NE Task**.

No.	Task Name	Enable	Task Type	Execution ...	Task Progress	Task Status	Execution ...	Start Time of the Task
337	test	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05
338	111111111111	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05
339	moli	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05

Current Entry 1, selected 1 of 3 entries

Refresh Create Delete Execute Now

- Click a desired NE automatic discovery task in the left pane to view the IP address, type and status of the automatically discovered NE.

No.	Task Name	Enable	Task Type	Execution ...	Task Progress	Task Status	Execution ...	Start Time of the Task
106	1	<input checked="" type="checkbox"/>	Auto Detect NE Task	One-off	0%	Free	Succeeded	2014-09-23 15:25:21

Current Entry 1, selected 1 of 1 entries

Refresh Create Delete Stop Execute Now Hide Details

IP Address	NE Type	Status
10.170.99.160	AMS116-06B	NE Exists
10.170.99.161	AMS116-06B	NE Exists
10.170.99.162	AMS116-06B	NE Exists
10.170.99.163	AMS116-06B	NE Exists

Total 254 entries

Refresh Create All Create Selected

5.3.3.2 Adding an NE Automatic Discovery Task

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

Prerequisite

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

Procedure

- Select one of the following access methods to open the **Policy Task Management** tab.
 - In the main menu, select **Resource**→**Auto NE Discovery**.
 - In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window. In the left pane, select **Data Synchronization**→**Auto Detect NE Task**.

No.	Task Name	Enable	Task Type	Execution ...	Task Progress	Task Status	Execution ...	Start Time of the Task
337	test	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05
338	111111111111	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05
339	moli	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05

Current Entry 1, selected 1 of 3 entries

Refresh Create Delete Execute Now

- 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** to open the dialog box.
- Set the related parameters in the **Basic information** and **Extend information** tabs, and click **OK** after completing the settings. Then the added tasks will be displayed in the task list.

The image displays two screenshots of the 'Create Auto Detect NE Task' dialog box. The top screenshot shows the 'Basic information' tab, which includes fields for 'Task name', 'Enable' (checked), 'Task Type' (radio buttons for 'One time', 'Every', 'Every week', 'Every month'), 'Execution time', 'Start time', and 'End time'. The bottom screenshot shows the 'Extend information' tab, which includes fields for 'IP Address Range', 'Detect Parameter Settings' (SNMP Parameter Template, Auto Create NE, NE Name Prefix, Logic Domain of the NE), and 'Filter IP List'.



Note:

- ◆ Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name** of other tasks. This can improve the setting efficiency.
- ◆ In the **Extend information** tab, click **Import IP Address** to import the IP addresses in a batch manner.

5.3.3.3 Automatic Discovery of NEs

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

Prerequisite

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

Procedure

- Select one of the following access methods to open the **Policy Task Management** tab and view the existing NE automatic discovery tasks.
 - In the main menu, select **Resource**→**Auto NE Discovery**.
 - In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window. In the left pane, select **Data Synchronization**→**Auto Detect NE Task**.

No.	Task Name	Enable	Task Type	Execution ...	Task Progress	Task Status	Execution ...	Start Time of the Task
337	test	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05
338	111111111111	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05
339	moli	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05

Current Entry 1, selected 1 of 3 entries

Refresh Create Delete Execute Now

- Right-click the task, and select **Execute Now**, or click the task, and then click the **Execute Now** button at the bottom of the tab to execute the NE automatic 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

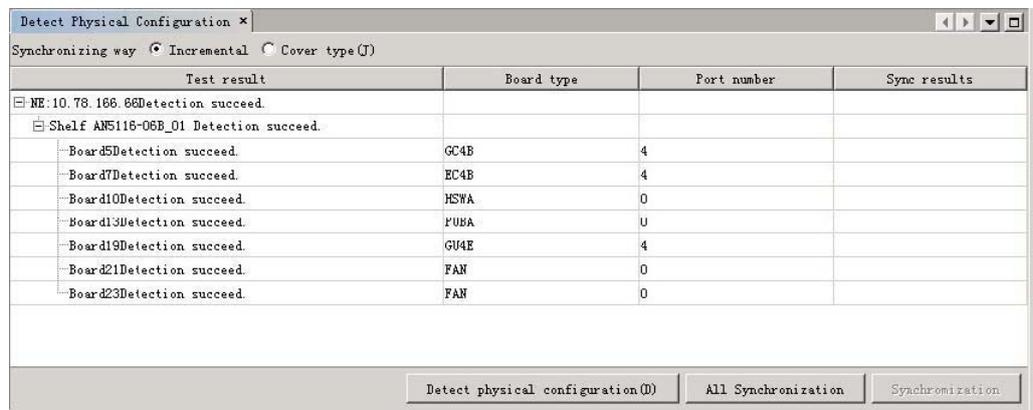
The physical configuration detection function enables you to implement the automatic discovery of physical cards, which then can be synchronized to the UNM2000 automatically using the synchronization operation.

Prerequisite

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

Procedure

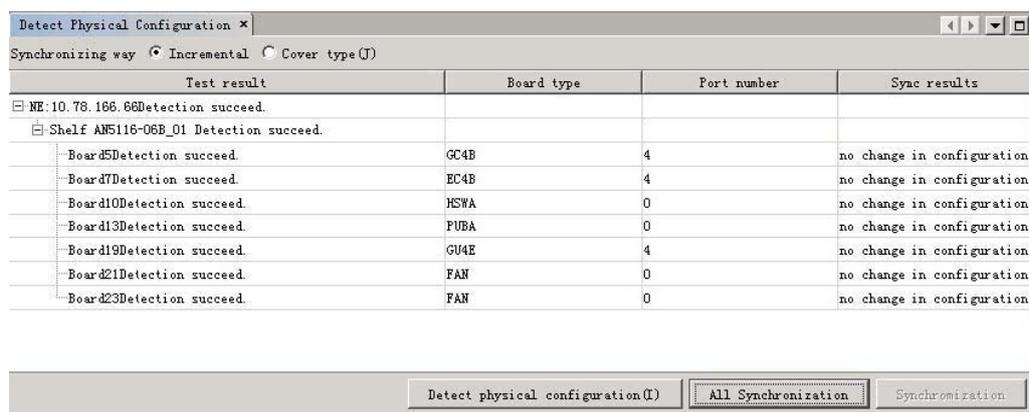
1. In the main menu, select **Resource**→**Detect Physical Configuration** to open the **Detect Physical Configuration** tab.
2. Select the system to be detected in the object tree pane, and click **Detect Physical Configuration (D)** at the lower part of the tab to execute the detection command. Then 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 network management system).
Cover type	Overrides the current configuration in the network management system using the newest physical card configurations.



5.4.2 Adding Cards Manually

Users can add cards manually or pre-configure cards as required.

Prerequisite

- ◆ You have the authorities of **Operator Group** or higher authorities.
- ◆ 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.
 - ▶ Add 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 actual card quantity and the corresponding card location of the project.
- ▶ Add a single card.

Right-click the slot of the card in the subrack view and select **Add Card**→ to add the corresponding card according to the actual card quantity and the corresponding card location of the project.

5.5 Creating a Virtual Connection

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. This kind of connection is called virtual connection.

Prerequisite

- ◆ You have the authorities of **Operator Group** or higher authorities.
- ◆ 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. Set the parameters according to Table 5-4.

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 sink NE of the virtual connection.

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

Parameter	Description
Direction	Includes the following four types: <ul style="list-style-type: none"> ◆ Bidirectional: The connection line has bidirectional arrows. ◆ Forward: The connection line has an arrow from the source NE to the sink NE. ◆ Backward: The connection line has an arrow from the sink NE to the source NE. ◆ None: The connection line has no directional arrows.
Control Point Format	Includes folding line and curve.
Width	The width of the connection line. It ranges from 1 to 10; the bigger this value is, the wider the line is.

3. After completing the settings, click **OK**. The connection line appears between the source and sink NEs.

5.6 Editing NEs

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.

Prerequisite

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

Procedure

1. Right-click the desired NE and select **Attribute** from the shortcut menu to open the **Attribute Page** pane.

The screenshot shows the 'Attribute Page' window with the following configuration details:

Basic Information	
NE Type*	AN5116-06B
NE Name*	10.190.41.100
NE IP Address	10.190.41.100
NE Mask	255.255.255.0
NE Gateway	0.0.0.0
Alias Name	
NE SN	
Manufacturer Name	
Remark	
Username	
Password	
longitude	-0.13664
latitude	0.08926
Communication Info	
Manager	ann_manager-1507393536 (10...
SIMP Parameter Template*	default

Below the table, there are fields for (Name) and (Description).

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 authorities of **Operator Group** or higher authorities.

Procedure

1. 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. Click **OK**.

5.6.3 Setting the Displayed Contents 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 authorities of **Operator Group** or higher authorities.

Procedure

1. In the main menu, select **View**→**Topology View**→**Show NE IP and Type**. This sub-menu option will be selected and the NE icon will display its IP address and type.



5.6.4 Tagging NEs

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

Prerequisite

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

Procedure

1. In the **Main topology** tab, select the NE to be added with a tag.
2. Select **Resource**→**Mark the NE As** in 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 the object with a tag.

Procedure

1. Select **View**→**Label Query** in the main menu to open the **Label Query** tab, which displays all the objects that have been labeled by default.
2. Perform the following operations as required:
 - ▶ **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.

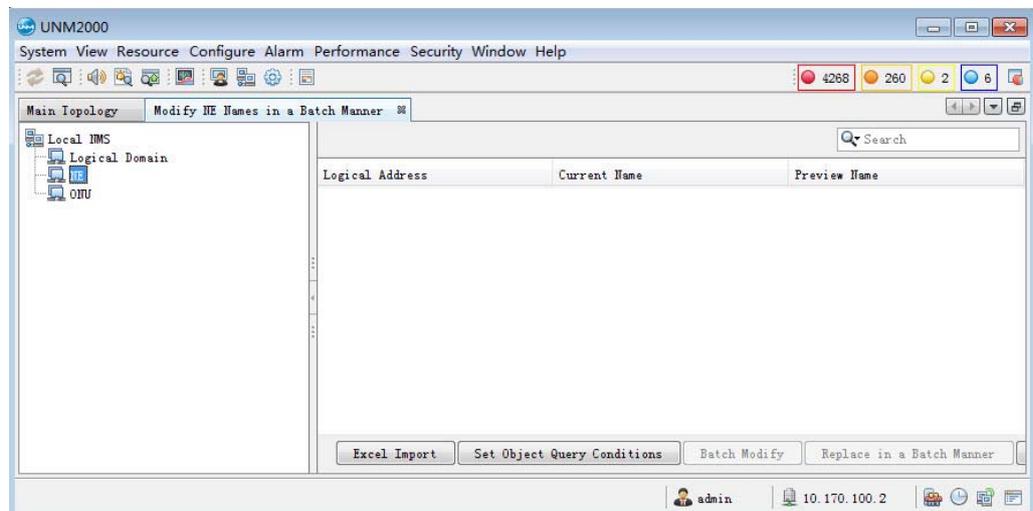
5.6.6 Modify NE Names in a Batch Manner

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.

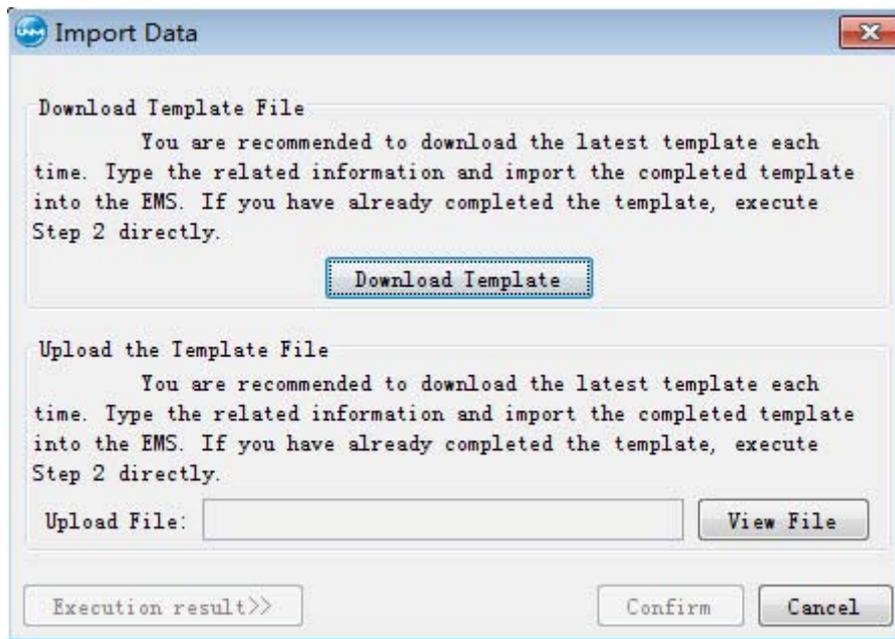
Prerequisite

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

1. Select **Resource**→**Batch modify NE name** from the main menu and open the **Batch modify NE name** tab.



2. In the left pane of the **Modify NE Names in a Batch Manner** tab, click **NE** 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.

	A	B	C
1	Logical Address	Current Name*	Preview Name*
2	/AN5116-20_10.171.0.38	AN5116-20_10.171.0.38	AN5116-20_10.171.0.38
3	/AN5116-30_10.171.0.39	AN5116-30_10.171.0.39	AN5116-30_10.171.0.39
4			
5			

- iii) In the **Import Data** dialog box, select **View File** to upload the Excel table already edited and then click **OK**.

Logical Address	Current Name	Preview Name
/AN5006-30_10.171.0.39	AN5006-30_10.171.0.39	AN5006-30_10.171.0.39
/AN5006-20_10.171.0.38	AN5006-20_10.171.0.38	AN5006-20_10.171.0.38

- Set the modification rules to batch-modify the NE names.
 - 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 Descriptions of Settings in the **Batch Modify** Dialog box

Parameter		Description
Information		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 batch-modify the NE names.
 - 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** 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

The following introduces how to modify the connection line properties and how to expand / collapse the connection line.

5.7.1 Modifying the Connection Line Properties

The user can modify the properties of the connection line between NEs; for example, direction, type and width.

Prerequisite

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

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, the user can collapse or expand the lines.

Prerequisite

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

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 Checking the Topology View

In the topology view, the user can know the network layout, and the networking operation of each NE.

5.8.1 Checking the Physical Topology View

In the physical topology view, the user 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 picture.

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, users 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

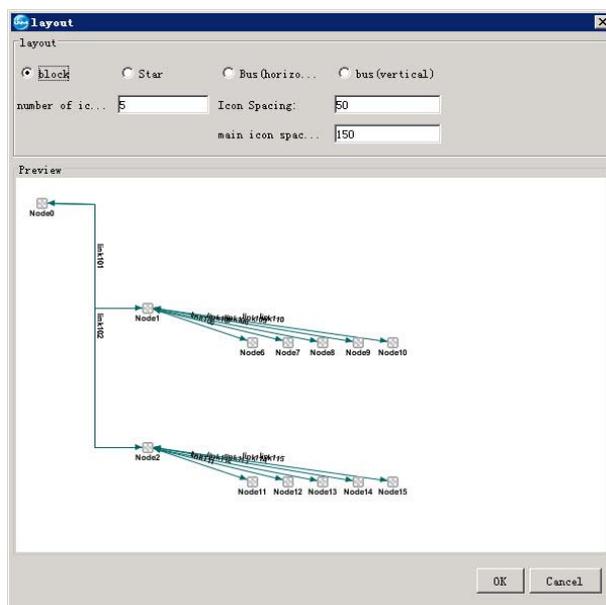
You can perform the following operations in the sub-topology view via the shortcut menus.

- ◆ Set the background image.

Right-click the blank area in the **Topology View** tab, and select **Set a 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 **Topology View** tab, and select **layout...** to open the **layout** dialog box.



- 2) Adjust the layout style as required, and preview the adjustment results in the **Preview** pane.
- 3) After completing the settings, click **OK**.

◆ Hide nodes.

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

◆ Manage the hidden nodes.

Right-click the blank area in the sub-topology view, select **Hidden Node Manager...**; select the hidden nodes to be displayed in the **Hidden Node Manager** dialog box, 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 icon...**; in the **edit icon** dialog box, set the size and style of the node icon, and click **OK**.

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

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

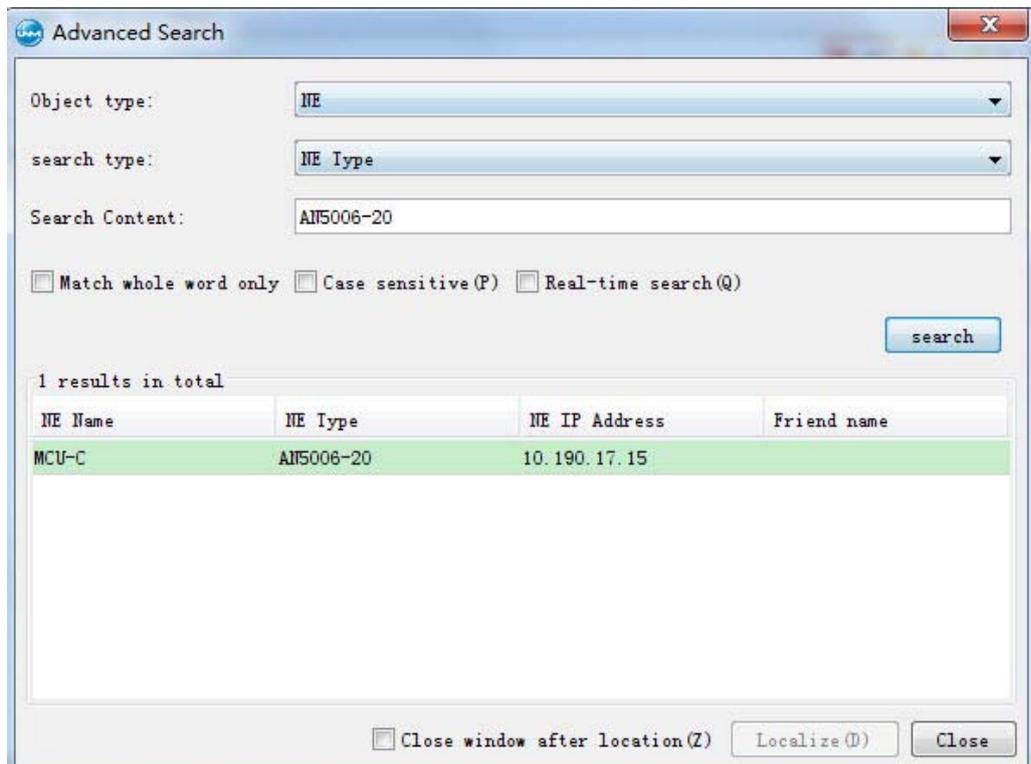
You can search for and locate the object quickly via the object search functions.

Background Information

The objects include NEs, logical domains and cards.

Procedures

1. Select **Resource**→**Search Object** in the main menu.
2. In the displayed **Advanced Search** dialog box, set the object type, search type and search content, and then click **Search**.



3. 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 authorities of **Operator Group** or higher authorities.

Procedure

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

5.9.2 Delete NEs

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 authorities of **Operator Group** or higher authorities.

Procedure

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



Caution:

Deleting an NE will delete all the related connections simultaneously.

5.9.3 Deleting the System

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 authorities of **Operator Group** or higher authorities.

Procedure

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

5.9.4 Deleting Cards

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 authorities of **Operator Group** or higher authorities.
- ◆ Before deleting a card, you need to delete the services and protection groups related to the card.

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) Click **Yes** in the displayed dialog box.
 - ▶ Delete a single card
 - a) Right-click the desired card in the device tree and select **Delete Card** from the shortcut menu.
 - b) Click **Yes** in the displayed dialog box.

6 Managing Access NEs

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

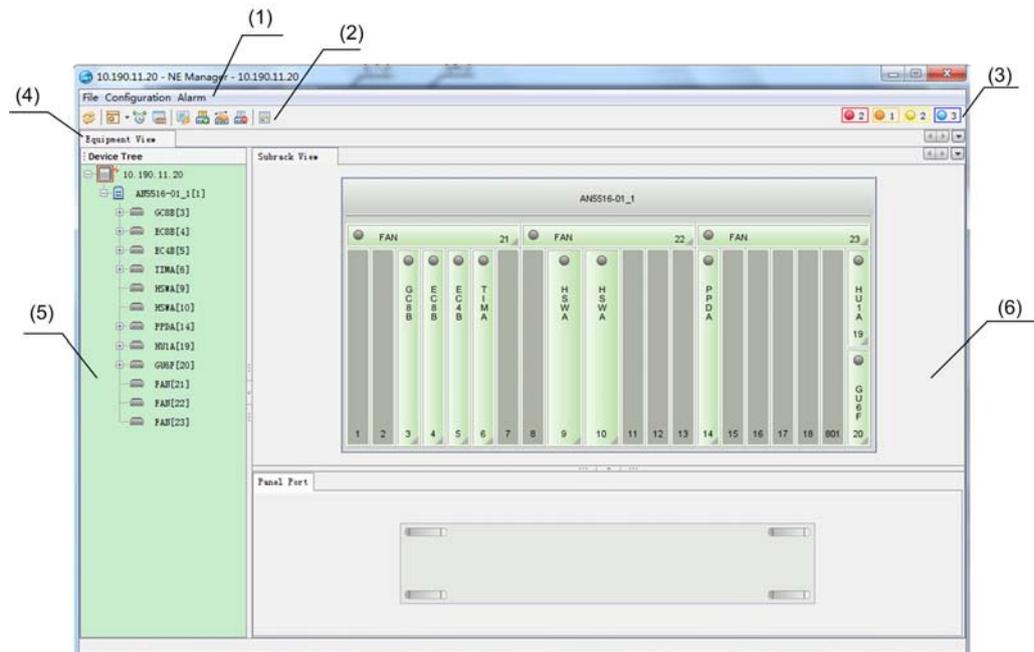
- The NE Manager GUI
- Configuring Local Services
- ONU Query Management
- Authorizing ONUs
- ONU Registration Management
- Rule Tasks of Enabling the ONU Port
- Authorizing Cards
- Synchronizing ONUs Manually
- Obtaining Unauthorized ONUs
- Authorizing ONUs Manually
- Comparing and Synchronizing the ONU Manually
- Querying the Card Software / Hardware Versions
- Upgrading the Card
- Managing the Test Task
- Managing ONU MGC Query Tasks
- Managing NE Automatic Discovery Tasks

6.1 The 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) Main menu | (2) Toolbar |
| (3) Alarm statistical panel | (4) View group |
| (5) Device tree / operational tree pane | (6) Display pane |

Figure 6-1 The NE Manager GUI

6.2 Configuring Local Services

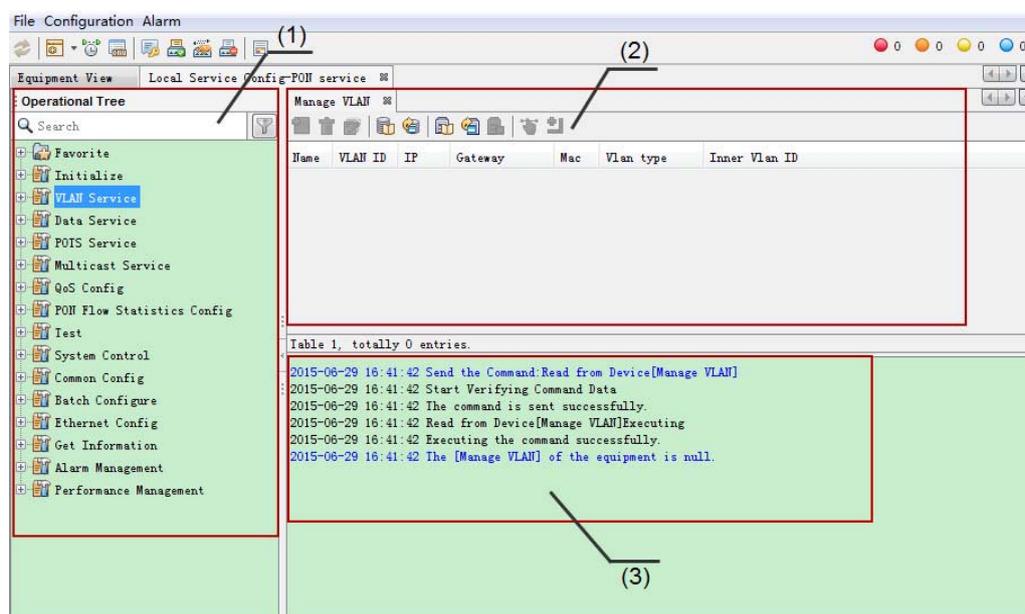
The following introduces the access method and GUI layout of the **Local Service Configuration** function in the **NE Manager**.

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, click **Configuration**→**Local Service Configuration**.

GUI Introduction

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



(1) The Operational Tree pane

(2) The service configuration pane

(3) The operation information pane

Figure 6-2 Local Service Configuration GUI

6.3 ONU Query Management

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 the ONU by different ONU attributes. It also supports fuzzy query and complete match. The ONU query conditions fall into two parts:

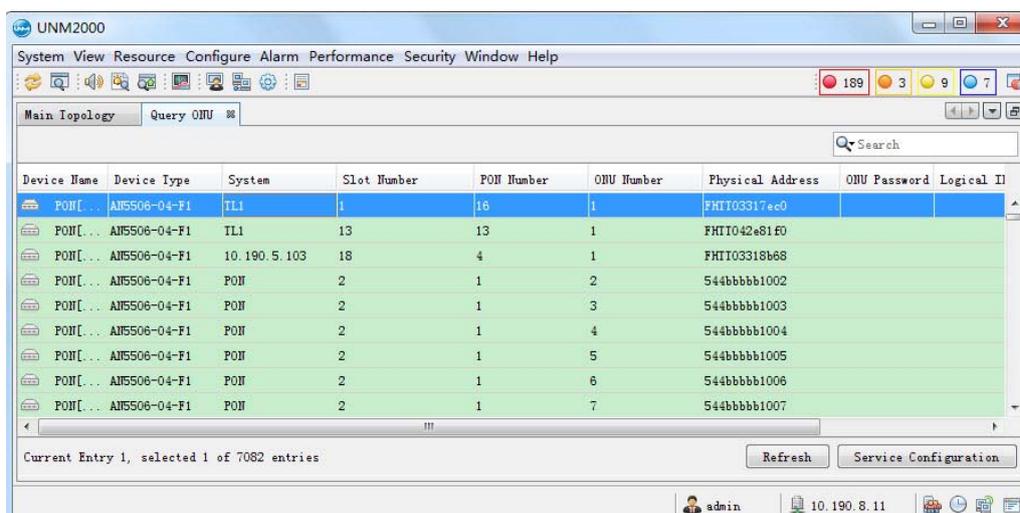
- ◆ General query conditions: Include the logical domain, type, name, logical ID, physical ID, OLT IP address, voice service and data service of the ONU.
- ◆ Advanced query conditions: Include slot No., ONU No., ONU password, logical SN password, optical splitter No., optical splitter port No., ONU label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

Prerequisite

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

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.



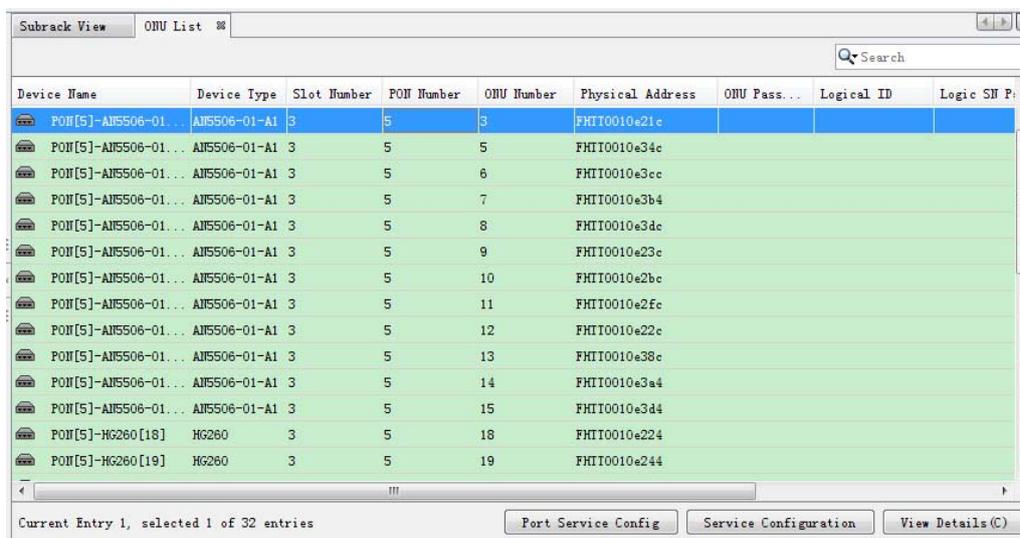
- In the **Query ONU** tab, select one or more entries and click **Service Configuration** at the lower-right corner to go to the **NE Manager** window. Then you can query the service configuration information of the ONU device.

6.3.2 Viewing the ONU List

The user can view the detailed ONU information and perform ONU configurations.

Procedure

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



2. You can also perform the following operations as required.

- ▶ Configure the port service.

Click **Port Service Config** to view the port type of the ONU service and the number of ports of different types.

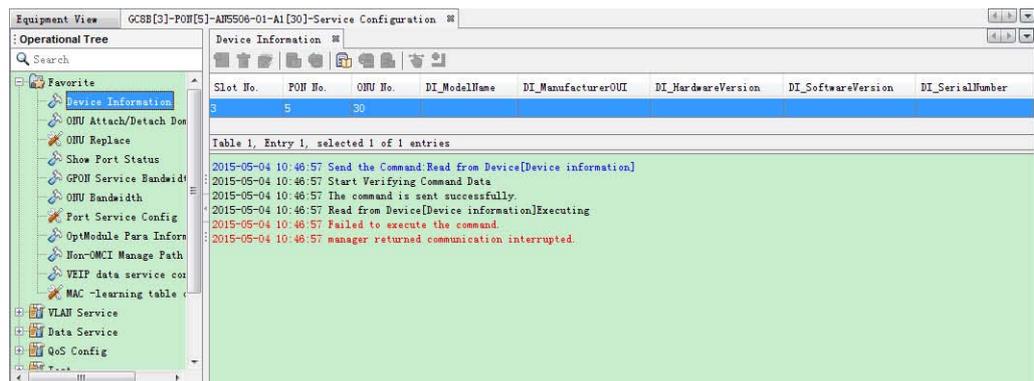


Port Category	Count
Data Port	4
Voice Port	2

(Data Source: Device) Total 2 entries

- ▶ Configure the service.

Click **Service Configuration** to access the designated ONU service configuration tab and perform the service configuration of the ONU.



Slot No.	PON No.	ONU No.	DI_ModelName	DI_ManufacturerOUI	DI_HardwareVersion	DI_SoftwareVersion	DI_SerialNumber
3	5	30					

Table 1, Entry 1, selected 1 of 1 entries

```

2015-05-04 10:46:57 Send the Command:Read from Device[Device information]
2015-05-04 10:46:57 Start Verifying Command Date
2015-05-04 10:46:57 The command is sent successfully.
2015-05-04 10:46:57 Read from Device[Device information]Executing
2015-05-04 10:46:57 Failed to execute the command.
2015-05-04 10:46:57 manager returned communication interrupted.

```

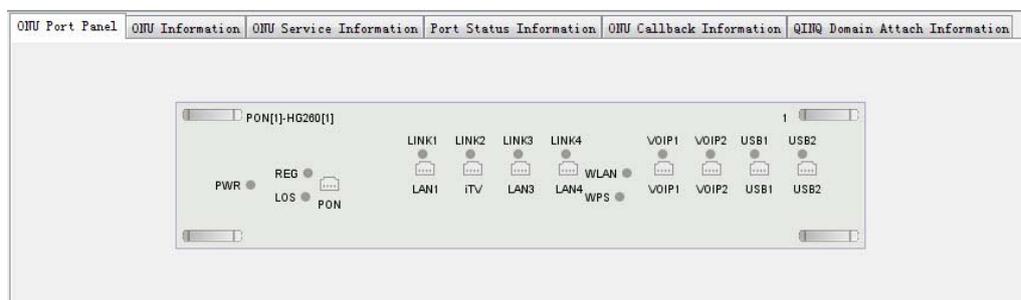


Note:

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 the details.

Click **View Details** to view the detailed information of the specified ONU, including **ONU Port Panel**, **ONU Information**, **ONU Service Information**, and **ONU Callback Information**.



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 Information

The UNM2000 supports querying the ONU by different ONU attributes. It also supports fuzzy query 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** in 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** in 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** in the main menu.
2. Select the logical domain where the desired ONU locates from the **Logical Domain** drop-down list.
3. Click the **Advanced** tab in the **Set ONU Query Conditions** dialog box.
4. Specify **Slot Number** and **ONU Number**.
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

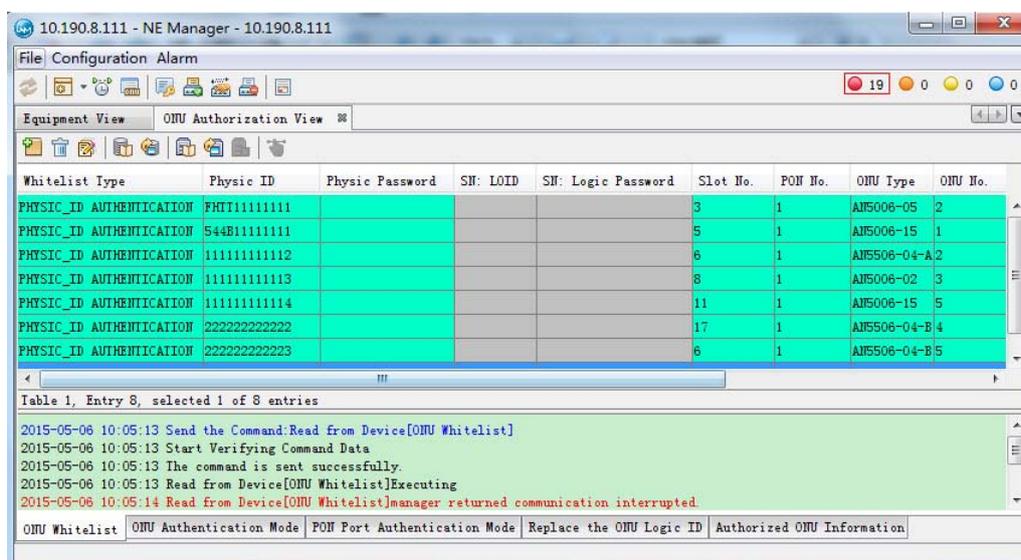
You can query the information of the authorized ONUS and pre-authorize the unauthorized ONUs. The ONUs in the white list can be authorized and service-provisioned, while the ONUs not in the whitelist cannot be authorized and provisioned.

Prerequisite

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

Procedure

1. In the **NE Manager GUI**, 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

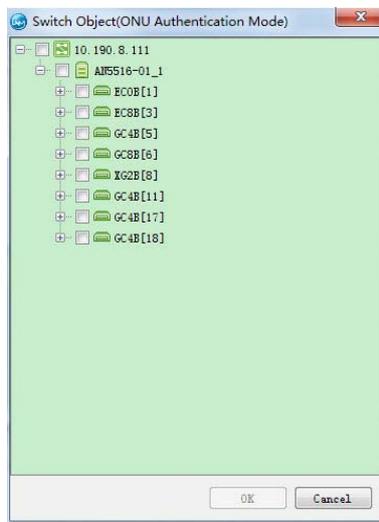
View and modify the authentication mode of the ONU connected to a single PON port, card or device.

Prerequisite

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

Procedure

1. In the NE Manager GUI, select **Configuration**→**ONU Authentication**→**ONU Authentication Mode** in the main menu of the NE manager.
2. In the **Changing objects (ONU authentication way)** 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. The authentication modes are described in Table 6-1.

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.

Table 6-1 Description of the ONU Authentication Modes (Continued)

Authentication Mode	Description
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 write the configuration to device.

6.4.3 Managing PON Port Authentication Modes

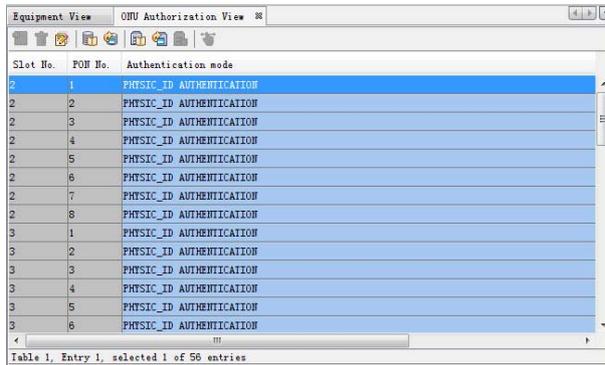
You can view and modify the authentication mode of each PON port. After the authentication mode of the PON port is set, the ONUs under this PON port will be authenticated adopting the set authentication mode.

Prerequisite

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

Procedure

1. Select **Configuration**→**ONU Authentication**→**PON Port Authentication Mode** in the main menu of the NE manager to open the **ONU Authorization View** tab, displaying the authentication modes of all PON ports.



- 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. The authentication modes are described in Table 6-2.

Table 6-2 Description of PON Port Authentication Modes

Authentication Mode	Description
Physical ID authentication	Authenticates based on the MAC address of the ONU.
Physical ID + password authentication	Authenticates based on the MAC address and password of the ONU.
Password authentication	Authenticates based on the password of the ONU.
Logical ID authentication (with password)	Authenticates based on the SN or password of the ONU.
Physical ID / Logical ID (with password) authentication	Authenticates based on the MAC address, SN or password of the ONU.
No authentication	No authentication is required for the ONU.
Logical ID authentication (without password)	Authenticates based on the SN of the ONU.
Physical ID / Logical ID (without password) authentication	Authenticates based on the MAC address or SN of the ONU.
Physical ID / Logical ID 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.	

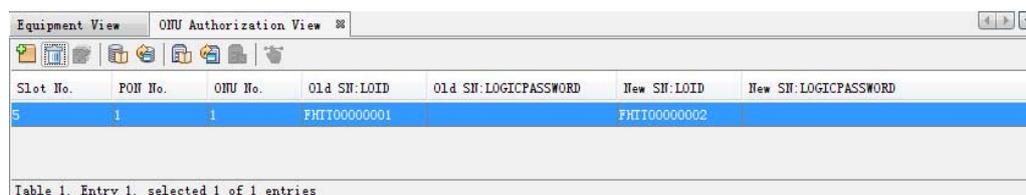
- Click  to write the configuration to device.

6.4.4 Replacing the ONU Logical Identifier

When an ONU adopting 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, without the need to configure the services.

Procedure

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



Slot No.	PON No.	ONU No.	Old SN:LOID	Old SN:LOGICPASSWORD	New SN:LOID	New SN:LOGICPASSWORD
5	1	1	FHT100000001		FHT100000002	

Table 1, Entry 1, selected 1 of 1 entries

6.4.5 Viewing the Authorized ONU Information

The user can view the authorized ONU information.

Procedures

1. Select **Configuration**→**ONU Authentication**→**Authorized ONU Information** in the main menu of the NE manager to open the **Switch Object (Authorized ONU Information)** tab.
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.

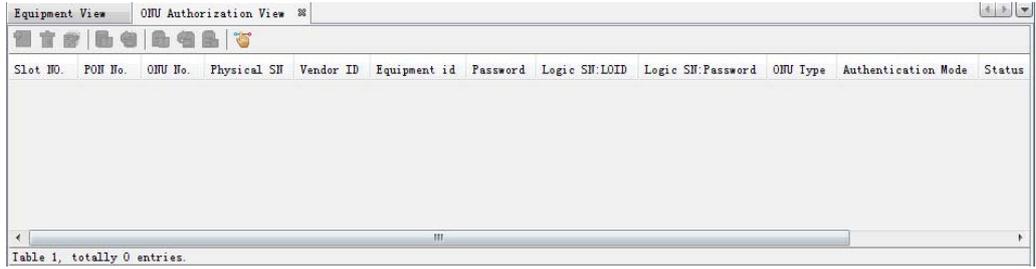


Table 6-3 ONU Authorization Status

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 Querying the ONU RMS Error Information

You can query and gather statistics of registration information of the ONUs to understand the running status of the ONUs.

Procedure

1. In the main topology, select **Resource**→**ONU RMS Error Information Query**.
2. In the **Query ONU RMS Error Information** dialog box, set the query conditions, query object and registration status.
3. Click **OK**. The **Query ONU RMS Error Information** window displays details of the ONUs matching the conditions.

6.5.2 Querying the ONU Network Access Interception Logs

By querying the interception records of ONU registration, you can understand whether there are multiple ONUs registering using a same MAC address. This provides the registration failure information for the maintainer to query.

Procedure

1. In the main topology, select **Resource**→**ONU Network Intercept Log Query**.
2. In the **ONU Network Intercept Log Query** dialog box, set the query conditions, query object and registration status.
3. Click **OK**. The **ONU Network Intercept Log Query** window displays the information of the ONUs matching the conditions.

6.6 Rule Tasks of Enabling the ONU Port

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 authorities of **Maintainer Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** 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 (basic information, object source and extension information) of the task.

6.6.2 Adding a Rule Task

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** 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 select **Create** to open the dialog.
3. Set the parameters in the **Basic information**, **Object information**, and **Object source** and **Extend information** tabs as required, and then click **OK**. The added task appears in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name:** of other tasks. This can improve the setting efficiency.

6.6.3 Executing Rule Tasks

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

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** 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 rule task, and select **Execute now**, 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

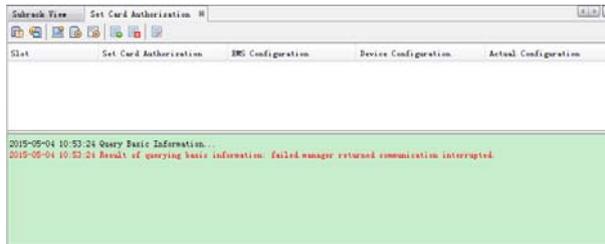
Right-click the executed rule task and select **View** from the shortcut menu. A pane appears in the lower part, displaying the execution object and status.

6.7 Authorizing Cards

You need to authorize the cards of the devices.

Procedures

1. In the main menu of the NE Manager GUI, select **Configuration**→**Set Card Authentication** to open the **Set Card Authentication** tab, displaying the current card authorization information.



2. Authorize the card according to the description of parameters in Table 6-4 and the description of operations in Table 6-5.

Table 6-4 Parameters

Parameter	Description
EMS Configuration	The card type configured in the network management GUI.
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
	Sets the EMS configuration as the card configuration.
	Sets the device configuration as the card configuration.
	Sets the actual configuration as the card configuration.
	Adds all cards.
	Deletes all cards.
	Hides empty slots.

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

6.8 Synchronizing ONUs Manually

The user can synchronize the ONU authorization information on the device to the network management system.

Prerequisite

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

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

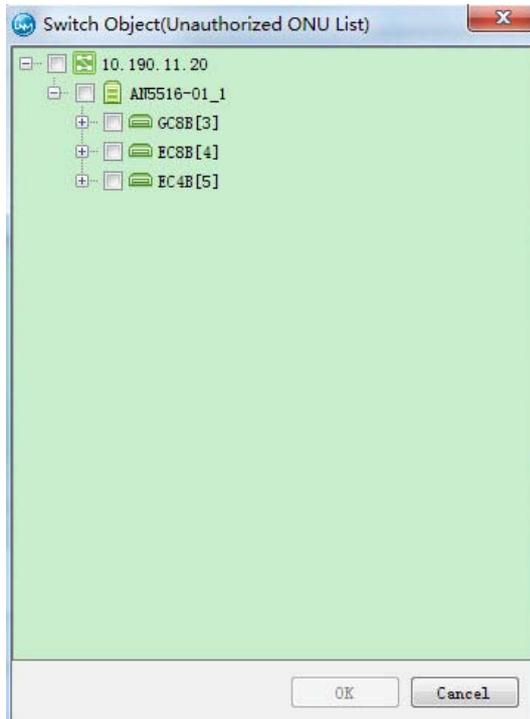
The user can obtain the authorized ONU information.

Prerequisite

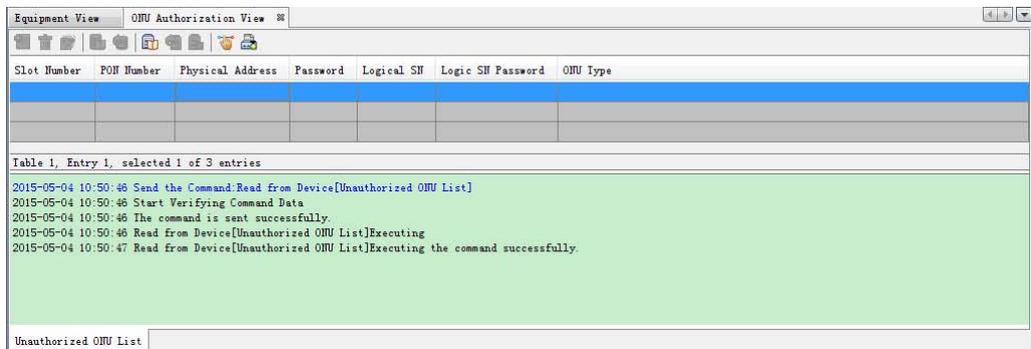
You have the authorities of **Maintainer Group** or higher authorities.

Procedure

1. In the main menu of the **NE Manager** GUI, select **Configuration**→**Obtain Unauthorized ONU** to open the **Switch Object (Unauthorized ONU List)** dialog box.



2. Select the desired PON port and click **OK**. The **ONU Authorization View** tab displays the information of unauthorized ONUs.



Subsequent Operation

- ◆ Click  to read the authorized ONU 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

The user can authorize the ONU manually.

Prerequisite

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

Procedure

1. In the main menu of the NE manager GUI, select **Configuration**→**Manual ONU Authorization** to open the **Manual ONU Authorization** dialog box.

2. Configure the basic information and authentication information, and click **Write Database** or **Write Equipment** according to Table 6-6 to authorize the ONU manually.

Table 6-6 Buttons

Button	Application
Write database	Applicable when the ONU is not physically connected. After the ONU is connected, the user can write the configuration in the database to the device via configuration synchronization operations.
Write device	Applicable when the ONU is physically connected.

6.11 Comparing and Synchronizing the ONU Manually

You can compare the ONU authorization information on the device and that in UNM2000. If they are inconsistent, you can synchronize the ONU authorization

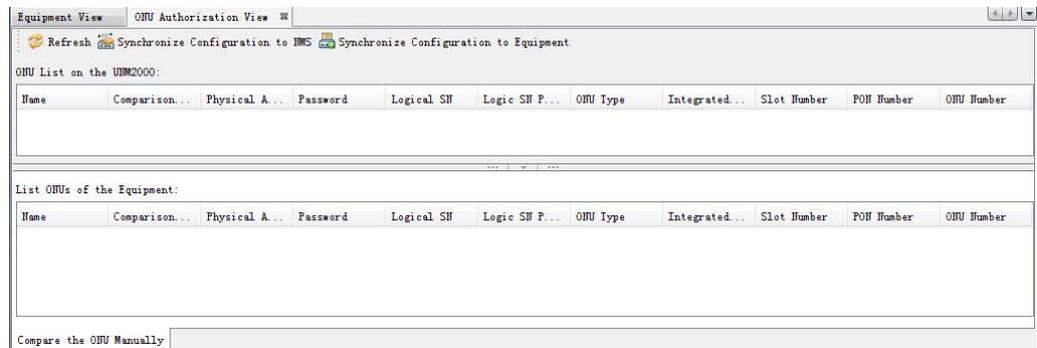
information on the device to the UNM2000 or synchronize that in the UNM2000 to the device.

Prerequisite

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

Procedure

1. In the main menu of the NE manager GUI, select **Configuration**→**Manually Compare and Synchronize ONU** to open the **Manually Compare and Synchronize ONU** tab, displaying the comparison result of the actual configuration on the device and the data in the UNM2000.



Subsequent Operation

When the ONU authorization information on the device is different from that on the network management system, the user can perform the following operations.

- ◆ Click **Synchronize configuration to NMS** and synchronize the ONU authorization information on the device to the network management system.
- ◆ Click **Synchronize configuration to device** and synchronize the ONU authorization information on the network management system to the device.
- ◆ Click **Refresh** to refresh the ONU authorization information.

6.12 Querying the Card Software / Hardware Versions

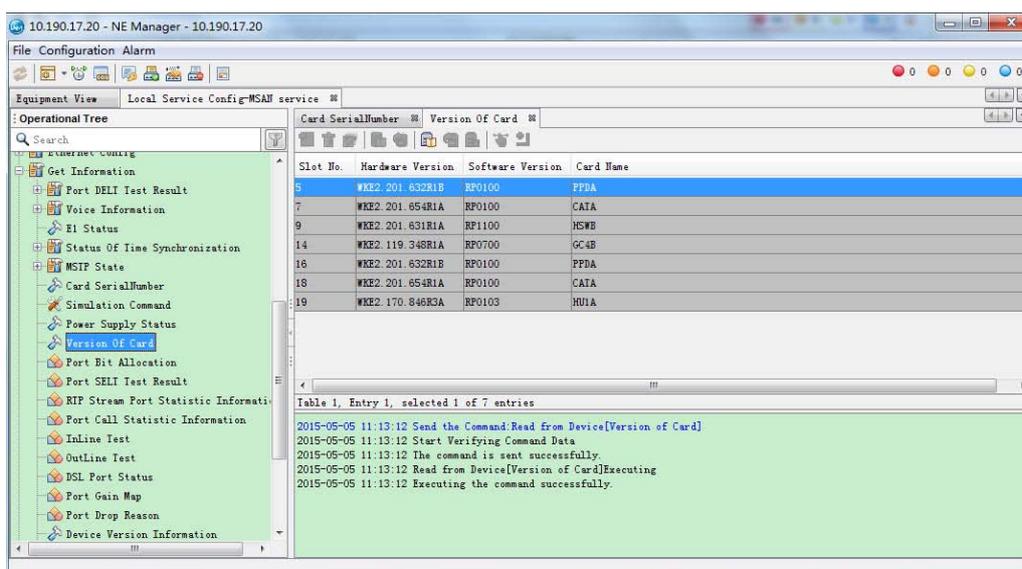
Before upgrading / degrading the device, you can query the card software / hardware version to get the version information of the current device card.

Prerequisite

- ◆ You have the authorities of **Operator Group** or higher authorities.
- ◆ The communication between the UNM2000 and the device where the desired card locates is normal.

Procedure

1. Right-click the object in the object tree of the main topology and select **Open NE Manager** from the shortcut menu to open the **NE Manager** GUI.
2. In the device subrack view of the NE manager, right-click the desired card and select **Card Service Config** to open the **Card Service Config** dialog box.
3. Select **Get Information** → **Version Of Card** to open the **Version Of Card** dialog box, displaying the software / hardware version of the card.



6.13 Upgrading the Card

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 Tasks of Upgrading the System Software

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.

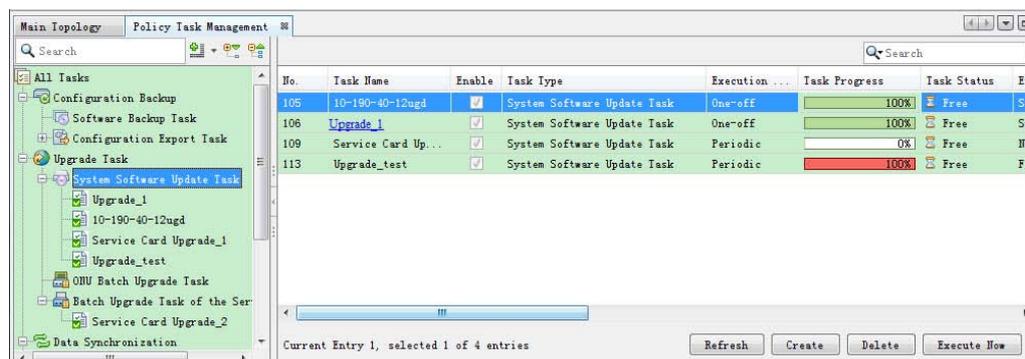
6.13.1.1 Viewing Upgrade Tasks

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**System Software Upgrade Task** in the left pane to view the current system software 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 (basic information, object source and extension information) of the task.

6.13.1.2 Adding an Upgrade Task

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** 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** from the shortcut menu to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required, and click **OK** after completing the settings. The added task appears in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name**: of other tasks. This can improve the setting efficiency.

Other Operations

When the system software upgrade tasks do not meet the upgrade requirements or will expire, you can right-click the task to **Delete / Disable** the task or view / modify its **Attribute**.

6.13.1.3 Executing an Upgrade Task

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**System Software Upgrade Task** in the left pane to view the current system software upgrade tasks.
3. Right-click the task meeting the requirement for system software upgrade, and select **Execute Now**, or click the task and then click the **Execute Now** button at the bottom of the tab to execute the system software upgrade task.

Other Operations

Right-click the executed system software upgrade task and select **View** from the shortcut menu. The execution object and status of the task appear in the lower part of the 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.

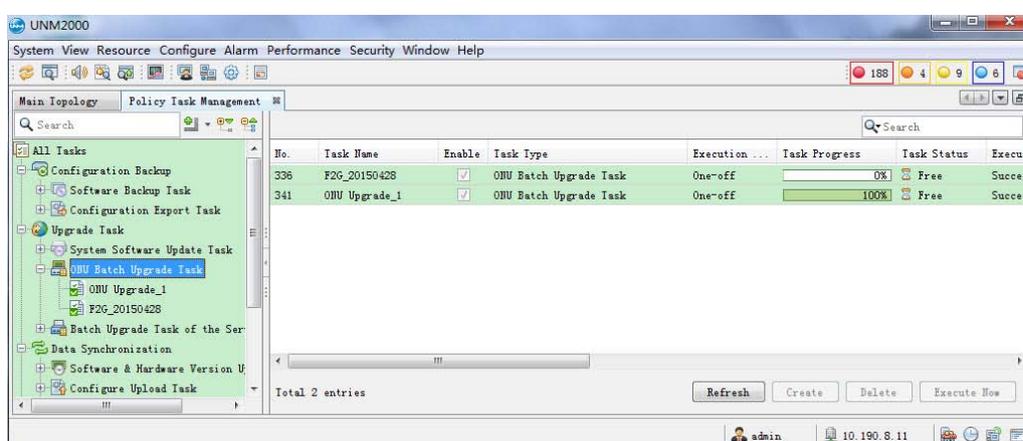
6.13.2.1 Viewing Upgrade Tasks

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**ONU Batch Upgrade Task** in the left pane to view the current tasks of upgrading ONUs in a batch manner.



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 (basic information, object source and extension information) of the task.

6.13.2.2 Adding an Upgrade Task

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** 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** from the shortcut menu to open the dialog box.
3. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required, and click **OK** after completing the settings. The added task appears in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name**: of other tasks. This can improve the setting efficiency.

Other Operations

When the ONU software upgrade tasks do not meet the upgrade requirements or will expire, you can right-click the task to **Delete** / **Disable** the task or view / modify its **Attribute**.

6.13.2.3 Executing an Upgrade Task

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**ONU Batch Upgrade Task** in the left pane to view the current tasks of upgrading ONUs in a batch manner.

- Right-click the task meeting the requirement for batch upgrade of ONUs, and select **Execute Now**, or click the task and then click the **Execute Now** button at the bottom of the tab to execute the batch upgrade of ONUs.

Other Operations

Right-click the batch upgrade task of ONUs and select **View** from the shortcut menu. The execution object and status of the task appear in the lower part of the pane.

6.13.3 Batch Upgrade Task of Service Cards

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

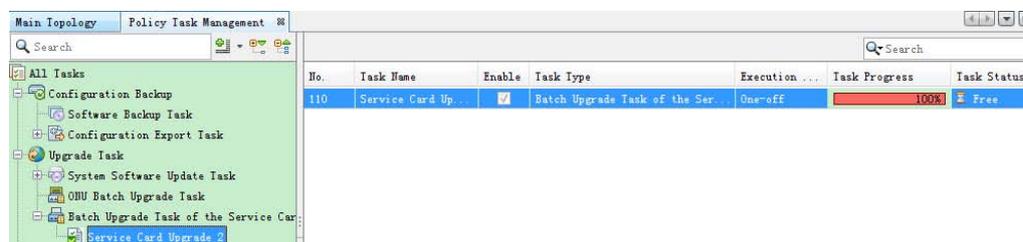
6.13.3.1 Managing the Task of Upgrading the Service Card in a Batch Manner

Prerequisite

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

Procedure

- In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
- Select **Upgrade Task**→**Batch Upgrade Task of the Service Card** in the left pane to view the current tasks of upgrading the service cards in a batch manner.



- 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 (basic information, object source and extension information) of the task.

6.13.3.2 Adding an Upgrade Task

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. Right-click **Batch Upgrade Task of the Service Card** in the left pane or right-click in 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 as required, and click **OK** after completing the settings. The added task appears in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name**: of other tasks. This can improve the setting efficiency.

Other Operations

When the service upgrade tasks do not meet the upgrade requirements or will expire, you can right-click the task to **Delete** / **Disable** the task or view / modify its **Attribute**.

6.13.3.3 Executing an Upgrade Task

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. Select **Upgrade Task**→**Batch Upgrade Task of the Service Card** in the left pane to view the current tasks of upgrading the service cards in a batch manner.
3. Right-click the task meeting the requirement for batch upgrade of service cards, and select **Execute Now**, or click the task and then click the **Execute Now** button at the bottom of the tab to execute the system software upgrade task.

Other Operations

Right-click the batch upgrade task of service cards and select **View** from the shortcut menu. The execution object and status of the task appear in the lower part of the pane.

6.14 Managing the Test Task

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 authorities of **Operator Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** 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 (basic information, object source and extension information) of the task.

6.14.1.2 Adding a Test Task

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** 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** after completing the settings. The added task appears in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name**: of other tasks. This can improve 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 **Delete** / **Disable** the task or view / modify its **Attribute**.

6.14.1.3 Executing a Test Task

Prerequisite

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



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. In the main menu, select **System**→**Policy Task Management** 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 the executed test task and select **View** from the shortcut menu. A pane appears in the lower part, displaying the execution object and status.

6.14.2 Managing the Task of VoIP Pinging Test

The VoIP PING test 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 authorities of **Operator Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. Select **test task**→**VOIP PING Task** in the left pane to view the current VoIP pinging 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 (basic information, object source and extension information) of the task.

6.14.2.2 Creating a Task

The VoIP pinging 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. In the main menu, select **System**→**Policy Task Management** 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; for **Parameter Settings** items in the **Extend information** tab, see Table 6-7. After completing the settings, click **OK**. The task appears in the task list.

Table 6-7 Description on the VoIP Pinging Parameters

Parameter	Description
-n	Sends the ECHO data packets with the number assigned by the transmission 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	Resolves the address into the NetBios name of the computer
-f	If the Not-Section flag is transmitted in a packet, this packet will not be sectioned by the gateways at the route
-i	Sets TTL to the given value
-k	Uses the computer list assigned by the computer-list to list the route packet



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name:** of other tasks. This can improve the setting efficiency.

Other Operations

When the VOIP PING test tasks do not meet the upgrade requirements or will expire, you can right-click the task to **Delete** / **Disable** the task or view / modify its **Attribute**.

6.14.2.3 Executing a Task

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. Select **test task**→**VOIP PING Task** in the left pane to view the current VoIP pinging tasks.
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 VOIP PING test task.

Other Operations

Right-click the executed test task and select **View** from the shortcut menu. A pane appears in the lower part, displaying the execution object and status.

6.15 Managing ONU MGC Query Tasks

The user can obtain the ONU MGC service configuration from the device and save to database via the ONU MGC query task.

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. In the left pane, select **Data Synchronization**→**ONU MGC Query** to view the existing ONU MGC query task.
3. Right-click a task and select **Execute Now**, or click the task and click **Execute now** at the lower right corner of the tab to execute the ONU MGC query task.
4. Click a certain task in the left pane to view its object information, status, or failure cause.

Other Operations

Right-click an ONU MGC query task to disable the task, and view / modify the task attributes.

6.16 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.

6.16.1 Viewing NE Automatic Discovery Tasks

You can set the NE automatic discovery task to automatically discover the NEs in the specified IP segment.

Prerequisite

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

Procedure

1. Select **Resource**→**Auto Detect NE Task** or select **System**→**Policy Task Management**→**Data Synchronization**→**Auto Detect NE Task** to view the existing NE automatic discovery tasks.

No.	Task Name	Enable	Task Type	Execution ...	Task Progress	Task Status	Execution ...	Start Time of the Task
337	test	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05
338	111111111111	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05
339	moli	<input checked="" type="checkbox"/>	Auto Detect NE Task	Periodic	100%	Free	Succeeded	2015-04-29 10:01:05

Current Entry 1, selected 1 of 3 entries

Refresh Create Delete Execute Now

2. Right-click a task entry and select **Attribute** from the shortcut menu to view the details of the task (such as execution period, execution time and IP address).

Subsequent Operation

- ◆ Right-click the task, and select **Execute Now**, or click the task, and then click the **Execute Now** button at the bottom of the tab to execute the NE automatic discovery task.
- ◆ Select the NE automatically discovered and click **Create Selected NE** or **Create All** to automatically save the NE data in the UNM2000.

6.16.2 Adding 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 authorities of **Operator Group** or higher authorities.

Procedure

1. In the main menu, select **Resource**→**Auto NE Discovery** 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 related parameters in the **Basic information** and **Extend information** tabs, and click **OK** after completing the settings. Then the added tasks will be displayed in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name** of other tasks. This can improve 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. Users should 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 the Alarm Information
- Remote Alarm / Event Notification
- Managing Alarm / Event Data
- Alarm Logs
- Managing Alarm Frequency Analysis Rules

7.1 Basic Concepts

The following 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 service, as well as synchronizing, verifying and confirming the alarms.

- ◆ Alarm browsing: You can browse the alarms of the devices or service 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 alarm logs: By browsing the alarm history recorded in the UNM2000, you can get the information of alarms that occurred in the UNM2000 for long-term performance analysis.
- ◆ Confirming alarms: If an alarm is confirmed, the alarm is processed. There are two ways to confirm alarms: manual confirmation and automatic confirmation.
 - ▶ 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.
- ◆ 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. There are two ways of alarm synchronization: manual synchronization and automatic synchronization.

- ▶ Manual confirmation: You can select the NE alarms and synchronize them in current alarm window.
- ▶ Automatic synchronization: You can specify the automatic synchronization conditions to have the alarms synchronized automatically.
- ◆ 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 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 and minor alarms in yellow. You can customize the colors of the alarm indicator to indicate alarms of different levels.
- ◆ Alarm sound: The UNM2000 provides the audible and visual alarm when 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 prompt 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.
Prompt 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

When the alarm history saved in the UNM2000 exceeds a certain limit, it will influence the operations performed in the UNM2000. The alarm saving function can be used to remove the alarm history data from the database to a specified file, which improves the running performance of the UNM2000. The UNM2000 supports manual save and overflow save of alarms.

- ◆ **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 to a specified file folder manually at anytime. You can set the saving period of alarm history data. 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

View whether the existing alarm reporting rules meet the requirements for current network maintenance.

Prerequisite

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

Procedure

1. In the main menu, select **Alarm**→**Alarm Reporting Settings** to open the **Alarm Report Settings** tab.
2. Select **Report rule** in the left pane, and view the current 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 authorities of **Operator Group** or higher authorities.
- ◆ The desired alarm reporting rule has been planned according to the maintenance requirement.

Procedure

1. In the main menu, select **Alarm**→**Alarm Reporting Settings** to open the **Alarm Report Settings** 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. After completing the settings, 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 Viewing Alarm Filter Rules

View whether the existing alarm filter rules meet the maintenance requirements of the UNM2000 and the NE.

Prerequisite

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

Procedure

1. In the main menu, select **Alarm**→**Alarm Shield Rule Management** to open the **Alarm Shield Rule Management** tab.
2. Select **Current Alarm Shield Rule** in the left pane, and view the current alarm filter 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.

7.2.2.2 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 authorities of **Operator Group** or higher authorities.
- ◆ The desired alarm filter rule has been planned according to the maintenance requirement.

Procedure

1. In the main menu, select **Alarm**→**Alarm Shield Rule Management** 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. After completing the settings, 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.

7.2.2.3 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** → **Shield Rule of North** from the main menu to open the **Filter Rule of North** tab.
2. Click **Create Rule**.
3. In the displayed **Filter Rule of North** 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 **Filter Rule of North** tab.

Other Operations

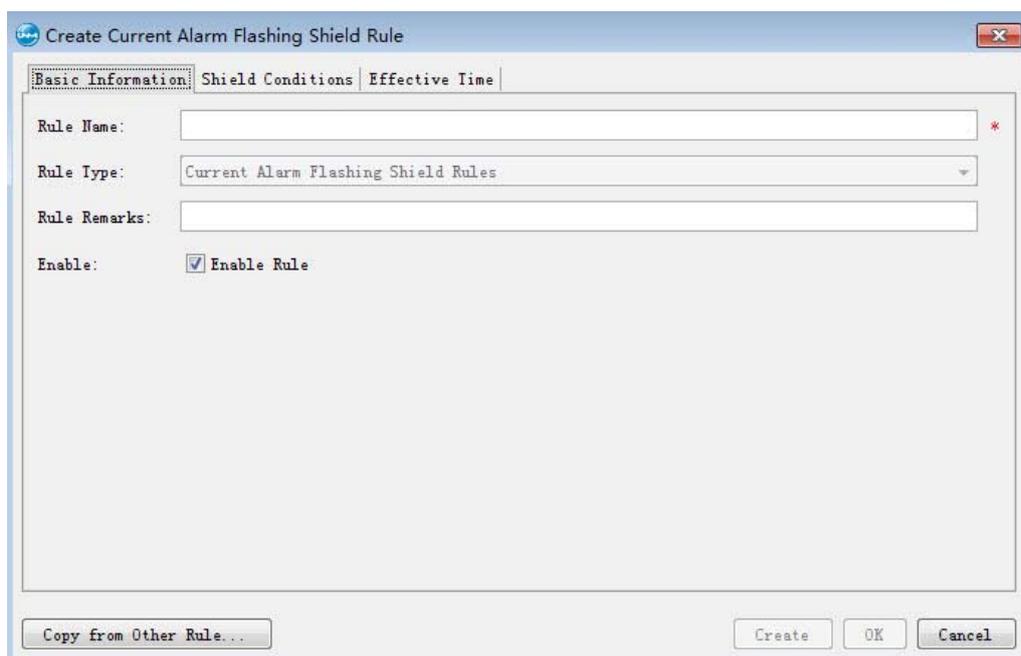
In the **Filter Rule of North** tab, right-click a northbound interface alarm rule and select the menus from the shortcut menu to perform the corresponding operations, including **Modify Rule**, **Delete Rule**, **Disable Rule**, **Copy Rule**, etc.

7.2.2.4 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. In the main menu, select **Alarm**→**Alarm Flashing Shield Rule Management** to open the **Alarm Flashing Shield Management** tab.
2. Click **Alarm Flashing Shield Management** in the left pane.
3. Click **Create** to create a rule.
4. In the displayed **Create Current Alarm Flashing Shield Rule** dialog box, set the filter rule as required.



5. Click **OK** to add an alarm filter rule and filter the current alarm in specific condition. The newly added alarm northbound interface file rules can be viewed in the **Alarm Flashing Shield Management** tab.

Other Operations

In the **Alarm Flashing Shield Management** tab, right-click a file rule and select the shortcut menus to perform the corresponding operations, such as **Delete** and **Copy**.

7.2.3 Setting the Audible Alarms

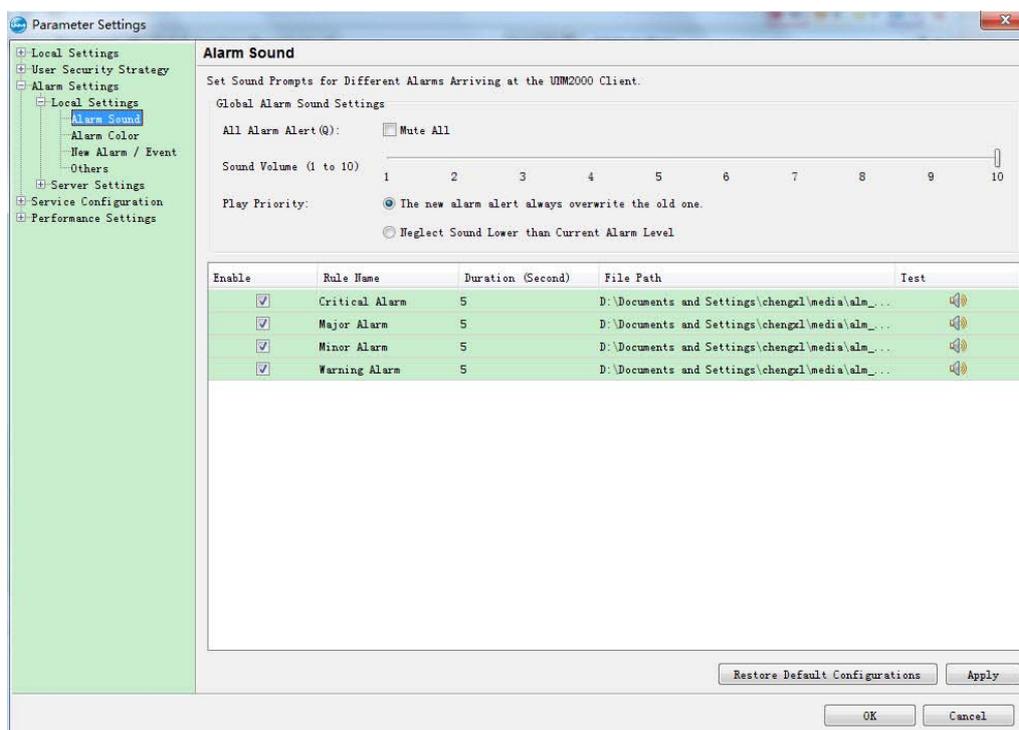
You can set different sounds for alarms of different levels and set the play priority of the alarm sounds. When an alarm occurs, the loudspeaker on the computer running the client will play the corresponding sound to notify of the reported alarm of the specific level.

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 and click **Apply** to apply the settings.

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

Users 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 as required. Then click **Apply** and the settings will be valid.

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: ■.
- ◆ The alarm color settings are applicable for all users at any client.

Procedure

1. Select **System**→**Parameter Settings**→**Alarm Settings**→**Local Alarm**→**Alarm Color** to open the **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 Settings**→**Others** in the left pane to open the dialog box.
3. Set the parameters and click **Apply** to apply the settings.
4. In the main menu, select **Alarm**→**Alarm Query Template** to view the parameter values already set.

Other Operations

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

7.2.8 Setting the Alarm Automatic Synchronization Policy

The alarm automatic synchronization policy includes two types: automatically synchronizing all alarms when the network management services are enabled, and

automatically synchronizing equipment alarms after the communication resumes from the interruption status. When the alarm automatic synchronization is set, the alarms will be automatically synchronized after the UNM2000 recovers from the communication interruption with the NE or restarts so as to ensure the consistency of the alarms in the UNM2000 and at the NE side.

Procedure

1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Alarm Settings**→**Server Settings**→**Automatic Synchronization** in the left pane to open the dialog box.
3. Set the alarm automatic synchronization policies and then click **Apply** to apply the settings.

7.2.9 Setting the Definition of the Alarm History

Users 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

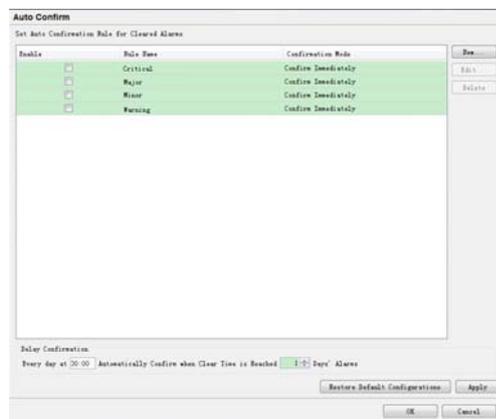
1. Select **System**→**Parameter Settings** in the main menu to open the **Parameter Settings** dialog box.
2. Select **Alarm Settings**→**Server Settings**→**Alarm History Definition** in the left pane to open the dialog box.
3. Set the delay for switching current alarms to the alarm history and then click **Apply** to apply the settings.

7.2.10 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.

7.2.11 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**→**Event to Alarm Settings** from the UNM2000 main menu.
2. In the **Event to Alarm Settings** tab, select the desired event entries, as shown below:

Select	No.	Name	Level
<input type="checkbox"/>	900	ONU_Register	Warning
<input type="checkbox"/>	901	OLT_Register	Warning
<input type="checkbox"/>	902	HG_REGISTER	Warning
<input type="checkbox"/>	903	Onu_Replace_event	Warning
<input type="checkbox"/>	904	ONU_REPLACE_REQUESTI	Warning
<input type="checkbox"/>	905	PULL_OUT_CARD	Critical
<input type="checkbox"/>	906	INSERT_CARD	Critical
<input type="checkbox"/>	907	CPU_SWITCH_SUCCESS	Warning
<input type="checkbox"/>	908	SLOT_INITSUCCESS_TRAP	Warning
<input type="checkbox"/>	909	PEER_INSERT	Warning
<input type="checkbox"/>	910	UPGRADE_FAILURE	Critical
<input type="checkbox"/>	911	UPGRADE_FILE_MISMATCH	Critical
<input type="checkbox"/>	912	AUTO_UPGRADE_SUCCESS	Warning
<input type="checkbox"/>	913	AUTO_UPGRADE_FAILURE	Critical
<input type="checkbox"/>	914	PHYSICALID_REPLACE_SUCCESSFUL	Warning

Select All / Clear None
 Select All/Clear the Selected Rows

3. Click **Save**.

7.2.12 Customizing Alarms

7.2.12.1 Viewing Custom Special Alarms

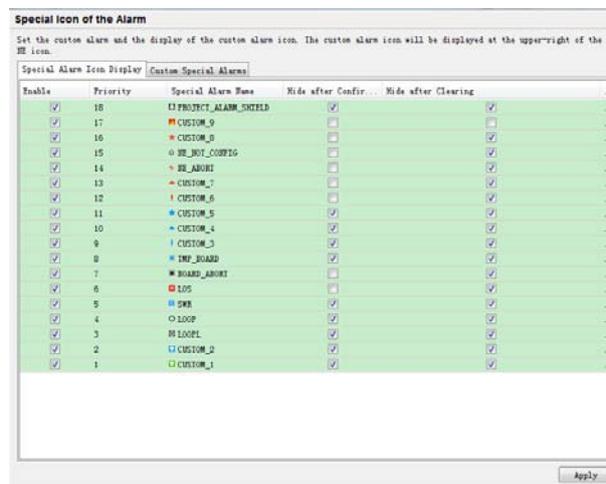
The following introduces the types of special alarms already defined.

Prerequisite

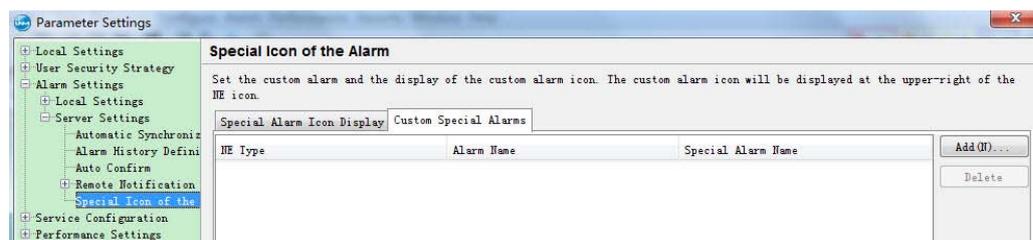
You have the authorities of **Operator Group** or higher authorities.

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. Select the **Customized special alarm** tab to view the special alarms already defined.



7.2.12.2 Customizing Special Alarms

Prerequisite

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

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 customized special alarms, and click **Delete** to delete them.

7.2.12.3 Setting the Special Alarm Icons

Background Information

By setting the special alarm icons, users can achieve the following functions: When the corresponding alarm occurs at the NE, the special icon of this alarm will be displayed at the right-upper corner of the NE, so as to make the related staff 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 17, with 17 being the highest.

Prerequisite

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

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 Icon of the Alarm** tab, 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:

- ◆ Alarm log statistical template
- ◆ Current alarm query template
- ◆ Alarm history query template
- ◆ Alarm log query 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 authorities of **Operator Group** or higher authorities.

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 Adding 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 authorities of **Operator Group** or higher authorities.

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.

3. 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.

4. After completing the settings, 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 (K)** and **Export**.

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:**

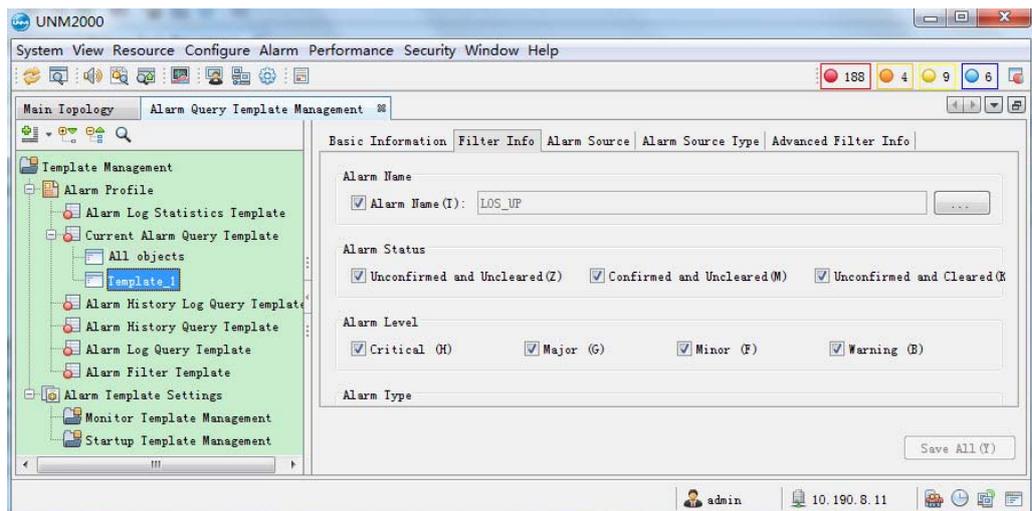
The following uses the current alarm query template as an example. You can follow the same procedures to modify other templates with the only difference in the access method.

Prerequisite

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

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 **Save All**.



7.3.1.4 Setting the Template Attributes

At the UNM2000 client, you can set the alarm template as a monitoring template, startup template and default template to facilitate monitoring, querying or gathering statistics of alarms.

Background Information

- ◆ Default profile: When users query or count the alarms via the menu, the UNM2000 will use this profile to open the tab of the corresponding functions. Users can only set one default profile in one type of alarm profiles.
- ◆ Monitoring profile: The **Alarm Statistics** dialog box in the toolbar of the UNM2000 client end will display the alarm statistics data according to this profile. The monitoring profile must be a current alarm profile, and users can set five monitoring profiles at most.



Note:

After users set the monitoring profile to the current profile in the **Alarm Statistics** dialog box, the indicators (with four colors) in the toolbar will display the statistics data of alarms with various levels according to the current profile.

- ◆ Starting profile: After logging in the UNM2000 client end successfully, the system will access the alarm query or statistics GUI automatically according to this profile. Users can set five starting profiles at most.

Prerequisite

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

Procedure

1. In the main menu, select **Alarm**→**Alarm Query Template** to open the **Alarm Query Template Management** tab.
2. Set the alarm template attributes, 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 the 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

You can save the frequently used event query conditions as a template so that you can use the template for quick query in the future.

Procedure

1. In the main menu, select **Alarm**→**Event Query Template** to access the **Event Query Template** tab.
2. Click **Event Report Query Template** in the left pane and 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 Adding an Event Template

You can save the frequently used event query conditions as a template so that you can use the template for quick query in the future.

Prerequisite

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

Procedure

1. In the main menu, select **Alarm**→**Event Query Template** to access 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 the **Copy from the Template** button, and users can copy all settings except for the **Template Name** of other profiles. 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 (K)**, 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 settings in case the query condition setting error occurs.

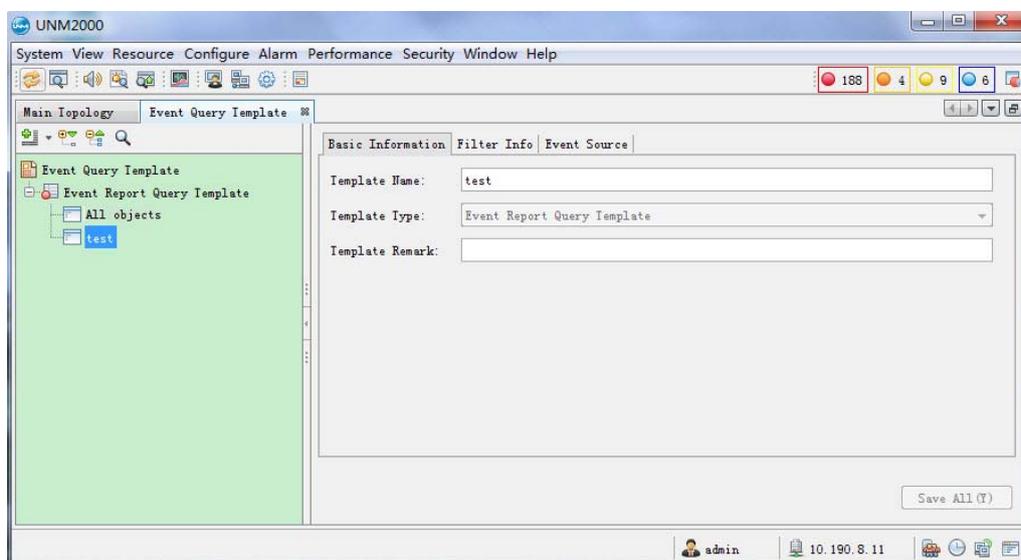
Prerequisite

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

Procedure

1. In the main menu, select **Alarm**→**Event Query Template** to access the **Event Query Template** tab.
2. Click **Event Report Query Template** in the left pane and view the existing event query templates.
3. Click the desired event reporting query template to view the details of the template.

4. Modify the relevant information of the event reporting query template in the right pane as needed 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 automatic and 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 NE in the main topology and select **Open NE Manager** from the shortcut menu to open 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.

7.4.2 Synchronizing Alarms Automatically

When the alarm automatic synchronization is set, the alarms will be automatically synchronized after the UNM2000 recovers from the communication interruption with the NE or restarts so as to ensure the consistency of the alarms at the UNM2000 side and at the NE side.

Prerequisite

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

Procedure

1. Set the UNM2000 to automatically synchronize all alarms and the device alarms after the recovery of the communication interruption upon startup of the UNM2000 services. See [Setting the Alarm Automatic Synchronization Policy](#).

7.5 Monitoring Network Alarms

By monitoring the network alarms, the user can know the operating status of the network in a timely manner.

Based on the alarms status, the UNM2000 divides the alarms into current alarms and alarm history.

- ◆ **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. To query each alarm record, you can check the alarm logs.

- ◆ Alarm history: The removed current alarms are added into the alarm history after the preset delay time has expired.

The alarm history will be transferred to 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

Users 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 described in Table 7-2 to open the **Query Current Alarm** dialog box.

Table 7-2 Access Method of 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.
	Select Alarm → Current Alarm from the main menu of the NE manager window.
	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 Status	Clear Status	Alarm Source	Location Information
294237		Critical	CARD_NOT_PRESENT	Unconfirmed	Not Cleared	10.190.5.125	10.190.5.125:(15)EC88[15]
294319		Critical	MCOMFAIL	Unconfirmed	Not Cleared	test	test
294569		Warning	ILLEGAL_OIU/BIU_REGISIE	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(3)GC8B[3]:POH[S]-AHS
294570		Critical	CARD_NOT_PRESENT	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(5)EC4B[5]
294572		Major	CONFIG_HAVENOT_SAVED	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(9)HSWA[9]
294573		Minor	DOWN_BIPS_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(3)GC8B[3]:POH[S]-AHS
294574		Minor	DOWN_BIPS_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(3)GC8B[3]:POH[S]-AHS
294575		Minor	UP_BIPS_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(3)GC8B[3]:POH[S]-AHS
294576		Minor	DOWN_BIPS_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(3)GC8B[3]:POH[S]-HG2
294577		Minor	DOWN_BIPS_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(3)GC8B[3]:POH[S]-AHS
294578		Minor	DOWN_BIPS_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(3)GC8B[3]:POH[S]-HG2
294588		Minor	DOWN_BIPS_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20:(3)GC8B[3]:POH[S]-AHS
294589		Critical	MCOMFAIL	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20

Current Entry 1, selected 1 of 56 entries

Query by Template... Query... Confirm Alarm Clear Alarm View Details (C)

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 tab to perform the corresponding operations.
 - ▶ Select an alarm and click **View Details** to view the detailed information 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 mentioned in Table 7-3 to open the **Alarm History Query** dialog box.

Table 7-3 Access Method of Viewing the Alarm History

Operation	Access Method
Viewing Alarm History	Select Alarm → Alarm History from the main menu.
	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.
	In the Diagram pane of the NE manager window, right-click the corresponding card and select Alarm History from the shortcut 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**. The **Alarm History Query** 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 **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 Status	Clear Status	Alarm Source	Location Information	Port Number	Occur
290779		Critical	LINK_LOSS	Auto Confirmation	JMS Clear...	10.190.5.125	10.190.5.125: (7)EC4B[7]: PON4	4	2015-
290780		Critical	OPTMODULE_NOT_PRESENT	Auto Confirmation	JMS Clear...	10.190.5.125	10.190.5.125: (7)EC4B[7]: PON4	4	2015-
293719		Major	CONFIG_HAVERNOT_SAVED	Auto Confirmation	JMS Clear...	10.190.11.20	10.190.11.20: (9)HWA[9]	0	2015-
293720		Minor	DOWN_BIP8_OVER_THRESH_A...	Auto Confirmation	JMS Clear...	10.190.11.20	10.190.11.20: (3)GC8B[3]: PON[S]-AMS506-01-A1[12]: (12)	0	2015-
293735		Warning	ILLEGAL_OIU/BIU_REGISTE...	Auto Confirmation	JMS Clear...	10.190.11.20	10.190.11.20: (3)GC8B[3]: PON[S]	5	2015-
293736		Warning	RDI	Auto Confirmation	JMS Clear...	10.190.11.20	10.190.11.20: (3)GC8B[3]: PON[S]-AMS506-01-A1[12]: (12)	0	2015-
293737		Warning	RDI	Auto Confirmation	JMS Clear...	10.190.11.20	10.190.11.20: (3)GC8B[3]: PON[S]-HG280[17]: (17)	0	2015-
293738		Minor	UP_BIP8_OVER_THRESH_ALAR...	Auto Confirmation	JMS Clear...	10.190.11.20	10.190.11.20: (3)GC8B[3]: PON[S]-AMS506-01-A1[6]: (6)	0	2015-
293739		Minor	DOWN_BIP8_OVER_THRESH_A...	Auto Confirmation	JMS Clear...	10.190.11.20	10.190.11.20: (3)GC8B[3]: PON[S]-AMS506-01-A1[12]: (12)	0	2015-
293745		Minor	DOWN_BIP8_OVER_THRESH_A...	Auto Confirmation	JMS Clear...	10.190.11.20	10.190.11.20: (3)GC8B[3]: PON[S]-AMS506-01-A1[12]: (12)	0	2015-
294028		Critical	MCOMFAIL	Auto Confirmation	JMS Clear...	10.190.11.20	10.190.11.20	0	2015-
294055		Critical	NO_OPTICS_SIGNAL	Auto Confirmation	JMS Clear...	10.190.5.125	10.190.5.125: (19)H1A[19]: SFP2	3	2015-
294056		Critical	NO_OPTICS_SIGNAL	Auto Confirmation	JMS Clear...	10.190.5.125	10.190.5.125: (19)H1A[19]: SFP1	2	2015-
294099		Critical	NO_OPTICS_SIGNAL	Auto Confirmation	JMS Clear...	10.190.5.125	10.190.5.125: (19)H1A[19]: SFP4	5	2015-
294101		Critical	DYING_GASP	Auto Confirmation	JMS Clear...	10.190.5.125	10.190.5.125: (14)GC4B[14]: PON[2]-AMS506-04-F1[20]:...	0	2015-
294102		Critical	DYING_GASP	Auto Confirmation	JMS Clear...	10.190.5.125	10.190.5.125: (14)GC4B[14]: PON[3]-AMS506-04-F1[11]: (1)	0	2015-
294103		Critical	DYING_GASP	Auto Confirmation	JMS Clear...	10.190.5.125	10.190.5.125: (14)GC4B[14]: PON[4]-AMS506-04-F1[14]:...	0	2015-

Total 300 entries

Buttons: Refresh, Query by Template..., Query..., View Details(C)

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

Viewing NE-related alarms can help understand the NE operation in details.

Procedures

1. See [Viewing Current Alarms](#) or [Viewing Alarm History](#) for opening the **Current Alarm** or **Alarm History** tab.
2. Right-click the corresponding alarm and select **View current alarm of the relevant NE / View NE history alarm** to view the current alarms or the alarm history of the selected NE.

7.5.4 Viewing Alarm Details

By viewing the detailed alarm information, the user can obtain the alarm name, alarm cause, recovery advice, isolation information, etc.

Procedures

1. Open the **Current Alarm** or **Alarm History** tab. See **Viewing Current Alarms** or [Viewing Alarm History](#).
2. Select an alarm and click the **View Details** at the lower right corner of the tab to view the detailed information of the corresponding alarm.

Basic information		Service information		Maintenance information	
Alarm Layer:	Normal	Level:	Critical	Name:	MCOMFAIL (MCOMFAIL)
Alarm source:	test	Location information:	test	Frequency:	1
First create time:	2014-03-17 09:19:23	Latest occurrence time:	2014-03-17 09:19:23	(reverse) confirm time:	
(reverse) operator confirmation:		Clear time:		Clear operator:	
Confirm the status:	Unconfirmed	Clear the status:	Uncleared	Alarm type:	Equipment alarm
NE Type:	AN5006-30	Key information:			

Row2, select 1, 123 in total

Query by the Template Query Confirm alarms Clear alarm View Details(T)<<

3. 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.

Alarm Details

```

Number:25886
Level:Critical
Name:MCOMFAIL (MCOMFAIL)
Alarm source:test
Location information:test
Frequency:1
First create time:2014-03-17 09:19:23
Latest occurrence time:2014-03-17 09:19:23
(reverse) confirm time:
(reverse) operator confirmation:
Clear time:
Clear operator:
Confirm the status:Unconfirmed
Clear the status:Uncleared
Key information:
Appendix information:
Remark:
NE Type:AN5006-30

```

Copy Previous Next item Close

Subsequent Operation

You can handle the alarms according to the suggestion in the **Maintenance Information** tab.

7.5.5 Viewing Alarm Logs

Users 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 [Adding 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 Status	Clear Status	Alarm Source	Location Information
294569		Warning	ILLEGAL_OIU/BIU_REGISIE	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M5
294570		Critical	CARD_NOT_PRESENT	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (5)EC4E[5]
294572		Major	CONFIG_HAVENTOT_SAVED	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (9)H5WA[9]
294573		Minor	DOWM_EIPIB_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M[5]-AHS506-01-A1[12]: (
294574		Minor	DOWM_EIPIB_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M[5]-AHS506-01-A1[2]: (2
294575		Minor	UP_EIPIB_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M[5]-AHS506-01-A1[6]: (6
294576		Minor	DOWM_EIPIB_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M[5]-H6280[17]: (17)
294577		Minor	DOWM_EIPIB_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M[5]-AHS506-01-A1[3]: (3
294578		Minor	DOWM_EIPIB_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M[5]-H6280[24]: (24)
294579		Minor	DOWM_EIPIB_OVER_THRESH_ALARM	Unconfirmed	Equipment Clear...	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M[5]-AHS506-01-A1[5]: (5
294585		Minor	DOWM_EIPIB_OVER_THRESH_ALARM	Unconfirmed	Equipment Clear...	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M[5]-AHS506-01-A1[5]: (5
294587		Critical	MCOMFAIL	Unconfirmed	NMS Clearance	10.190.11.20	10.190.11.20
294588		Minor	DOWM_EIPIB_OVER_THRESH_ALARM	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20: (3)GC8B[3]: P0M[5]-AHS506-01-A1[5]: (5
294589		Critical	MCOMFAIL	Unconfirmed	Not Cleared	10.190.11.20	10.190.11.20
293719		Major	CONFIG_HAVENTOT_SAVED	Auto Confirmation	NMS Clearance	10.190.11.20	[HISTORY]10.190.11.20: (9)H5WA[9]
293720		Minor	DOWM_EIPIB_OVER_THRESH_ALARM	Auto Confirmation	NMS Clearance	10.190.11.20	[HISTORY]10.190.11.20: (3)GC8B[3]: P0M[5]-AHS506-01
293735		Warning	ILLEGAL_OIU/BIU_REGISIE	Auto Confirmation	NMS Clearance	10.190.11.20	[HISTORY]10.190.11.20: (3)GC8B[3]: P0M5

Total 411 entries

Refresh Query by Template... Query... Confirm Alarm Clear Alarm View Details(C)



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 detailed information of the selected alarm. For details, 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 Statistical Data of the Alarm Logs

Users can set the statistics conditions for the statistics of alarm logs.

Procedure

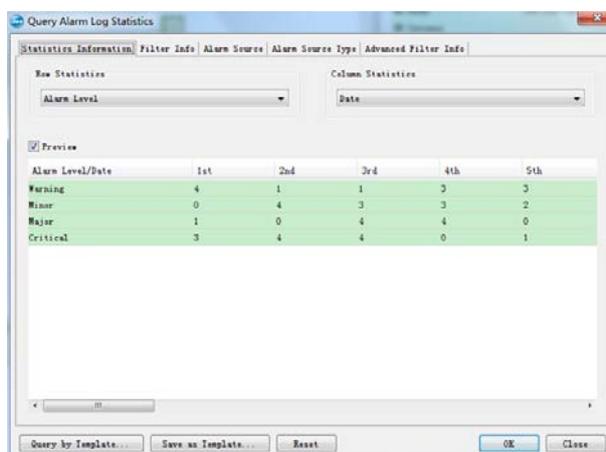
1. Select **Alarm**→**Alarm Log**→**Current Alarm Log Statistics** from the main menu to open the **Query Alarm Log Statistics** dialog box.



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](#).

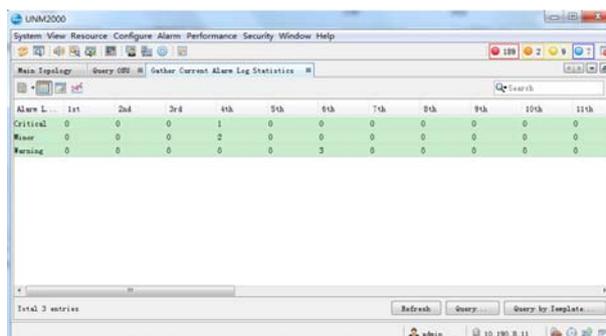
2. Set the statistics conditions in the **Alarm log statistics query** dialog box, and then click **OK**.



Note:

After setting the query conditions in the **Alarm log statistics query** dialog box, users can click **Save As a Template** to save the query conditions as a profile. When needing to query according to the same conditions, users 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. By clicking , you can query and compare the alarms occurred in different time periods.
- ▶ 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 from the alarm bulletin board.

Procedures

1. Click  on the shortcut toolbar in 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

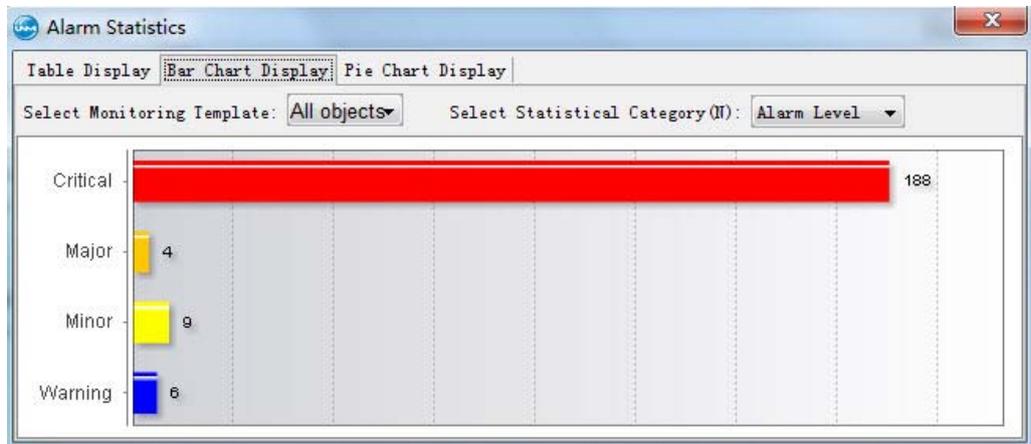
- ◆ Select **Table Display**.

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	Crit...	Major	Less	Note	Unconfirmed	Uncleared
All objects	139	123	3	0	13	137	135

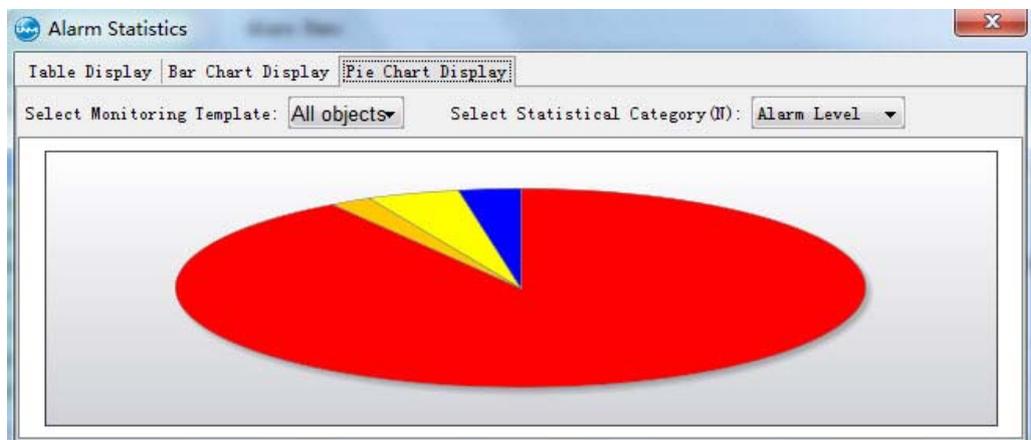
- ▶ Select **Flashing Alarm Indicator LED** to flicker the corresponding LED automatically on the toolbar when an alarm occurs.
 - ▶ Click the **Select Template** or right-click in the table display area to select **Select Template**. In the displayed **Select Template** dialog box, select the corresponding 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 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 the 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.

- 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 **Select 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.

- In the **Query Reported Events** tab, view the query results.

Number	Icon	Level	...	Occuring time	Location information	Remark	NE
8877		Note	...	2014-03-13 16:38:11	10.78.166.130:(9)GSCA[9]		AN5006-30
8727		Critical	...	2014-03-13 16:52:34	10.78.166.130:(18)XACA[18]		AN5006-30
8919		Note	...	2014-03-13 17:58:07	10.78.166.130:(9)GSCA[9]		AN5006-30
8937		Note	...	2014-03-13 18:56:12	10.78.166.130:(9)GSCA[9]		AN5006-30

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 prompt alarms.
- ◆ Click the buttons at the bottom of the **Query Reported Events** tab to perform the corresponding operations.
 - ▶ Click **Query** to re-set 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 menus 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 as a TXT, XLS, CSV or HTML file to the specified directory.
- ◆ Select **Export**→**Export Selected Record** to export the selected events as a TXT, XLS, CSV or HTML file to the specified directory.

7.5.9 Viewing the Reported Alarms

The following introduces the related operations of viewing the reported alarms.

Prerequisite

The alarm reporting rules have been set and enabled.

Procedure

1. Select **Alarm** → **Automatic alarm report** in the main menu.
2. In the **View Reported Alarm** tab, view the information on the alarms meeting the reporting conditions.

Number	Icon	Level	Name	Confirm t...	Clear the...	Alarm source	Location information	Port...	Freq...	First create time
4430		Critical	CCM LOC	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(8)...	256	1	2014-03-25 14:01
4431		Note	UNEXPECTED_LEVEL	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(8)...	424	1	2014-03-25 14:01
4432		Note	Unexpect MEP ID	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(8)...	3	1	2014-03-25 14:01
4433		Note	UNEXPECTED_MEP_ID	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(8)...	86	1	2014-03-25 14:01
4434		Note	UNEXPECTED_PERIOD	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(8)...	183	1	2014-03-25 14:01
4435		Note	Y1731_REMOTE_DEFEC...	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(8)...	286	1	2014-03-25 14:01
4436		Note	AIS	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(8)...	89	1	2014-03-25 14:01
4437		Note	LCK	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(8)...	427	1	2014-03-25 14:01
4438		Note	SLOT_INITSUCCESS_TRAP	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(14)...	118	1	2014-03-25 14:01
4439		Note	ONU_UNAUTHENTICATED	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(14)...	258	1	2014-03-25 14:01
4440		Critical	SLOT_DOWN_AND_UP	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(14)...	333	1	2014-03-25 14:01
4441		Note	CPU_USAGE_OVER_THR...	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(14)...	433	1	2014-03-25 14:01
4442		Note	MEM_USAGE_OVER_THR...	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(14)...	170	1	2014-03-25 14:01
4443		Critical	LASER_ALWAYS_ON	Unconfi...	Clear t...	10.78.200.200	10.78.200.200:(14)...	155	1	2014-03-25 14:01



Note:

For the related operations of the buttons, shortcut icons, and shortcut menus in the **Report alarm automatically** 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 appears, you should handle the alarm following the procedures to exclude 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 removed alarms, as well as manual confirmation and identification of a certain processed alarm.

Procedure

- ◆ Confirm alarms manually.
 - 1) See [Viewing Current Alarms](#) or [Viewing 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

After excluding the fault, the equipment will clear the alarms automatically. If the alarms cannot be cleared automatically, you can remove them manually.

Procedure

1. See [Viewing Current Alarms](#) or [Viewing 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 Locating Alarms

By isolating the alarm, the user can locate the topological object that generated this alarm.

Procedure

1. See [Viewing Current Alarms](#), [Viewing Alarm History](#) or [Viewing Alarm Logs](#) for opening the **Current Alarm**, **Alarm History** or **Alarm Log** tab.
2. Right-click the corresponding alarm and select **Topology Location**. The corresponding NE will be located in the **Main Topology** tab.

7.6.4 Filtering Alarms

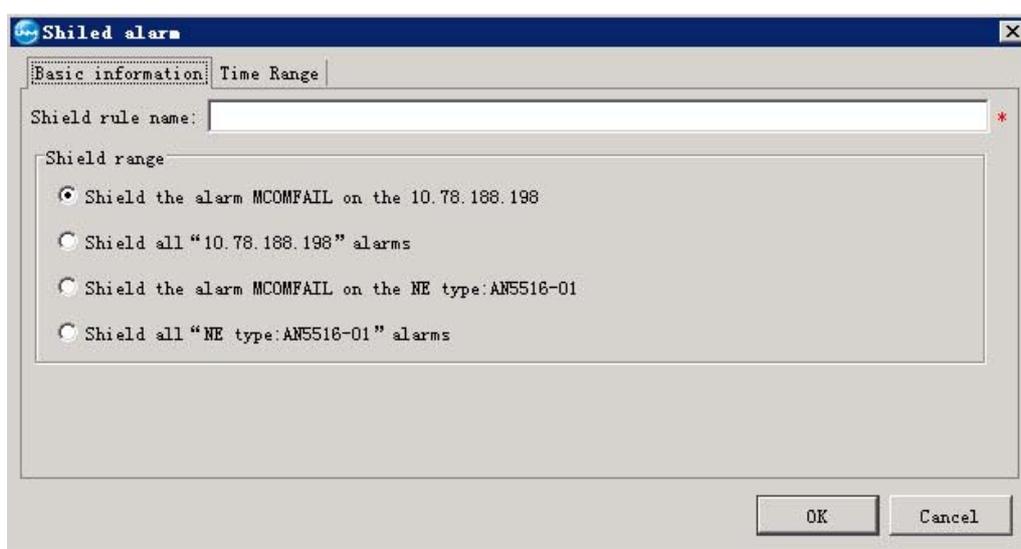
The following introduces how to shield a certain alarm in the current alarm query interface. When some alarms do not need to be handled, you can filter these alarms.

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](#).

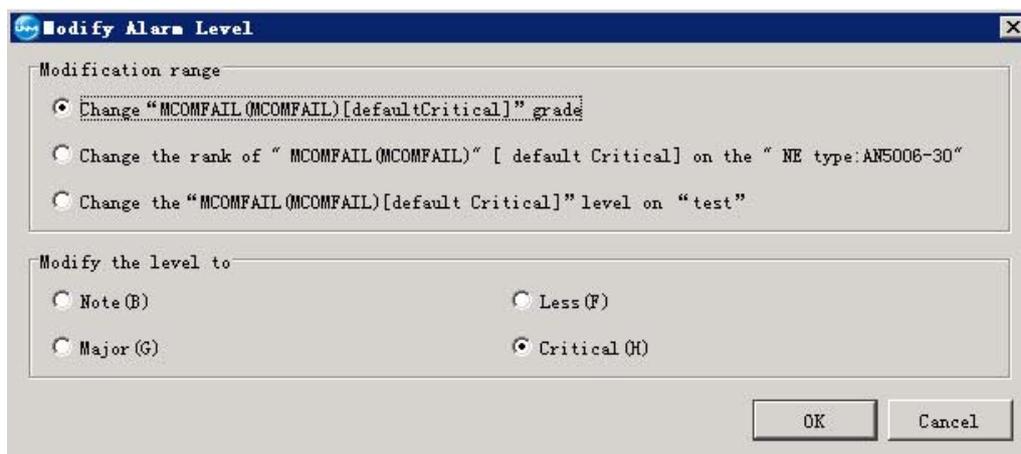
7.6.5 Modifying Alarm Levels

The user can set the alarm levels of the network management alarms as needed, so as to enhance the alarm monitoring efficiency.

Procedures

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 displayed **Modify Alarm Level** dialog box, select the corresponding check boxes of the **Modification Range** and the **Modify the Level to**.



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

7.6.6 Editing Alarm Remarks

The user can edit the alarm remarks to record extra alarm information for future maintenance.

Procedures

1. See [Viewing Current Alarms](#) for opening the **Current Alarm** tab.
2. Right-click the corresponding alarm and select **Remark**.
3. In the **Edit alarm remark** dialog box that appears, enter the alarm remarks.
4. Click **OK** and you can view the entered alarm remarks in the **Remark** field of the corresponding alarm.

7.6.7 Exporting Alarms

The following introduces how to print or export the alarm information.

Procedures

1. Refer to [Viewing Current Alarms](#), [Viewing Alarm History](#) or [Viewing Alarm Logs](#) and open the **Current Alarm**, the **Alarm History** or the **Alarm Log** tab.
2. Export 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 as a TXT, XLS, CSV or HTML file.
 - Export the selected alarm entry. Select the alarm entry and right-click to select **Export**→**Export Selected Record** to export the selected alarm entries as a TXT, XLS, CSV or HTML file.

7.6.8 Editing Alarm Maintenance Experience

By recording the alarm maintenance experience, the user can handle the alarms of the same type quickly and conveniently.

Procedures

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, the user can manage the maintenance referring to [Managing Maintenance Experience](#).

7.6.9 Managing Maintenance Experience

By managing the maintenance experience, users can refer to the maintenance experience for handling the alarms of the same type.

Procedure

1. Select **Alarm** → **Maintenance experience management** in the main menu.
2. In the **Alarm Maintenance Experience Management** tab, view the alarm maintenance experience entries.
3. Perform the following operations as required:
 - ▶ In the right pane, select the experience entry and click the corresponding buttons at the lower right corner, or right-click the entry and select **Edit**, **Delete**, **Copy Cell**, **Print**, or **Export** from the shortcut menu.
 - ▶ Filter the maintenance experience. Click  above 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.

- In the **New Alarm Maintenance Experience** dialog box, set **Equipment Type** and **Alarm Name**, enter the maintenance experience information and click **OK**.

7.6.10 Exporting All Alarm Data to the FTP Service

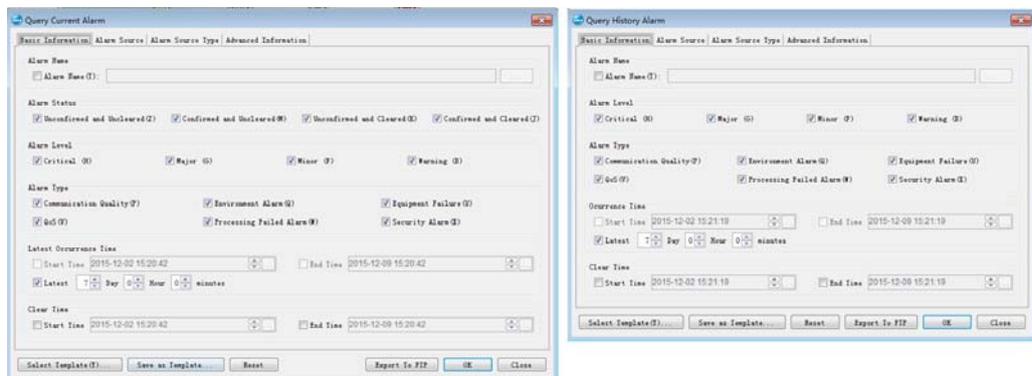
You can set the FTP server and export all the current alarms and alarm history to the local client or other hosts in the network so that you need not perform operations on the UNM2000 server remotely.

Prerequisite

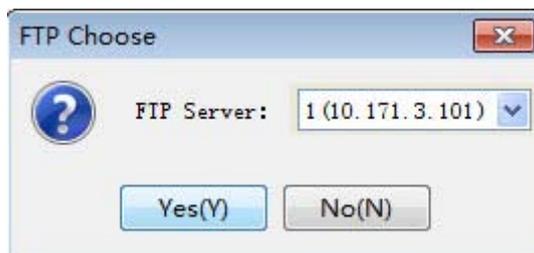
The FTP server is configured.

Procedure

- On the UNM2000 main menu, select **Alarm**→**Current Alarm / History Alarm** to open the **Query Current Alarm / Query History Alarm** dialog box.



- In the alarm query dialog box, select **Export to FTP** to open the **FTP Choose** dialog box.



- Specify the FTP server address and click **Yes** to export all alarm data to the specified FTP server.

7.7 Customizing the Alarm Information

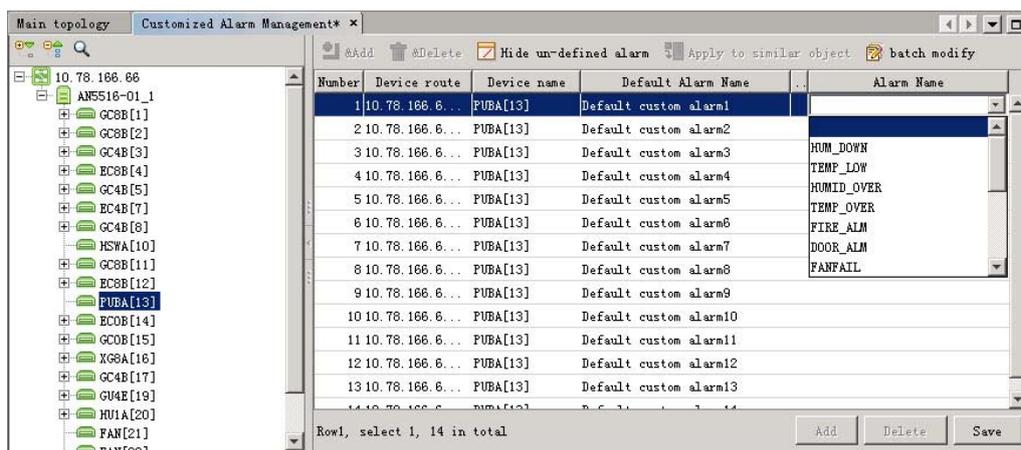
The user can customize alarm names and levels according to maintenance requirements, for easier management and alarm monitoring.

7.7.1 Customizing Alarm Names

To obtain the physical environment information of the equipment, users 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

- Select **Alarm** → **Custom alarm management (N)** in the main menu.
- In the **Please Select a NE** dialog box, select the desired NE and click **OK**.
- In the left pane of the **Custom Alarm Name** tab, select the PUBA card or ONU which needs the customized alarms, and click the **Default Alarm Name** bar to select the alarm name.



- Click **Save** to save the settings in 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 Customizing Alarm Levels

Users can adjust the alarm levels of all objects, the appointed types of equipment, or the appointed equipment as required.

Procedure

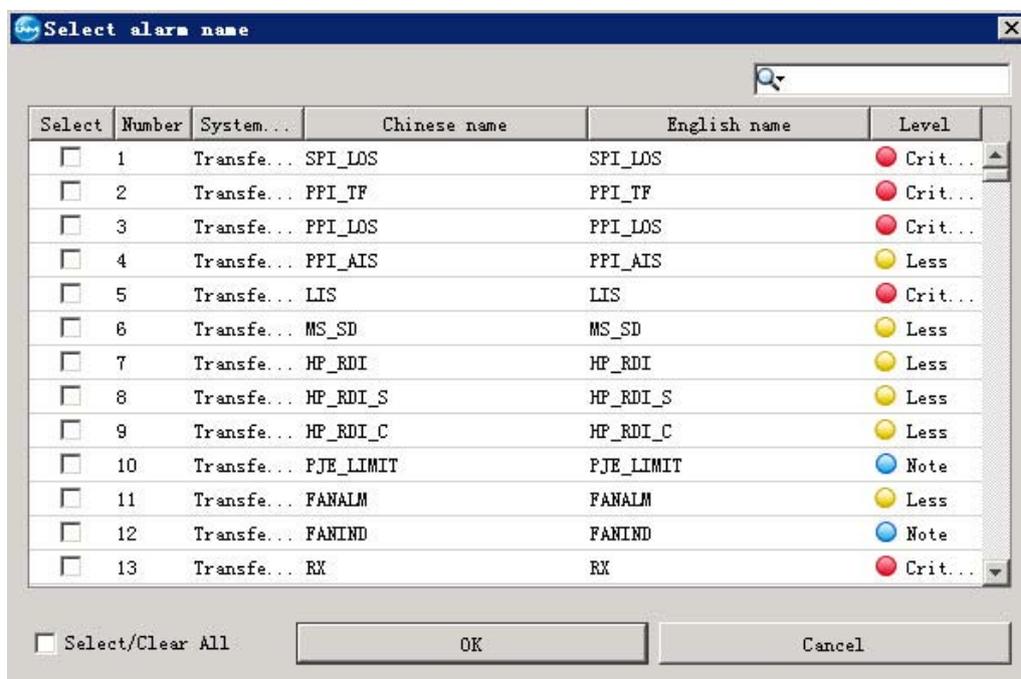
1. Select **Alarm**→**Custom alarm level** in the main menu.
2. At the lower right corner of the **Customize Alarm Level** tab, click **Create**; or right-click in the blank area of the tab, and select **Create**.
3. In the **New Customized Rule of the Alarm Level** dialog box, set **Alarm Source**.
 - ▶ Select **All Objects**, and the customized alarm levels apply to all objects.
 - ▶ Select **Select Equipment**, click  in the **Select object** dialog box, select the card of a certain equipment set, and 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**.



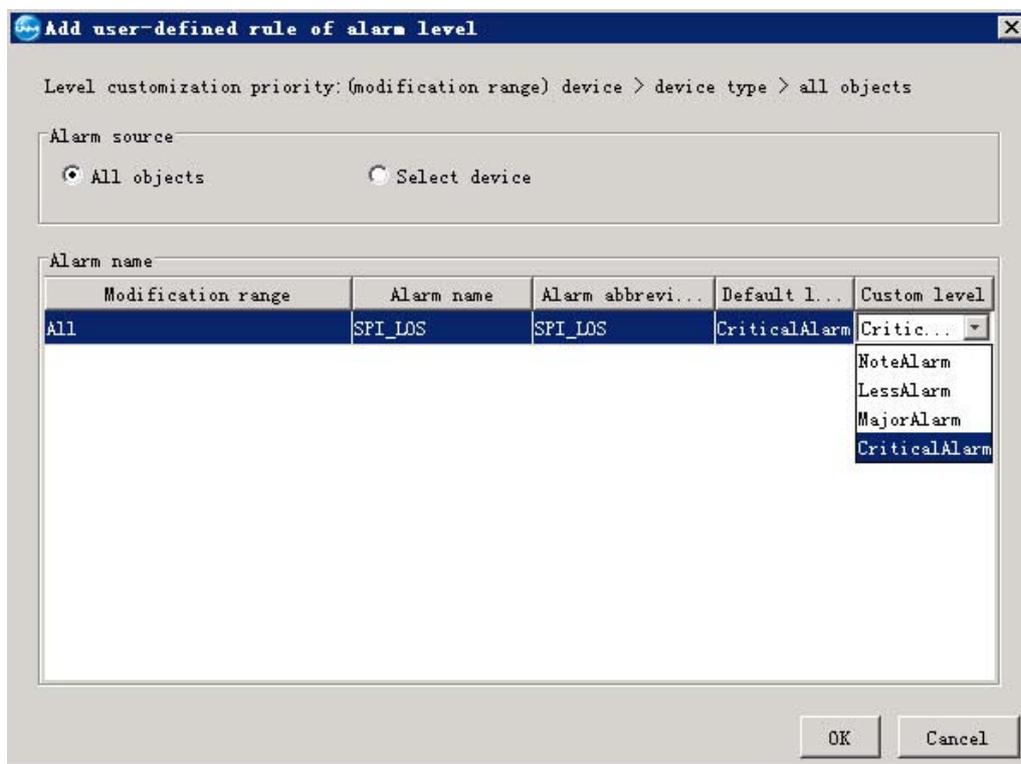
Note:

The priorities of custom alarm levels are as follows: equipment > equipment type > all objects.

4. Right-click in the blank area of the **Alarm Name** section, click **Select** from the shortcut menu, select the desired alarms in the **Select Alarm Name** dialog box, and click **OK**.



5. Click the **Custom level** bar of the corresponding alarm, and select the needed alarm level. Then click **OK**.



- 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 **Custom Alarm Level** tab, click the **Custom Level** column of the corresponding alarm entry to reset the alarm level. Then click **Save all**.

7.7.3 Setting the Project Alarm Filter

During the project installation, commissioning, cut over and maintenance, massive alarms may occur, which will distract maintainers from significant alarms. Users can automatically filter all the alarms and alarm clearance information reported by the resources 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 7-4 and set the relevant project alarm filtering parameters.

Table 7-4 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 filter.

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**.

7.8 Remote Alarm / Event Notification

When the remote alarm / event notification rules are set, the UNM2000 will send the alarms / events matching the conditions to the maintainer via email or SMS so that the maintainer not on-site can obtain the alarms / events generated on the devices and UNM2000 timely and take the corresponding measures.

7.8.1 Setting Remote 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 Parameter** to open the dialog box.

3. Set the related parameters in the **Email Notice**, **Message modem setting**, and **Message gate setting** tabs respectively. Click **Apply** to apply the settings.

7.8.2 Setting the Remote Notification Format of the Alarm / Event

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 dialog box.
3. Set the remote notification format of the alarm / event.
 - ▶ 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** to apply the settings.

Other Operations

Click **Restore Default Configurations** to restore the parameters to the values set last time.

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

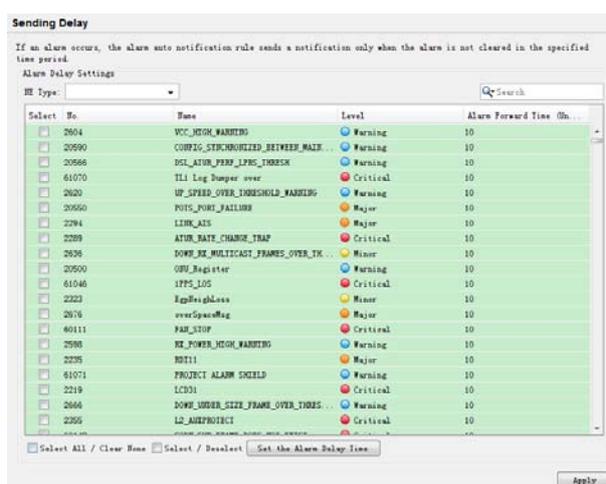
1. Select **Alarm**→**Alarm remote notification management** in the main menu.
2. Execute the following operations as required:
 - ▶ In the right pane, click the button below the corresponding entry, or right-click the entry, and select operations such as **Enable/Disable**, **Delete**, **copy cell (K)**, **Print...**, or **Export**.
 - ▶ Select the corresponding receiver in the left pane, and modify the information items in the right pane. After completing the modification, 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 ways 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 completing the settings, click **OK**.

7.8.4 **Setting the Remote Notification Rules of the Alarm / Event**

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.



3. Set the alarm delay time interval and then click **Apply**. Set all **Alarm Forward Time** items in the **Sending Delay** dialog box to the new values set.
4. 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.
- ◆ Users can modify the delay time interval of a certain alarm as required.

5. Click **Apply** after the settings are completed, and the settings will be valid.

7.8.5 Sending the Remote Alarm / Event Notification

After analyzing and editing the current alarms / events of different stations via the UNM2000 client, the maintainer of the central office equipment room sends the

alarms / events of different stations to the maintainer who is nearest to the failure location according to geographical distribution of maintainers. This achieves quick and prompt processing of alarms / events, greatly improving the device maintenance efficiency.

Prerequisite

- ◆ The parameters and rules related to the remote alarm / event notification have been configured.
- ◆ You have the authorities of **Maintainer Group** or higher authorities.

Procedure

1. In the main topology, right-click the NE and select **Current Alarm**.
2. In the **Current Alarm** dialog box, right-click the alarm entry and select **Remote Notification**→**Email / Message** from the shortcut menu to open the **Send a Mail to Notify** or **Notify via SMS** dialog box.
3. Select **Receiver**, and enter **Title** and **Content**. Then click **OK**.

7.9 Managing Alarm / Event Data

When the alarm history saved in the UNM2000 exceeds a certain limit, it will influence the operations performed in the UNM2000. The alarm saving function can be used to remove the alarm history data from the database to a specified file, which improves the running performance of the UNM2000. The UNM2000 supports manual save and overflow save of alarms.

- ◆ **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 to a specified file folder manually at anytime. You can set the saving period of alarm history data. 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.

7.9.1 Settings the Alarm / Event Overflow Save

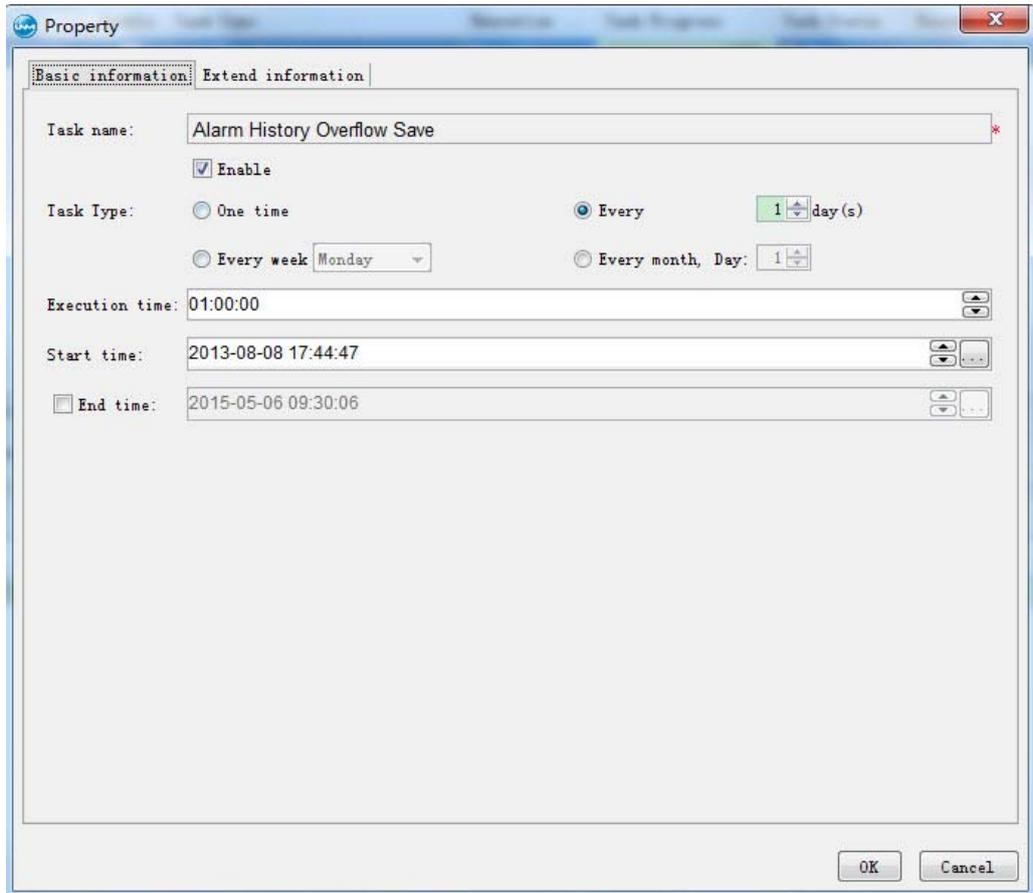
When the alarm / event overflow save task is set, the UNM2000 will regularly check whether the alarm / event historical data in the database have met the preset conditions. If yes, the UNM2000 will save the alarm / event historical data automatically. The saved alarm / event historical data will be deleted from the database.

Background Information

The default historical data overflow save task provided by the UNM2000 cannot be deleted. The user can modify the overflow save conditions of the corresponding task as required.

Procedures

1. Select **System**→**Save Data** in the main menu to open the **Save the Data** tab.
2. In the left pane, select **Save History Data**→**Overflow Saving**→**Historical Overflow Save** to view the existing historical data overflow save task.
3. Open the **Property** dialog box of the corresponding historical data save task via one of the following ways:
 - ▶ Double-click the corresponding overflow save task in the right pane.
 - ▶ Right-click the corresponding overflow save task in the right pane and select **Attribute** from the shortcut menu.
 - ▶ In the left pane, click  next to the **Overflow Saving**, right-click the corresponding overflow save task and select **Attribute** from the shortcut menu.



4. See Table 7-5 for setting the properties of the overflow save task.

Table 7-5 Descriptions of the Alarm / Event Overflow Save Task Settings

Parameter		Description
Basic Information	Task name	The name of the overflow save task; read-only.
	Yes	Select this check box to start this task.
	Task type	The task execution cycle. The default setting is once every other day.
	Execution time	The execution time of the task.
	Begin Time	The start time of the task.
	End Time	The end time of the task.

Table 7-5 Descriptions of the Alarm / Event Overflow Save Task Settings (Continued)

Parameter		Description
Extend Information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the historical data meeting the overflow save conditions to a file. You can select to save the historical data as a CSV file to the server's hard disk or in the FTP server. ◆ Select Delete and the historical data meeting the overflow save conditions are deleted directly.
	Overflow Border	The preset save proportion of the database when the save task is carried out as soon as the historical data have exceeded the maximum storage entry quantity or the threshold value.
	Capacity limit	The preset days of saving the historical data in the database when the save task is carried out.

5. After completing the settings, click **OK**.
6. Select the corresponding overflow save task in the left pane, and click **Execute Now** in the upper right pane. The execution result is shown in the lower right pane.

7.9.2 Settings the Manual Save of the Alarms / Events

The UNM2000 supports manual save of historical alarm / event data to avoid insufficient database space.

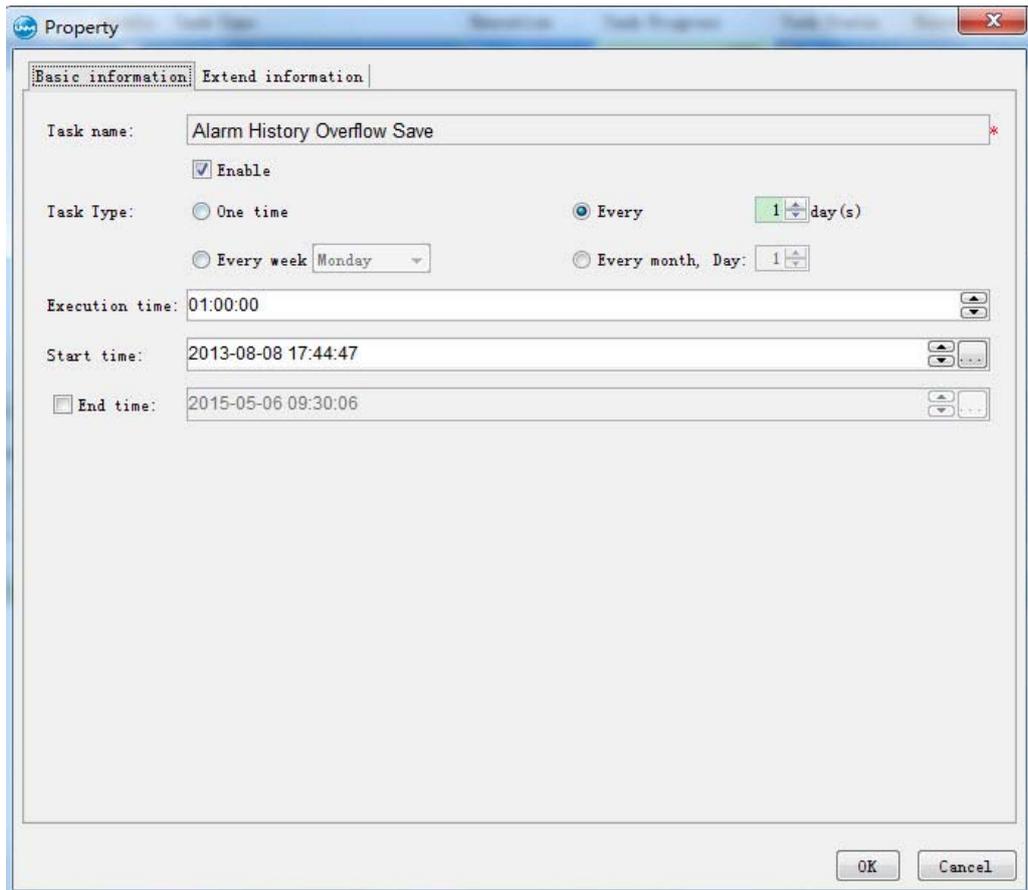
Background Information

The default manual save task of historical alarm / event data provided by the UNM2000 cannot be deleted. The user can modify the manual save conditions of the corresponding task as required.

Procedures

1. Select **System** → **Save Data** in the main menu to open the **Save the Data** tab.
2. In the left pane, select **Save History Data** → **Save Manually** → **Alarm History** to view the existing manual save task of alarm history.
3. Select either way below to open the **Properties** of the corresponding manual save task of historical data.

- ▶ Double-click the corresponding manual save task in the right pane.
- ▶ Right-click the corresponding manual save task in the right pane and select **Properties**.
- ▶ In the left pane, click  next to the **Manual Dump**, right-click the corresponding manual save task in the right pane and select **Properties**.



4. See Table 7-6 for setting the properties of the overflow save task.

Table 7-6 Descriptions of the Alarm / Event Overflow Save Task Settings

Parameter		Description
Basic Information	Task name	The name of the overflow save task; read-only.
	Yes	Select this check box to start this task.
	Task type	The task execution cycle. The default setting is once every other day.
	Execution time	The execution time of the task.
	Begin Time	The start time of the task.

Table 7-6 Descriptions of the Alarm / Event Overflow Save Task Settings (Continued)

Parameter		Description
	End Time	The end time of the task.
Extend Information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the historical data meeting the overflow save conditions to a file. You can select to save the historical data as a CSV file to the server's hard disk or in the FTP server. ◆ Select Delete and the historical data meeting the overflow save conditions are deleted directly.
	Overflow Border	The preset save proportion of the database when the save task is carried out as soon as the historical data have exceeded the maximum storage entry quantity or the threshold value.
	Capacity limit	The preset days of saving the historical data in the database when the save task is carried out.

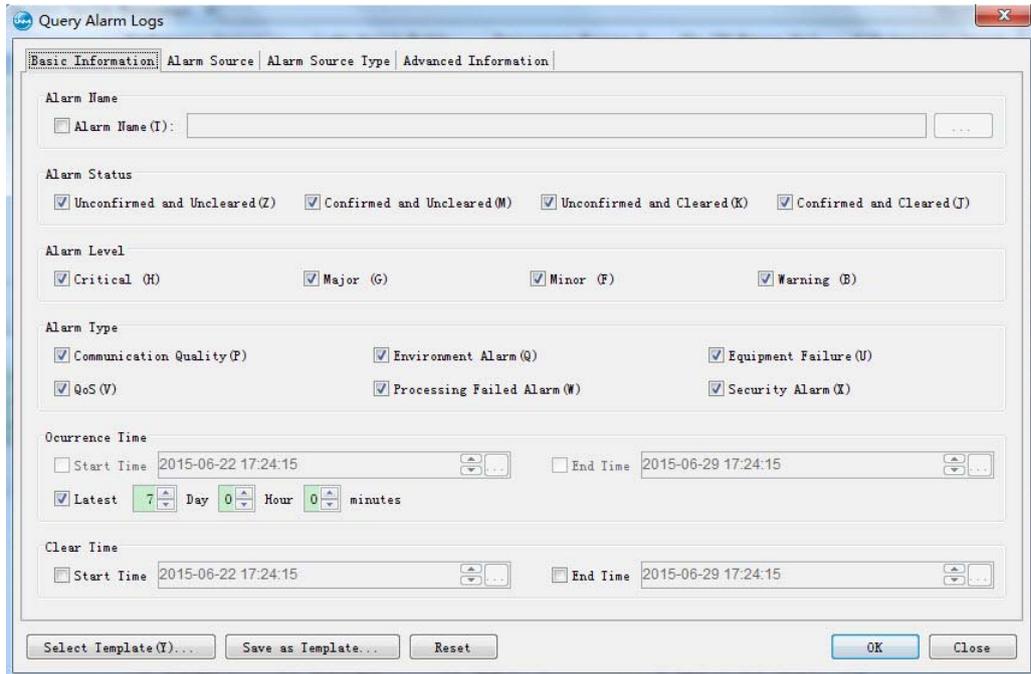
5. Select the corresponding manual save task in the left pane, and click **Execute now** in the upper right pane. The execution result is shown in the lower right pane.

7.10 Alarm Logs

The **Alarm Log** function supports querying alarm logs, and gathering statistics of alarm history logs and current alarm logs. You can set the statistical conditions as needed to query the alarm logs.

Querying Alarm Log

1. On the UNM2000 main menu, select **Alarm** → **Alarm Log** → **Query Alarm Log**.
2. Set the query conditions, as shown below.



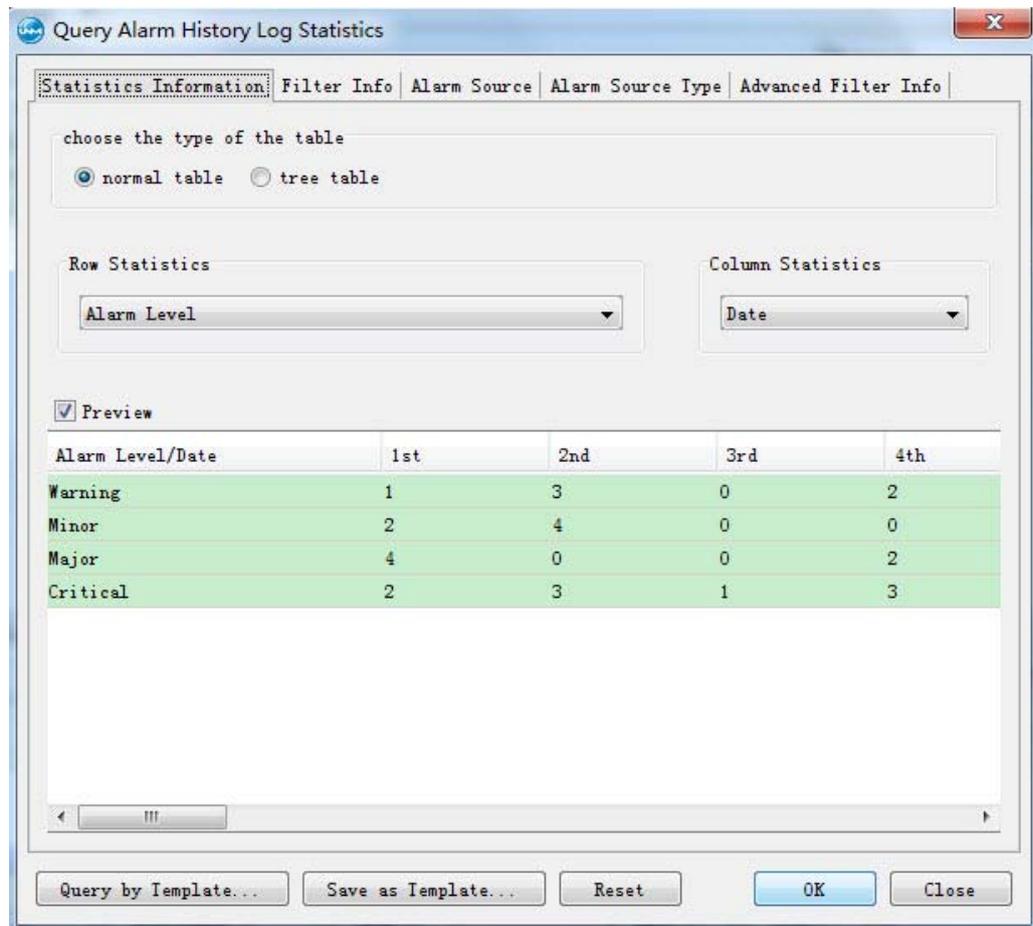
Note:

- ◆ Click **Select Template** to select the alarm log query template.
- ◆ Click **Save as Template** to save the current query conditions as the alarm log query template.

3. Click **OK**. The query result appears in the **Alarm Log** tab.

Gathering Statistics of Alarm History Logs

1. On the UNM2000 main menu, select **Alarm**→**Alarm Log**→**Alarm History Log Statistics**.
2. Set the query conditions, as shown below:



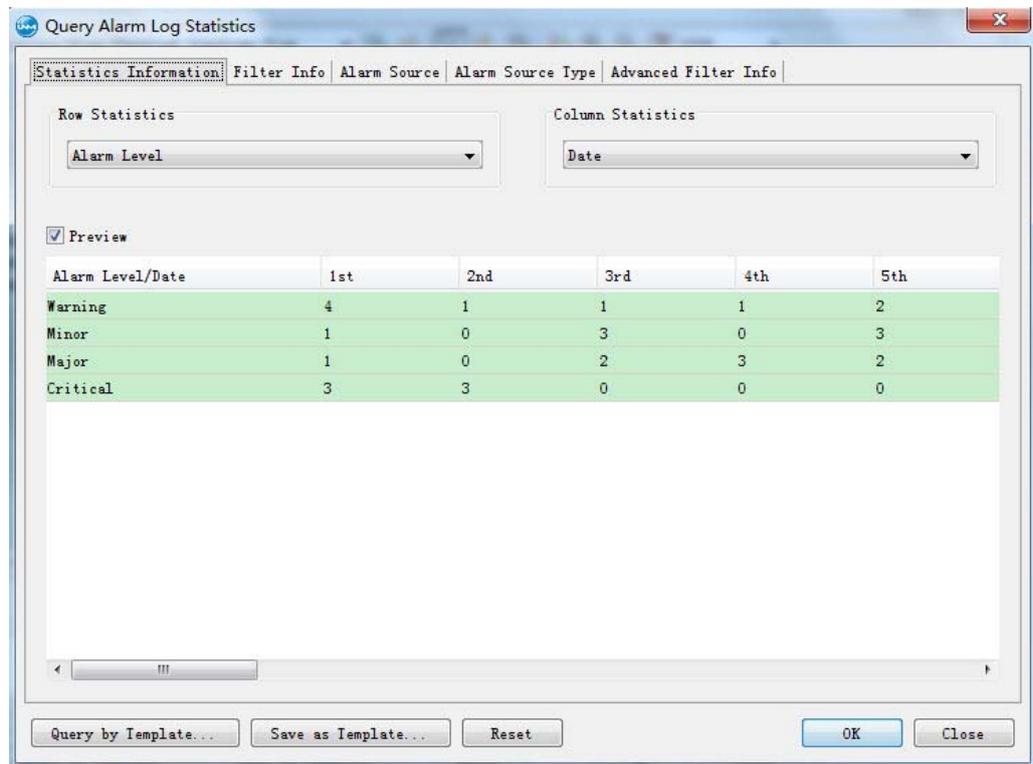
Note:

- ◆ Click **Query by Template** to select the corresponding statistical template.
- ◆ Click **Save as Template** to save the current query conditions as the statistical template of current alarm logs.

3. Click **OK**. The statistical result appears in the **Alarm Log History Statistics** tab.

Gathering Statistics of Current Alarm Log

1. On the UNM2000 main menu, select **Alarm** → **Alarm Log** → **Current Alarm Log Statistics**.
2. Set the query conditions, as shown below:



Note:

- ◆ Click **Query by Template** to select the corresponding statistical template.
- ◆ Click **Save as Template** to save the current query conditions as the statistical template of current alarm logs.

3. Click **OK**. The statistical result appears in the **Current Alarm Log Statistics** tab.

7.11 Managing Alarm Frequency Analysis Rules

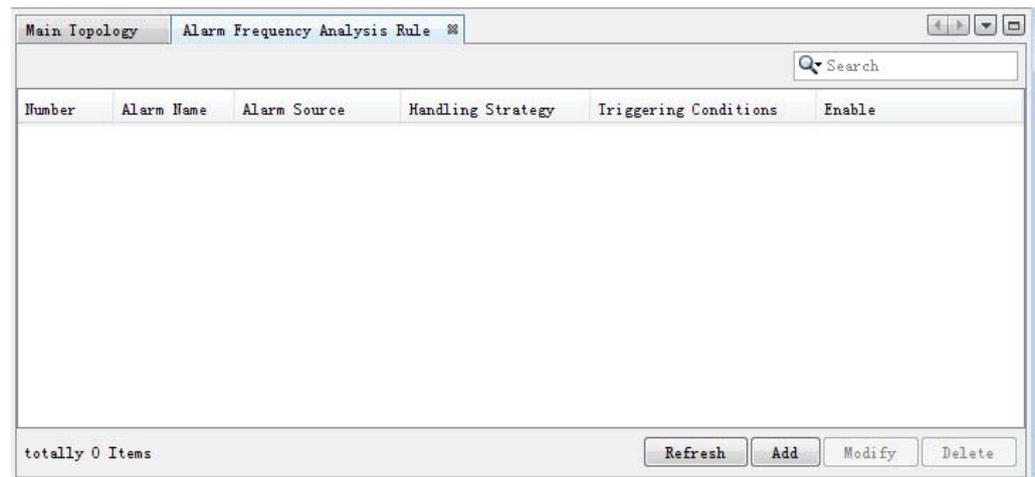
For alarms (such as ONU fiber disconnection, power failure and MGC link alarms) with a large quantity but little impact in current networks, you can set the alarm frequency analysis rules and set **Handling Strategy** and **Triggering Conditions** for different alarms. The UNM2000 will filter the alarms or generate new alarms based on the rules.

Prerequisite

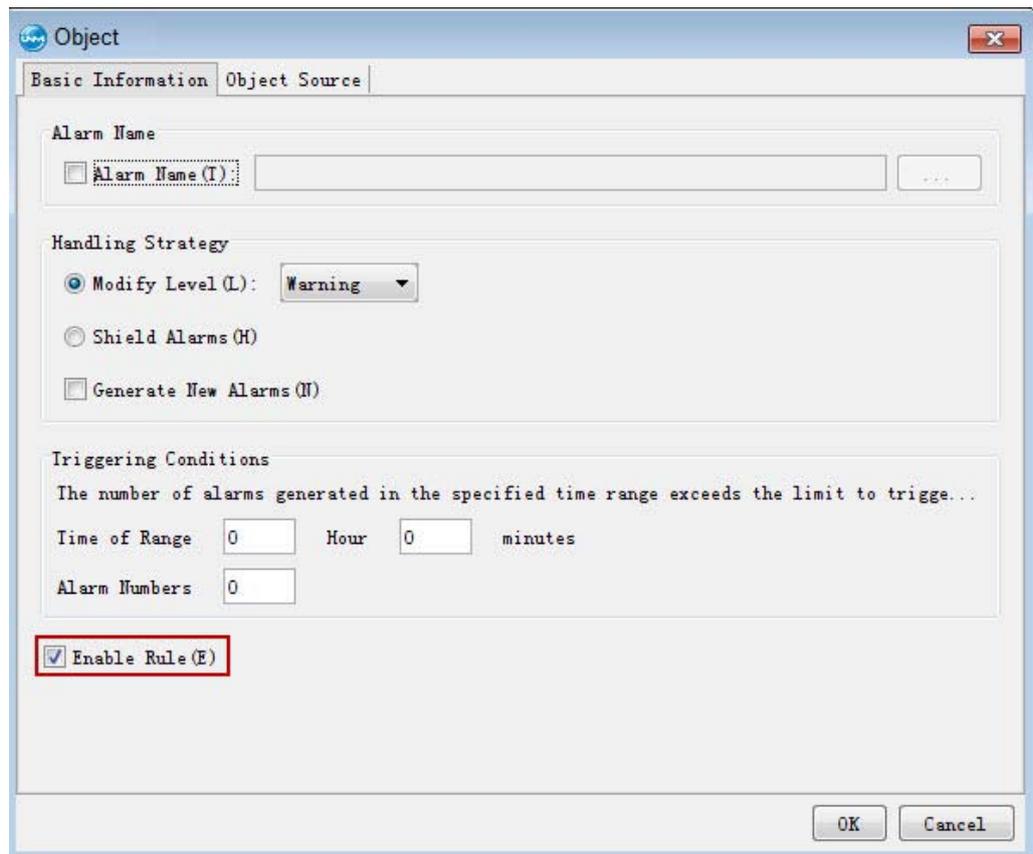
You have the authorities of **Operator Group** or higher authorities.

Procedure

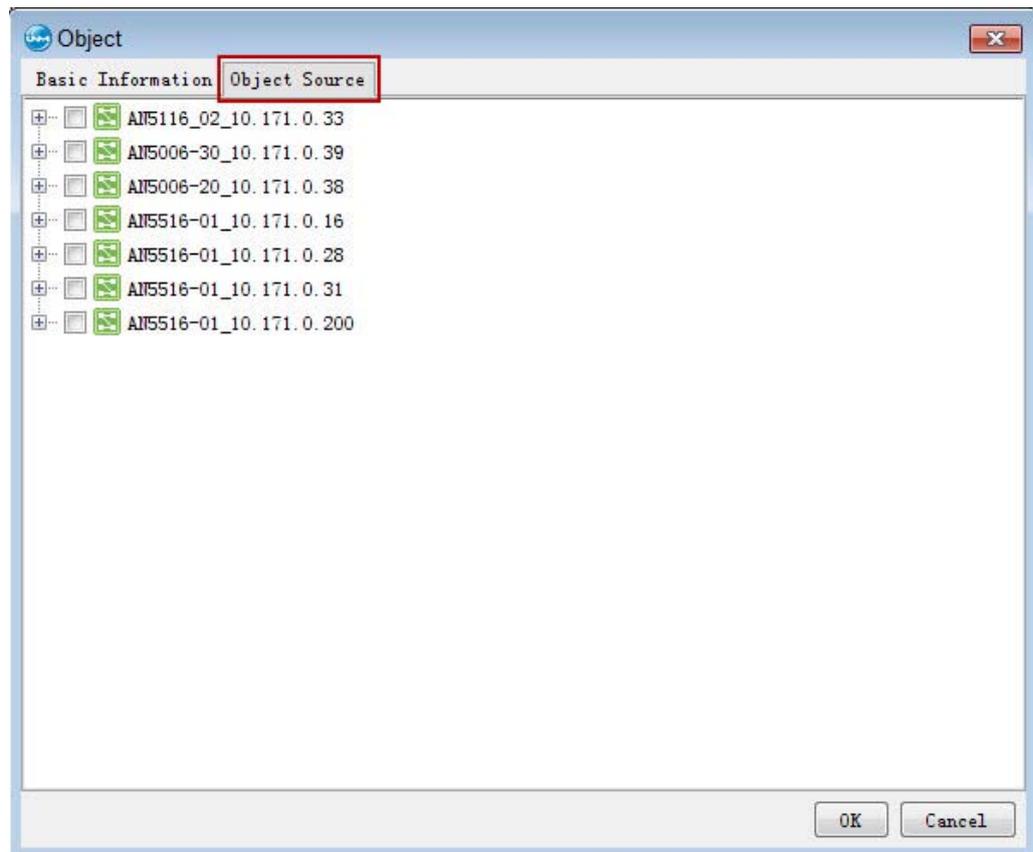
1. On the UNM2000 main menu, select **Alarm**→**Alarm Frequency Analysis Rule** to open the **Alarm Frequency Analysis Rule** tab.



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**. Select or clear the **Enable Rule** check box to enable or disable the alarm frequency analysis rule.



4. In the **Object** dialog box, select the **Object Source** tab to set the applicable objects of the alarm frequency analysis rule.



5. Click **OK** to create an alarm frequency analysis rule successfully.

8 Performance Management

The UNM2000 performs strong performance management functions. Users can monitor the performance data to eliminate the potential problems in a timely manner and reduce the risks that will influence the reliable operation of the equipment.

- 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 the Performance Collection
- Managing Performance Data

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 be used to remove the performance history data from the database to a specified file, which improves the running performance of the UNM2000.

Comparing Performance

Compare the performance data in appointed period of an appointed object, so as to understand the operating status of this object in different periods.

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 authorities of **Operator Group** or higher authorities.

Procedure

1. In the main menu, select **Performance**→**Performance Query Template** to open the **Performance Query Template** 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.

8.2.2 Creating a Performance Query Profile

Users can save the current performance history query conditions as a profile to avoid setting query conditions repeatedly. Then users can select the corresponding

profile to query the performance in the future. The following introduces how to create performance query template.

Prerequisite

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

Procedure

1. In the main menu, select **Performance** → **Performance Query Template** to open the **Performance Query Template** tab.
2. Select one of the following access methods to open the **Create 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 right pane and select New Performance History Search Template from the shortcut menu.
3	Right-click Performance History Query Template in the left pane and select New Performance History Search Template from the shortcut menu.

3. In the **AddPerformance query template** dialog box, set the parameters in the **Template information**, **Basic information**, and **Advance information** tabs as required.



Note:

Click **Copy from other objects Performance query template...**, select the profile in the **Choose template** dialog box, and copy the basic and advanced information of the selected profile. This can improve the setting efficiency.

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

Other Operations

In the right pane, select the button below the corresponding entry, or right-click the entry, and select operations such as **Delete**, **Refresh**, **Set / Cancel Default Template**, **Print...**, **copy cell (K)**, 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 authorities of **Operator Group** or higher authorities.

Procedure

1. In the main menu, select **Performance**→**Performance Query Template** to open the **Performance Query Template** 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**.

8.3 Setting the Performance Collection Time

Users can set the collection time of the 24-hour performance as required.

Prerequisite

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

Procedure

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

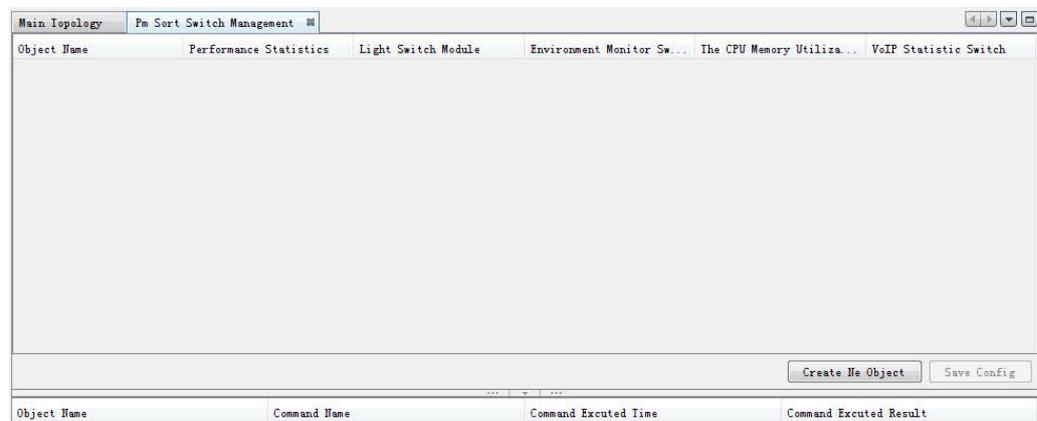
2. Select **Performance setting**→**Server Settings** in the left pane to open the dialog box.
3. Set the 24-hour performance collection time and then click **Apply** to apply the settings.

8.4 Configuring the Performance Classification Switch in a Batch Manner

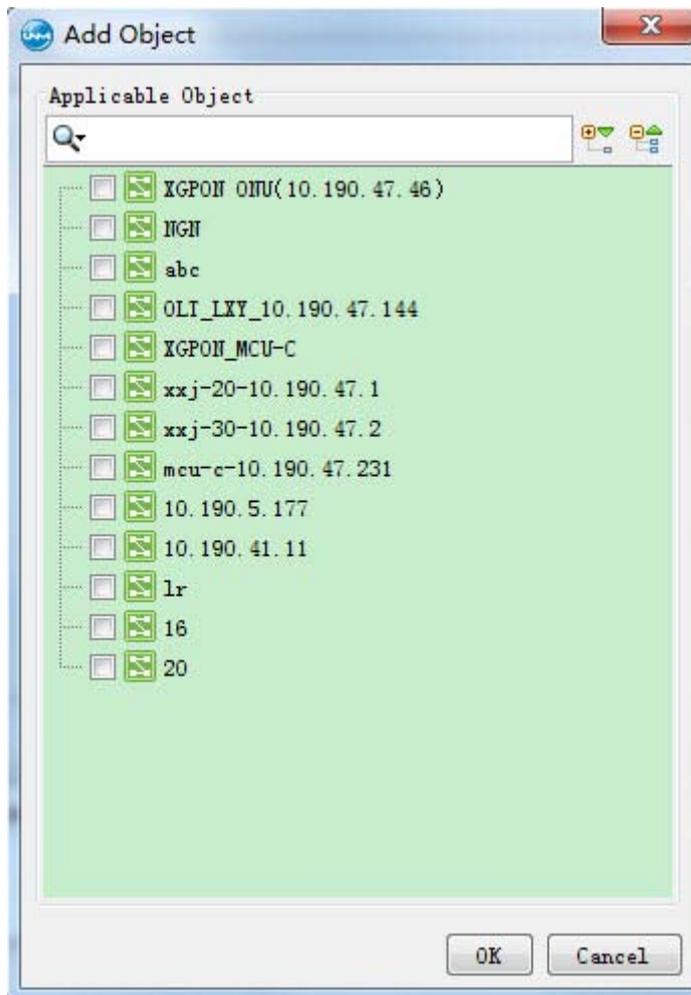
The UNM2000 new function, **Performance Classification Switch Configuration**, is used to meet the following requirements: selecting one or multiple OLT NEs in the UNM2000, querying the line card or the ONU performance classification switch, modifying the existing switches in a batch manner in the UNM2000 and delivering the changes to the device.

Procedure

1. On the UNM2000 main menu, select **Performance**→**Performance Switch Config** to open the **Pm Sort Switch Management** tab, as shown below:



2. Click **Create NE Object** to open the **Add Object** dialog box and then select one or multiple NEs, as shown below:



3. Click **OK**. The UNM2000 reads the performance classification switch status of the selected device, as shown below:

Object Name	Performance Statistics	Light Switch Module	Environment Monitor S...	The CPU Memory Util...	VoIP Statistic S
XGPON ONU(10.190.47.46)					
GC0B[1]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
XP4A[7]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
XP4A[14]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	

Object Name	Command Name	Command Executed Time	Command Executed Result
XGPON ONU(10.190.47.46) ...		2015-06-29 17:16:45	Succeeded
XGPON ONU(10.190.47.46) ...		2015-06-29 17:16:45	Succeeded
XGPON ONU(10.190.47.46) ...		2015-06-29 17:16:45	Succeeded

4. Modify the performance classification switches in a batch manner and then click **Save Config**.

8.5 Managing the Card Performance

The following introduces how to manage the card performance, including viewing the current performance and the real-time performance and conducting the performance comparison.

- ◆ **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.
- ◆ **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 appointed period of an appointed object, so as to understand the operating status of this object in different periods.

8.5.1 Viewing the Current Performance

Users can understand the operating status of the equipment via viewing the current performance.

Prerequisite

- ◆ The performance classification function of the corresponding device is **Enabled**.
- ◆ You have the authorities of **Operator Group** or higher authorities.

Procedure

1. Right-click the corresponding NE in the object tree at the left side of the **Main topology** tab or the physical topology view at the right side, and select **Open NE manager** from the shortcut menu.
2. Select one of the following methods to view the current performance.

- ▶ In the **Device Tree** of the **NE Manager** window, right-click the corresponding card or port and select **Current Performance** from the shortcut menu.
- ▶ In the **Subrack View** of the **NE Manager** window, right-click the corresponding card and select **Current Performance** from the shortcut menu.

The screenshot shows a window titled 'Shelf Board-Current performance-HSWA[10]'. It contains a table with performance data for three HSWA[10] objects. The table has columns for Object Name, Performance Code, Value, Unit, Begin Time, and End Time. Below the table, there is a '15 Minutes' drop-down menu and 'Query (F)' and 'Refresh' buttons.

Object Name	Performance Code	Value	Unit	Begin Time	End Time
HSWA[10]	CPU/Memory Usage	5.57	%	2009-01-0...	2009-01-0...
HSWA[10]	Memory Usage	58.75	%	2009-01-0...	2009-01-0...
HSWA[10]	Environment Temperature	49.0	°C	2009-01-0...	2009-01-0...

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 the current performance tab, and select operations such as **Print**, **copy cell (K)**, 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

You can obtain the abnormal performance data of the devices by viewing the performance history 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 authorities of **Operator Group** or higher authorities.

Procedure

1. Select the access method mentioned in Table 8-1 to open the **History property query** dialog box.

Table 8-1 Access Method of Viewing the Performance History

Operation	Access Method
Viewing 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 in the shortcut menu.

2. Set the query conditions in the **History property query** dialog box according to requirements.



Note:

- ◆ In the **Advance information** tab, users 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 Comparison of Performance Data

Compare the performance data in appointed period of an appointed object, so as to understand the operating status of this object in different periods.

Prerequisite

- ◆ The system has waited two test periods (15 minutes for each test period) at least.
- ◆ The performance statistics function is enabled.
- ◆ You have the authorities of **Operator Group** or higher authorities.

Procedure

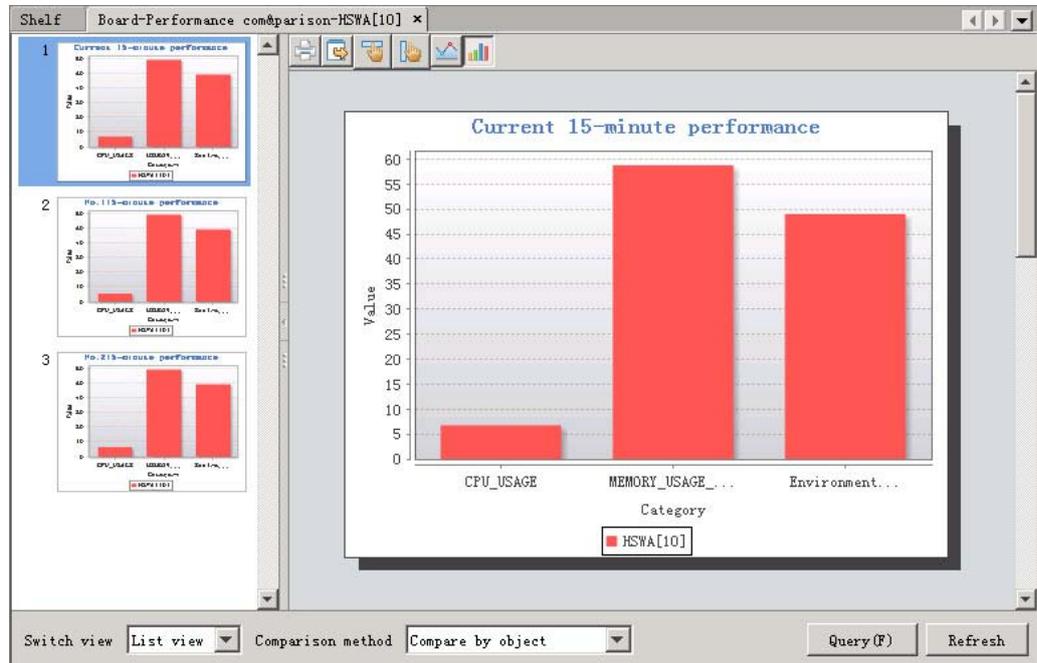
1. Right-click the corresponding NE in the object tree at the left side of the **Main topology** tab or the physical topology view at the right side, and select **Open NE manager** from the shortcut menu.
2. Select one of the following methods to open the **Performance Comparison Query** dialog box.
 - ▶ In the **Device Tree** of the **NE Manager** window, right-click the corresponding card or port, and select **Performance Comparison** from the shortcut menu.
 - ▶ In the **Subrack View** of the **NE Manager** window, right-click the corresponding card and select **Performance Comparison** from the shortcut menu.
3. In the **Performance Comparison Query** dialog box, set the query conditions of the performance comparison.



Note:

Select at least two periods from the **15 Minutes** drop-down list.

- 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 the corresponding button at the top part of the right pane, and users can print the comparison results or export them to a ***.jpeg** file and save the file in the appointed directory.

8.5.4 Viewing the Real-time Performance

This function enables you to monitor the performance data of the selected resources in real time.

Prerequisite

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

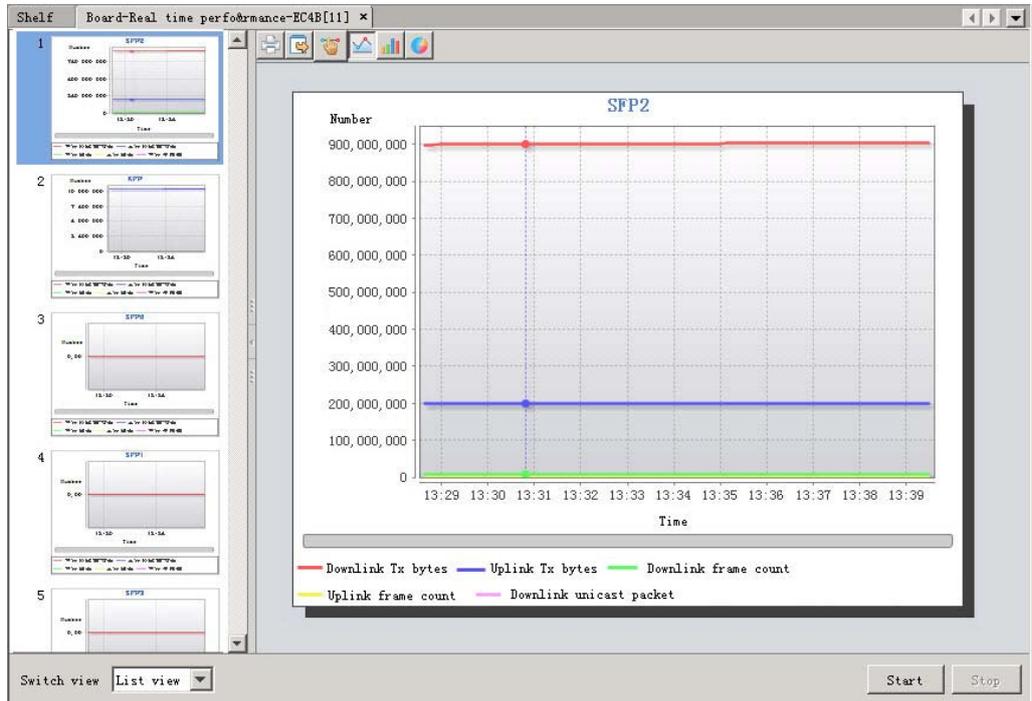
Procedure

1. Right-click the corresponding NE in the object tree at the left side of the **Main topology** tab or the physical topology view at the right side, and select **Open NE manager** in the shortcut menu.
2. Select one of the following methods to open the **Real-time Performance** dialog box.
 - ▶ In the **Device Tree** of the **NE Manager** window, right-click the corresponding card or port, and select **Real-time Performance** from the shortcut menu.
 - ▶ In the **Subrack View** of the **NE Manager** window, right-click the corresponding card and select **Real-time Performance** from the shortcut menu.
3. Set **Collection Cycle**, **Time Length**, and **Object** for the real-time performance.
4. Click **OK**, and view the real-time performance of the selected object in the **Real-time Performance** tab after a certain period of time.



Note:

- ◆ The system displays the real-time performance in the **List view** and **Curve chart** modes by default. You can select other display modes as required.
 - ◆ Click **Stop** to stop collecting the real-time performance.
-



Subsequent Operation

Click the corresponding button at the top part of the right pane, and users can print the real-time performance results or export them to a *.jpeg file and save the file in the appointed directory.

8.5.5 View Performance History Trend

Users can understand the network operating status by viewing the performance data variation of the designated object using the performance history chart.

Prerequisite

- ◆ The object to be queried has its performance history data.
- ◆ You have the authorities of **Operator Group** or higher authorities.

Procedure

1. Select **Performance** → **View Performance History Trend** from the main menu.

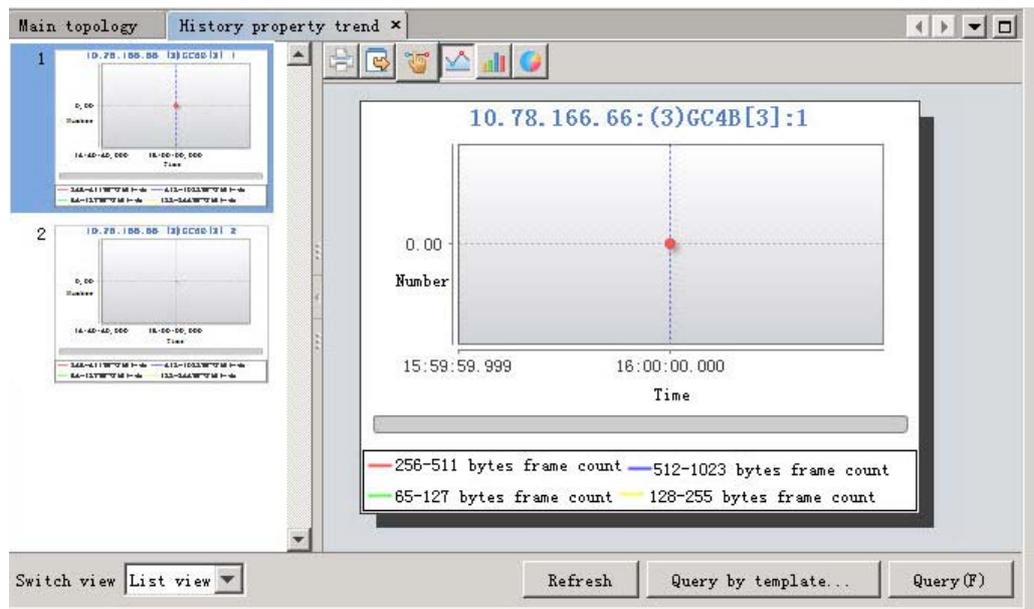
- Set the query conditions in the **History property query** dialog box according to requirements.



Note:

- In the **Advance information** tab, users 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.

- 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.

8.6 Managing the Performance Collection

You can use the scheduled performance collection to query and process the performance data of NEs. The UNM2000 provides the scheduled collection of NE performance data via **NE Performance Indicator Collection** and **NE Performance Threshold Collection** and supports exporting the collection result as a text file to reduce repeated labor.

8.6.1 Managing Performance Index Sets

The following introduces how to view and set the performance index 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 authorities of **Inspector Group** or higher authorities.
- ◆ The time at the NE side has been synchronized with the time at the UNM2000 side.
- ◆ The performance monitoring time and performance event monitoring status of the NE are configured.

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 threshold set, including **Basic Information** and **Member**.

Subsequent Operation

- ◆ Modify the indicator set.

In the left pane, select the corresponding index, 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 Adding 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 authorities of **Inspector Group** or higher authorities.
- ◆ The time at the NE side has been synchronized with the time at the UNM2000 side.
- ◆ The performance monitoring time and performance event monitoring status of the NE are configured.

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** dialog box.

No.	Access Method
1	Click the Performance Collection Management in the left pane, right-click in the right pane and select Create Indicator Set from the shortcut menu.
2	Click the Performance Collection Management in the left pane, right-click in the right pane and select Create Indicator Set from the shortcut menu.
3	Right-click Indicator Set in the left pane and select Create Indicator Set from the shortcut menu.

No.	Access Method
4	Click Indicator Set in the left pane and click Create Indicator Set in the right pane.
5	Click the Indicator Set in the left pane, right-click in the right pane and select Create Indicator Set from the shortcut menu.

- 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.

- After completing the settings, 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 Performance Threshold Sets

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 authorities of **Inspector Group** or higher authorities.
- ◆ The time at the NE side has been synchronized with the time at the UNM2000 side.
- ◆ The performance monitoring time and performance event monitoring status of the NE are configured.

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 Adding a Performance Threshold Set

The user 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 authorities of **Inspector Group** or higher authorities.
- ◆ The time at the NE side has been synchronized with the time at the UNM2000 side.
- ◆ The performance monitoring time and performance event monitoring status of the NE are configured.

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.

No.	Access Method
1	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.
2	Select Threshold Set in the left pane and then right-click in the right pane to select Create Threshold Set from the shortcut menu.
3	Right-click Threshold Set in the left pane and select Create Threshold Set from the shortcut menu.
4	Click Performance Collection Management in the left pane, right-click in the right pane to select Create Threshold Set from the shortcut menu.
5	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 according to 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.
	Remark	Enters the remark information for the threshold set.
Member	Performance code	Click Select and choose the performance code that needs the threshold setting.
	Upper threshold	The upper limit of the corresponding performance code.
	Lower threshold	The lower limit of 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.

Table 8-2 Threshold Set Parameters (Continued)

Parameter		Description
	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
Note: The performance threshold values must be set as follows: Upper limit value > Upper clearance value > Lower clearance value > Lower limit value.		

4. Click **OK**.

8.6.3 Managing Performance Collection Task

The following introduces how to view and create the performance collection tasks.

8.6.3.1 Viewing Performance Collection Tasks

View the performance collection task already set and select the desired performance collection task to collect the performance.

Prerequisite

- ◆ You have the authorities of **Inspector Group** or higher authorities.
 - ◆ The time at the NE side has been synchronized with the time at the UNM2000 side.
 - ◆ The performance monitoring time and performance event monitoring status of the NE are configured.
1. Select **Performance** → **Property collecting management** from the main menu and open the **Performance Collection Management** tab.
 2. In the **Performance collection management** tab, select **Gather task** and view the existing collection tasks in the right tab.

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 Adding a Performance Collection Task

You can monitor the performance data by setting the performance collection task.

Prerequisite

- ◆ You have the authorities of **Inspector Group** or higher authorities.
 - ◆ The time at the NE side has been synchronized with the time at the UNM2000 side.
1. Select **Performance** → **Property collecting management** from the main menu and open the **Performance Collection Management** tab.
 2. Select one of the following access methods to open the **Create Collection Task** dialog box.

No.	Access Method
1	Click Performance Collection Management in the left pane and click Create Collection Task in the right pane.
2	Click Performance Collection Management in the left pane, right-click in the right pane and 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.

No.	Access Method
4	Click Collection Task in the left pane, right-click in the right pane and 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.

- In the **Create Collection Task** dialog box, set the parameters in the **Basic Information**, **Collection Object**, **Collection Specification** and **Collection Cycle** tabs.



Note:

Click **Copy from Other Collection Task** to open the **Select Collection Task** dialog box, select the desired collection task to copy the settings of the corresponding collection task. This improves the setting efficiency.

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

8.7 Managing Performance Data

When the performance history data saved in the UNM2000 exceeds a certain limit, it will influence the operations performed in the UNM2000. The performance data saving function can be used to remove the performance history data from the database to a specified file, which improves the running performance of the UNM2000. The UNM2000 supports manual save and overflow save of performance data.

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

8.7.1 Setting the Overflow Save of Performance

When the performance overflow save task is set, the UNM2000 will regularly check whether the performance history data in the database have met the preset conditions. If yes, the UNM2000 will save the performance history data automatically. The saved performance history data will be deleted from the database.

Background Information

The default historical data overflow save task provided by the UNM2000 cannot be deleted. The user can modify the overflow save conditions of the corresponding task as required.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. Select **System**→**Save Data** in the main menu to open the **Save the Data** tab.
2. In the left pane, select **Save History Data**→**Overflow Saving**→**Save 15-Minute Performance History / Save 24-Hour Performance History** to view the existing overflow save task of performance history.
3. Select one of the following access methods to open the **Properties** of the corresponding overflow save task of performance history.

No.	Access Method
1	Double-click the corresponding overflow save task in the right pane.
2	Right-click the corresponding overflow save task in the right pane and select Attribute from the shortcut menu.
3	In the left pane, click  before Overflow Saving , right click Save 15-Minute Performance History Overflow / Save 24-Hour Performance History Overflow and select Attribute from the shortcut menu.

4. See Table 8-3 for setting the properties of the overflow save task.

Table 8-3 Description of the Performance Overflow Save Task Settings

Parameter		Description
Basic Information	Task name	The name of the overflow save task; read-only.
	Yes	Select this check box to start this task.
	Task type	The task execution cycle. The default setting is once every other day.
	Execution time	The execution time of the task.
	Begin Time	The start time of the task.
	End Time	The end time of the task.
Extend Information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the historical data meeting the overflow save conditions to a file. You can select to save the historical data as a CSV file to the server's hard disk or in the FTP server. ◆ Select Delete and the historical data meeting the overflow save conditions are deleted directly.
	Overflow Border	The preset save proportion of the database when the save task is carried out as soon as the historical data have exceeded the maximum storage entry quantity or the threshold value.
	Capacity limit	The preset days of saving the historical data in the database when the save task is carried out.

5. After completing the settings, click **OK**.
6. Select the corresponding overflow save task in the left pane, and click **Execute Now** in the upper right pane. The execution result is shown in the lower right pane.

8.7.2 Setting the Manual Save of Performance

The UNM2000 supports manual save of historical alarm / event data to avoid insufficient database space.

Background Information

The default manual save task of historical alarm / event data provided by the UNM2000 cannot be deleted. The user can modify the manual save conditions of the corresponding task as required.

Procedures

1. Select **System**→**Save Data** in the main menu to open the **Save the Data** tab.
2. In the left pane, select **Save History Data**→**Save Manually**→**Save 15-Minute Performance History / Save 24-Hour Performance History** to view the existing manual save task of performance history.
3. Select one of the following access methods to open the **Properties** of the corresponding manual save task of performance history.

No.	Access Method
1	Double-click the corresponding manual save task in the right pane.
2	Right-click the corresponding manual save task in the right pane and select Properties .
3	In the left pane, click <input type="checkbox"/> next to the Manual Dump , right-click the corresponding manual save task in the right pane and select Properties .

4. See Table 8-4 for setting the properties of the overflow save task.

Table 8-4 Descriptions of the Performance Manual Save Task Settings

Parameter		Description
Basic Information	Task name	The name of the overflow save task; read-only.
	Yes	Select this check box to start this task.
	Task type	The task execution cycle. The default setting is once every other day.
	Execution time	The execution time of the task.
	Begin Time	The start time of the task.
	End Time	The end time of the task.
Extend Information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the historical data meeting the overflow save conditions to a file. You can select to save the historical data as a CSV file to the server's hard disk or in the FTP server. ◆ Select Delete and the historical data meeting the overflow save conditions are deleted directly.
	Overflow Border	The preset save proportion of the database when the save task is carried out as soon as the historical data have exceeded the maximum storage entry quantity or the threshold value.
	Capacity limit	The preset days of saving the historical data in the database when the save task is carried out.

5. Select the corresponding manual save task in the left pane, and click **Execute now** in the upper right pane. The execution result is shown in the lower right pane.

8.7.3 Gathering Statistics of PON Traffic

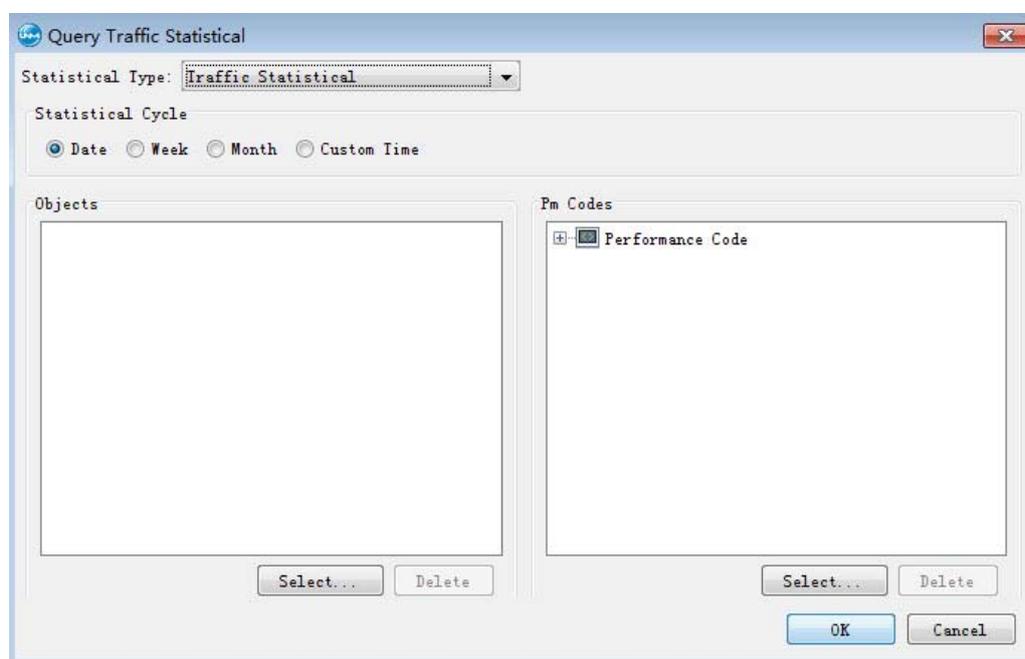
The PON traffic statistics and analysis function supports analyzing traffic, optical power and device health. It provides abundant reports for analyzing and monitoring services and device running status so as to provide detailed data for network planning.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

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 Setting the FTP Reporting Switch

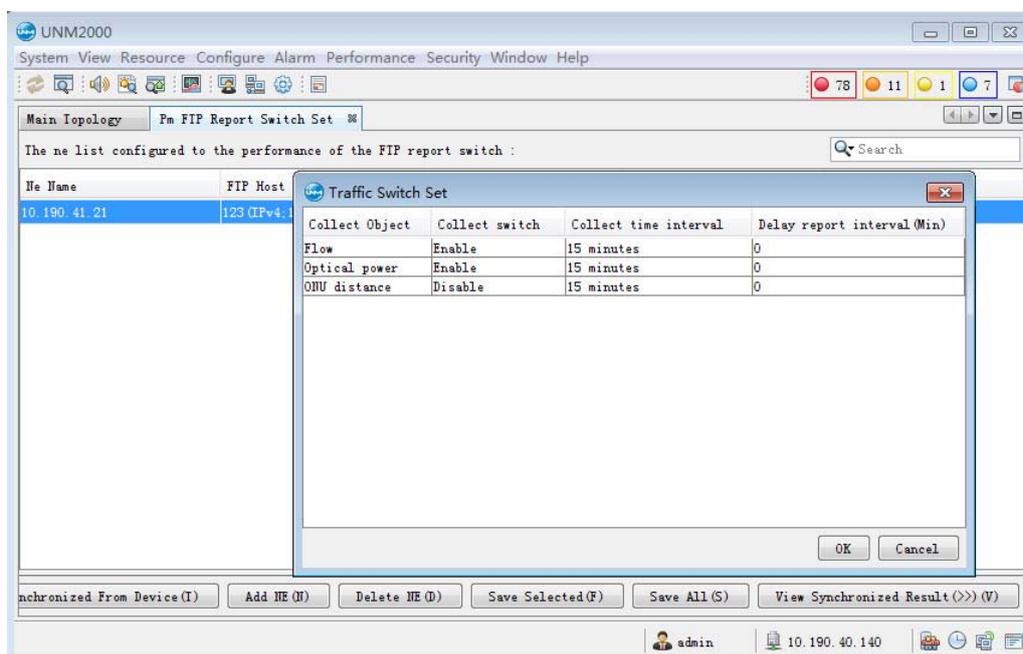
When the FTP reporting function is enabled, PON traffic data will be collected to a specified FTP server for you to view and back up.

Prerequisite

- ◆ The FTP server is set (Click SystemParameter Settings and then select Service ConfigurationFTP Server Setting).
- ◆ You have the authorities of **Inspector Group** or higher authorities.

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 an NE in the list and the buttons at the lower part of the tab to perform the corresponding operations, such as **Delete NE**.

Subsequent Operation

After enabling the FTP reporting function, create the performance collection task to collect the traffic, optical power or ONU test distance performance data. The following introduces how to collect the PON traffic data.

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.

The screenshot shows the 'Create Collection Task' dialog box with the following configuration:

- Task Name: Test
- NE Type: AN5516_01B
- Task Type: Collect Performance Data
- Data Type: 15-Minute Performance, 24-Hour Performance
- Enable Or Not: Yes (I), No (U)
- PON traffic Collection(): Yes, No
- Object Expand Level: Expand To Olt, Expand To Ont Port
- Remarks: (empty text box)

Buttons at the bottom: Copy from Other Collection Task..., OK, Create (N), Close.

4. Click **Create** to complete the settings.

8.7.5 Top Rank Statistics

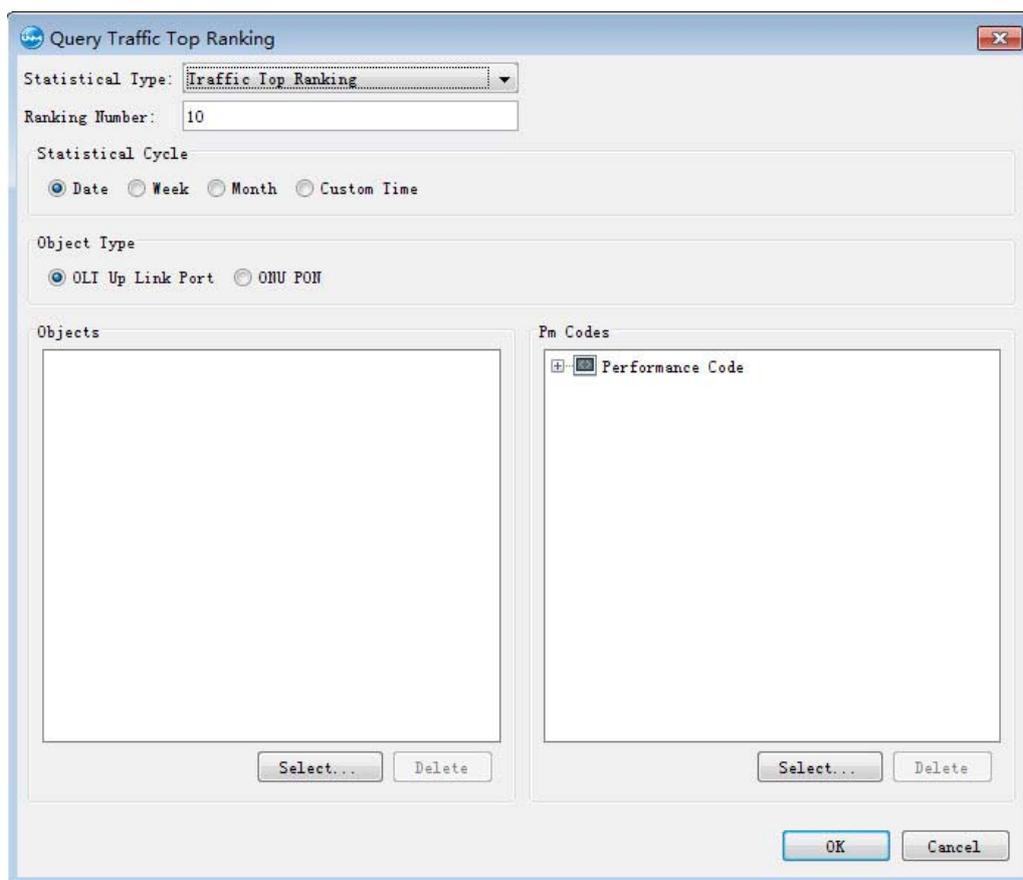
The **Top rank statistics** function supports PON traffic ranking and device health ranking so as to provide professional and abundant reports.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. Select **Performance** → **Top rank statistics** from the main menu to open the **Query Traffic Top Ranking** dialog box.



2. 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.

9 Log Management

The logs record the information on operations in the network management system and key events in the system. Via the log management function, users can query and output the logs.

- Log Management Policy
- Log Types
- Log Statistics
- Managing System Logs
- Managing Operation Logs
- Managing Security Logs
- Managing TL1 Command Logs
- Managing Log Data

9.1 Log Management Policy

The log security management includes managing the UNM2000 system logs, UNM2000 operation logs, UNM2000 security logs, TL1 command logs, log saving and log forwarding.

UNM2000 System 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.

UNM2000 Operation Logs

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.

UNM2000 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 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.

TL1 Command Logs

The TL1 command logs record the operations performed on the devices by users in the UNM2000 via the TL1 commands. By viewing the TL1 command logs, you can understand the TL1 command operations performed on the devices so as to obtain the running status of the devices.

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.

9.2 Log Types

The types of the UNM2000 logs include system logs, operation logs, security logs and TL1 command logs.

9.2.1 System Logs

The 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 saved in the database and can be queried through the client end.

Meaning of Logs

The system logs record the operations performed by the UNM2000 automatically. For example, executing scheduled tasks or system tasks.

Description of Log Parameters

Parameter	Description
Danger Level	The level of the risk that the operation may cause to the UNM2000. The risk levels include Prompt , General and Danger .
Source	The module that executes the operation.

Parameter	Description
Time	The specific execution time of the operation.
Operation Terminal	The terminal that executes the operation.
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 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 saved in the database and can be queried through the client end.

Meaning of Logs

The operation logs record all the operations performed at the UNM2000 client end except the operations that influence the security of the UNM2000. For example, creating logical domains, creating NEs and confirming alarms.

Description of Log Parameters

Parameter	Description
Operation Name	The name of the operation performed in the UNM2000.
Danger Level	The level of the risk that the operation may cause to the UNM2000. The risk levels include Prompt , General and Danger .
Username	The name of the user who performed the operation.
Login Mode	The login mode of the user who performed the operation. The login modes include Login to NMS and Login to Northbound Interface .

Parameter	Description
User Type	The type of the UNM2000 user who performs the operation.
Operation Time	The specific execution time of the operation.
Operation Terminal	The IP address of the terminal used for operation execution.
Operation Object	The execution object of the operation.
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.

9.2.3 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 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.

The security logs are saved in the database and can be queried through the client end.

Meaning of Logs

The security logs record all 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	Description
Security Event	The operation related to security.
Danger Level	The level of the risk that the operation may cause to the UNM2000. The risk levels include Prompt , General and Danger .
Username	The name of the user who performed the operation.
Login Mode	The login mode of the user who performed the operation. The login modes include Login to NMS and Login to Northbound Interface .
User Type	The type of the UNM2000 user who performs the operation.
Operation Time	The specific execution time of the operation.
Operation Terminal	The IP address of the terminal used for operation execution.
Operation Object	The execution object of the operation.
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.

9.2.4 TL1 Command Logs

The TL1 command logs record the operations performed on the devices by users in the UNM2000 via the TL1 commands. By viewing the TL1 command logs, you can understand the TL1 command operations performed on the devices so as to obtain the running status of the devices.

Meaning of Logs

The TL1 command logs record the operations performed on the devices by users in the UNM2000 via the TL1 commands.

Description of Log Parameters

Parameter	Description
NE IP Address	The IP address for running the TL1 commands.
Operation Object	The execution object of the operation.
Operation Name	The name of the operation performed on the NE.
Deliver Command	The TL1 command issued to the NE.
Operation Result	<p>Operation results include Succeeded, Failed and Unknown.</p> <ul style="list-style-type: none"> ◆ Succeeded: Indicates the operation is successful and all the operation results are returned. ◆ Failed: Indicates the operation failed. ◆ Unknown: Indicates the result of the operation is unknown.
Begin Time	The start time for executing the TL1 command.
End Time	The end time for executing the TL1 command.
Details	The details of the TL1 command.

9.3 Log Statistics

The UNM2000 new function, **Log Statistics**, includes **Statistical System Logs**, **Statistical Operation Logs**, **Statistical Security Logs** and **Statistical TL1 Command Logs**.

Statistical System Logs

- ◆ **Access Method**: On the UNM2000 main menu, click **Security**→**Statistical System Logs**.
- ◆ **Function Overview**: You can gather statistics of and analyze the system logs by setting **System Log Statistical Conditions** and **Query Conditions** so as to quickly understand the system service operation information.

Gathering Statistics of Operation Logs

- ◆ **Access Method**: On the UNM2000 main menu, click **Security**→**Statistical Operation Logs**.

- ◆ **Function Overview:** You can gather statistics of and analyze the operation logs by setting **Operation Log Statistical Conditions** and **Query Conditions** so as to quickly understand the operations performed by users in the UNM2000.

Gathering Statistics of Security Logs

- ◆ **Access Method:** On the UNM2000 main menu, click **Security**→**Statistical Security Logs**.
- ◆ **Function Overview:** You can gather statistics of and analyze the security logs by setting **Security Log Statistical Conditions** and **Query Conditions** so as to quickly understand the operations performed by users that may influence the security of the UNM2000.

Gathering Statistics of TL1 Command Logs

- ◆ **Access Method:** On the UNM2000 main menu, click **Security**→**Statistical TL1 Command Logs**.
- ◆ **Function Overview:** You can gather statistics of and analyze the TL1 command logs by setting **TL1 Command Log Statistical Conditions** and **Query Conditions** so as to quickly understand the TL1 relevant operations performed by users.

9.4 Managing System Logs

The system logs record the information on the operations performed by the UNM2000 automatically, so as to obtain the operating status of the UNM2000 easily. The following introduces how to manage the system log templates and query the system logs.

9.4.1 Managing System Log Templates

To conveniently and quickly query the system logs, you can set the most concerned system log types as a query template.

Prerequisite

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

Procedure

1. In the main menu, select **Security** → **Search the System Logs**.
2. In the **System Logs** tab, click **Query** to open the **Query System Logs** dialog box.
3. See Table 9-1 to set the query conditions as needed.

Table 9-1 Description of the Parameters in the **Query System Logs** Dialog Box

Parameter	Description	How to Set
Source Info	Selects the query objects of the system logs.	Select Source and click  to select the desired system from the Select Source dialog box. Note: ◆ By default, the system logs of all users will be queried.
Operation Result	Queries the operation logs by the operation result.	Select one or more options under Operation Result . All options are selected by default.
Danger Level	Queries the operation logs by risk level.	Select one or more options under Danger Level . All options are selected by default.
Time Range	Sets the time range, in which the operation logs are to be queried. If the time range is not set, all the logs will be queried.	Check the Start Time and End Time options and then set the specific time in the corresponding textboxes respectively.
Details contain	Filters the operation logs by the information entered in the Details contain textbox.	Check Details contain and enter the included fields in the textbox.

4. Click **Save as Template** to complete setting the system log query template.

Other Operations

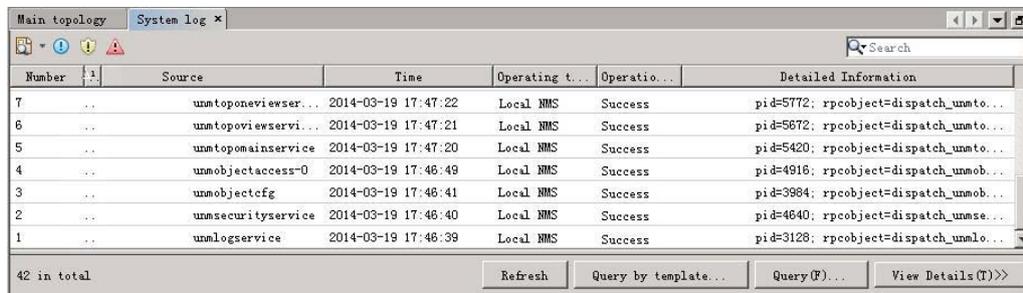
In the **System Logs** tab, right-click an entry and select **Template Management** from the shortcut menu to edit or delete the existing log templates.

9.4.2 Querying System Logs

The system logs record the information on the operations performed by the UNM2000 automatically, so as to obtain the operating status of the UNM2000 easily.

Procedure

1. In the main menu, select **Security** → **Search the System Logs**.
2. In the **System Logs** tab, view the query result. The system displays the system logs of the current day by default.



Number	Source	Time	Operating t...	Operatio...	Detailed Information
7	unmtoponeviewer...	2014-03-19 17:47:22	Local NMS	Success	pid=5772; rpcobject=dispatch_unmto...
6	unmtopoviewservi...	2014-03-19 17:47:21	Local NMS	Success	pid=5672; rpcobject=dispatch_unmto...
5	unmtopomainservice	2014-03-19 17:47:20	Local NMS	Success	pid=5420; rpcobject=dispatch_unmto...
4	unmobjectaccess=0	2014-03-19 17:46:49	Local NMS	Success	pid=4916; rpcobject=dispatch_unmob...
3	unmobjectcfg	2014-03-19 17:46:41	Local NMS	Success	pid=3984; rpcobject=dispatch_unmob...
2	unmsecurityservice	2014-03-19 17:46:40	Local NMS	Success	pid=4640; rpcobject=dispatch_unmse...
1	unmlogservice	2014-03-19 17:46:39	Local NMS	Success	pid=3128; rpcobject=dispatch_unmalo...

42 in total

Refresh Query by template... Query (F)... View Details (T)>>

3. In the **System Logs** tab, double-click the desired system log to view the log details.



Note:

Click the column heading of the query result to sort the result.

Other Operations

◆ Buttons

- ▶ Refresh: Obtains the latest data from the server end database and displays them in the client.
- ▶ Query According to Template: Selects an existing template to query the logs matching the condition preset in the template.
- ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing System Log Templates](#).
- ▶ View / Hide Details: Displays / hides the details pane of the selected log.

- ◆ **Shortcut Menus**

Right-click in the **System Logs** dialog box to open the shortcut menu, which is described as follows:

- ◆ **Query:** Sets the query condition to view the query result.
- ◆ **Refresh:** Obtains the latest data from the server end database and displays them in the client.
- ◆ **Template management:** Manages the log query templates or edits / deletes the existing log query template.
- ◆ **Copy Cell:** Edits / deletes the existing log template.
- ◆ **Print:** Prints out the operation logs.
- ◆ **Export All Records:** Exports all the operation logs as a TXT, XLS, CSV or HTML file to the specified directory.
- ◆ **Export Selected Record:** Exports the selected operation logs as a TXT, XLS, CSV or HTML file to the specified directory.

9.5 Managing Operation Logs

The operation logs record the information on the user operations, so as to monitor and check the user operations easily. The following introduces how to manage the operation log templates and query the operation logs.

9.5.1 Managing Operation Log Templates

To conveniently and quickly query the UNM2000 user operation logs, you can set the most concerned operation log types as a query template.

Prerequisite

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

Procedure

1. In the main menu, select **Security**→**Query Operation Logs**.

2. In the **Operation Logs** tab, click **Query** to open the **Query Operation Logs** dialog box.
3. See Table 9-2 to set the query conditions as needed.

Table 9-2 Description of the Parameters in the **Query Operation Logs** Dialog Box

Parameter		Description	How to Set
User Info	User-name	Selects the user, of whom the operation logs are to be queried.	Select the Username option and click  to select the desired user from the Select User dialog box. Note: <ul style="list-style-type: none"> ◆ By default, the operation logs of all users will be queried. ◆ The Select User dialog box only displays the users once logged into the UNM2000 client and performed operations.
	Operation Terminal	Select the operation terminal to query operation logs by operation terminal.	Select Operation Terminal and click  to select the desired operation terminal from the Select Operation Terminal dialog box. Note: By default, the operation logs of all terminals will be queried.
Operation Result		Queries the operation logs by the operation result.	Select one or more options under Operation Result . All options are selected by default.
Danger Level		Queries the operation logs by risk level.	Select one or more options under Danger Level . All options are selected by default.
Start Time Range		Sets the time range, in which the operation logs are to be queried. If the time range is not set, all the logs will be queried.	Check the Start Time and End Time options and then set the specific time in the corresponding textboxes respectively.
Details contain		Filters the operation logs by the information entered in the Details contain textbox.	Check Details contain and enter the included fields in the textbox.

Table 9-2 Description of the Parameters in the **Query Operation Logs** Dialog Box
(Continued)

Parameter	Description	How to Set
Select Operation Name	Selects 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.
Select Operation Object	Selects the operation objects to be queried.	Click Select under the Operation Object box and select the desired operation object from 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 an entry and select **Template Management** from the shortcut menu to edit or delete the existing log templates.

9.5.2 Querying Operation Logs

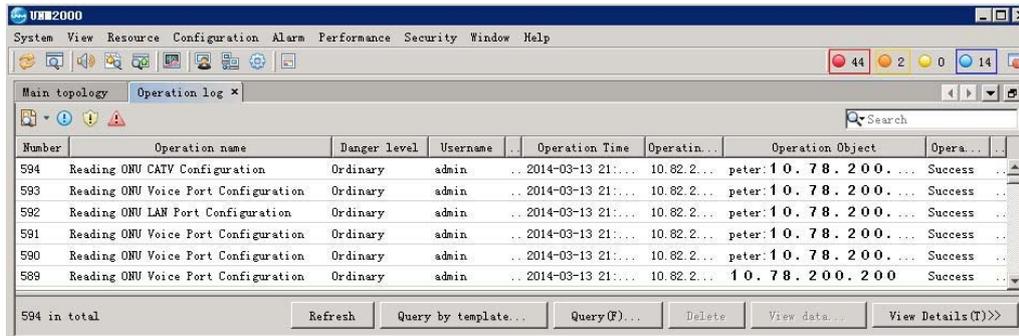
The operation logs record the information on the user operations, so as to monitor and check the user operations easily.

Background Information

- ◆ If you filter operation logs by user name, the **Unselected Value Filter** in the **Select User** dialog box only displays the names of the users that performed operations.
- ◆ The authorities of browsing operation logs for users of different roles are described as follows:
 - ▶ The users in the **Administrators** group can view the operation logs of all users.
 - ▶ Given the **Querying Operation Logs** authorities, the users in the **Security Administrator Group** can view the operation logs of all users.
 - ▶ Given the “Querying Operation Logs” authorities, the users neither in the “Administrators” group nor in the **Security Administrator Group** can only view the operations of themselves.

Procedure

1. In the main menu, select **Security**→**Query operational log...**
2. In the **Operation Logs** tab, view the query result. The system displays the operation logs of the current day by default.



The screenshot shows the UNM2000 interface with the 'Operation log' tab selected. The table displays the following data:

Number	Operation name	Danger level	Username	Operation Time	Operatin...	Operation Object	Opera...
594	Reading ONU CATV Configuration	Ordinary	admin	.. 2014-03-13 21:...	10.82.2...	peter:10.78.200....	Success ..
593	Reading ONU Voice Port Configuration	Ordinary	admin	.. 2014-03-13 21:...	10.82.2...	peter:10.78.200....	Success ..
592	Reading ONU LAN Port Configuration	Ordinary	admin	.. 2014-03-13 21:...	10.82.2...	peter:10.78.200....	Success ..
591	Reading ONU Voice Port Configuration	Ordinary	admin	.. 2014-03-13 21:...	10.82.2...	peter:10.78.200....	Success ..
590	Reading ONU Voice Port Configuration	Ordinary	admin	.. 2014-03-13 21:...	10.82.2...	peter:10.78.200....	Success ..
589	Reading ONU Voice Port Configuration	Ordinary	admin	.. 2014-03-13 21:...	10.82.2...	10.78.200.200	Success ..

At the bottom of the table, it shows '594 in total' and several action buttons: Refresh, Query by template..., Query(F)..., Delete, View data..., and View Details(T)>>.

3. In the **Operation Logs** tab, double-click the desired operation log to view the log details.



Note:

Click the column heading of the query result to sort the result.

Other Operations

◆ Buttons

- ▶ Refresh: Obtains the latest data from the server end database and displays them in the client.
- ▶ Query According to Template: Selects an existing template to query the logs matching the condition preset in the template.
- ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing Operation Log Templates](#).
- ▶ Delete: Deletes the selected operation logs.
- ▶ View Data: Views the data recorded in the corresponding operation logs.



Note:

View data... is only available for the write-to-device operation logs of the service configuration.

- ▶ View / Hide Details: Displays / hides the details pane of the selected log.

◆ **Shortcut Menu**

Right-click in the **Operation Logs** dialog box to open the shortcut menu, which is described as follows:

- ◆ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing Operation Log Templates](#).
 - ◆ View Data: Views the data recorded in the corresponding operation logs.
-



Note:

View data... is only available for the write-to-device operation logs of the service configuration.

- ◆ Delete: Deletes the selected operation logs.
- ◆ Refresh: Obtains the latest data from the server end database and displays them in the client.
- ◆ Template management: Manages the log query templates or edits / deletes the existing log query template.
- ◆ Copy Cell: Edits / deletes the existing log template.
- ◆ Print: Prints out the operation logs.
- ◆ Export All Records: Exports all the operation logs as a TXT, XLS, CSV or HTML file to the specified directory.
- ◆ Export Selected Record: Exports the selected operation logs as a TXT, XLS, CSV or HTML file to the specified directory.

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 the security log templates and query the security logs.

9.6.1 Managing Security Log Templates

To conveniently and quickly query the UNM2000 security logs, you can set the most concerned security log types as a query template.

Prerequisite

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

Procedure

1. In the main menu, select **Security**→**Query Security Log**.
2. In the **Security Logs** tab, click **Query** to open the **Query Security Logs** dialog box.
3. See Table 9-3 to set the query conditions as needed.

Table 9-3 Description of the Parameters in the **Query Security Logs** Dialog Box

Parameter		Description	How to Set
User Info	User-name	Selects the user, of whom the security logs are to be queried.	Select the Username option and click  to select the desired user from the Select User dialog box. Note: <ul style="list-style-type: none"> ◆ By default, the security logs of all users will be queried. ◆ The Select User dialog box only displays the users once logged into the UNM2000 client.

Table 9-3 Description of the Parameters in the **Query Security Logs** Dialog Box (Continued)

Parameter		Description	How to Set
	Operation Terminal	Select the operation terminal to query security logs by operation terminal.	Select Operation Terminal and click  to select the desired operation terminal from the Select Operation Terminal dialog box. Note: By default, the security logs of all terminals will be queried.
Operation Result		Queries the security operation logs by the operation result.	Select one or more options under Operation Result . All options are selected by default.
Danger Level		Queries the security logs by risk level.	Select one or more options under Danger Level . All options are selected by default.
Start Time Range		Sets the time range, in which the security operation logs are to be queried. If the time range is not set, all the logs will be queried.	Check the Start Time and End Time options and then set the specific time in the corresponding textboxes respectively.
Details contain		Filters the operation logs by the information entered in the Details contain textbox.	Check Details contain and enter the included fields in the textbox.
Select Security Event		Selects the security events to be queried.	Click Select under the Security Event box and select the desired security event from the Select Security Event dialog box.
Select Operation Object		Selects the operation objects to be queried.	Click Select under the Operation Object box and select the desired operation object from the Select Operation Object dialog box.

- Click **Save as Template** to complete setting the security log query template.

Other Operations

In the **Security Logs** tab, right-click an entry and select **Template Management** from the shortcut menu to edit or delete the existing log templates.

9.6.2 Querying Security Logs

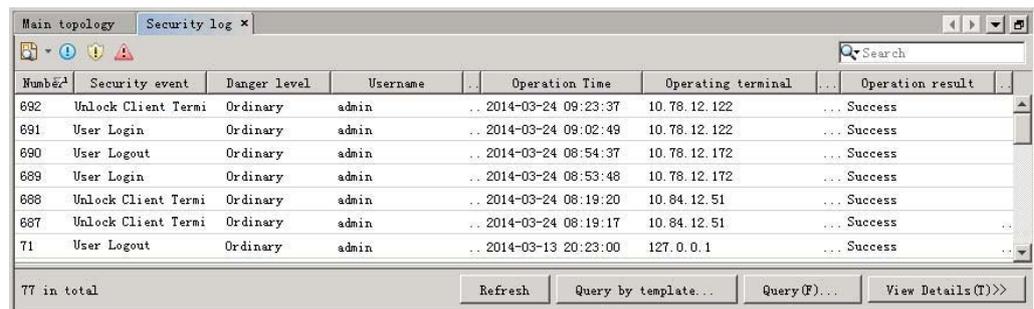
The security logs record the information on the security operations performed by the UNM2000. Querying security logs regularly helps ensuring the security of the network management system effectively.

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 Log**.
2. In the **Security Logs** tab, view the query result. The system displays the security logs of the current day by default.



Number	Security event	Danger level	Username	Operation Time	Operating terminal	Operation result
692	Unlock Client Termi	Ordinary	admin	.. 2014-03-24 09:23:37	10.78.12.122	... Success
691	User Login	Ordinary	admin	.. 2014-03-24 09:02:49	10.78.12.122	... Success
690	User Logout	Ordinary	admin	.. 2014-03-24 08:54:37	10.78.12.172	... Success
689	User Login	Ordinary	admin	.. 2014-03-24 08:53:48	10.78.12.172	... Success
688	Unlock Client Termi	Ordinary	admin	.. 2014-03-24 08:19:20	10.84.12.51	... Success
687	Unlock Client Termi	Ordinary	admin	.. 2014-03-24 08:19:17	10.84.12.51	... Success
71	User Logout	Ordinary	admin	.. 2014-03-13 20:23:00	127.0.0.1	... Success

77 in total

Refresh Query by template... Query (F)... View Details (T)>>

3. In the **Security Logs** tab, double-click the desired security log to view the log details.



Note:

Click the column heading of the query result to sort the result.

Other Operations

◆ Buttons

- ▶ Refresh: Obtains the latest data from the server end database and displays them in the client.

- ▶ Query According to Template: Selects an existing template to query the logs matching the condition preset in the template.
 - ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing Security Log Templates](#).
 - ▶ View / Hide Details: Displays / hides the details pane of the selected log.
- ◆ Shortcut menus

Right-click in the **Security Logs** dialog box to open the shortcut menu, which is described as follows:

- ▶ Query: Sets the query condition to view the query result. For the description of the query parameters, see [Managing Security Log Templates](#).
- ▶ Refresh: Obtains the latest data from the server end database and displays them in the client.
- ▶ Template management: Manages the log query templates or edits / deletes the existing log query template. See [Managing Security Log Templates](#).
- ▶ Copy Cell: Edits / deletes the existing log template.
- ▶ Print: Prints out the operation logs.
- ▶ Export All Records: Exports all the operation logs as a TXT, XLS, CSV or HTML file to the specified directory.
- ▶ Export Selected Record: Exports the selected operation logs as a TXT, XLS, CSV or HTML file to the specified directory.

9.7 Managing TL1 Command Logs

The TL1 command logs record the operations performed on the devices by users in the UNM2000 via the TL1 commands. By viewing the TL1 command logs, you can understand the TL1 command operations performed on the devices so as to obtain the running status of the devices. The following introduces how to manage the TL1 command log templates and query the TL1 command logs.

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 authorities of **Maintainer Group** or higher authorities.

Procedure

1. In the main menu, select **Security** → **View the TL1 Command Logs**.
2. In the **TL1 Logs** tab, click **Query** to open the **Query TL1 Command Logs** dialog box.
3. See Table 9-4 to set the query conditions as needed.

Table 9-4 Description of the Parameters in the **Query TL1 Command Logs** Dialog Box

Parameter	Description	How to Set
Operation Result	Queries the security operation logs by the operation result.	Select one or more options under Operation Result . All options are selected by default.
Start Time Range	Sets the time range, in which the security operation logs are to be queried. If the time range is not set, all the logs will be queried.	Check the Start Time and End Time options and then set the specific time in the corresponding textboxes respectively.
Details contain	Filters the operation logs by the information entered in the Details contain textbox.	Check Details contain and enter the included fields in the textbox.
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 Operation Object	Selects the operation objects to be queried.	Click Select under the Operation Object box and select the desired operation object from the Select Operation Object dialog box.

- Click **Save as Template** to complete setting the TL1 command log query template.

9.7.2 Querying TL1 Command Logs

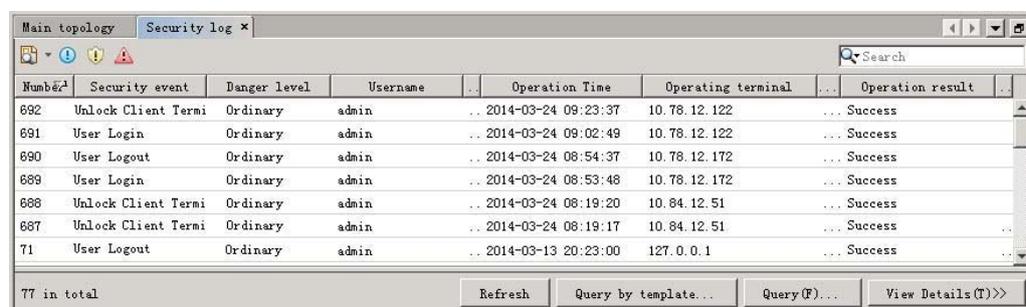
The TL1 command logs record the operations performed on the devices by users in the UNM2000 via the TL1 commands. By viewing the TL1 command logs, you can understand the operations performed on the devices by users via the TL1 commands so as to obtain the running information of the devices.

Prerequisite

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

Procedure

- In the main menu, select **Security**→**View the TL1 Command Logs**.
- In the **TL1 Logs** tab, view the query result. The system displays the security logs of the current day by default.



Number	Security event	Danger level	Username	Operation Time	Operating terminal	Operation result
692	Unlock Client Termi	Ordinary	admin	.. 2014-03-24 09:23:37	10.78.12.122	... Success
691	User Login	Ordinary	admin	.. 2014-03-24 09:02:49	10.78.12.122	... Success
690	User Logout	Ordinary	admin	.. 2014-03-24 08:54:37	10.78.12.172	... Success
689	User Login	Ordinary	admin	.. 2014-03-24 08:53:48	10.78.12.172	... Success
688	Unlock Client Termi	Ordinary	admin	.. 2014-03-24 08:19:20	10.84.12.51	... Success
687	Unlock Client Termi	Ordinary	admin	.. 2014-03-24 08:19:17	10.84.12.51	... Success
71	User Logout	Ordinary	admin	.. 2014-03-13 20:23:00	127.0.0.1	... Success

77 in total

Refresh Query by template... Query(F)... View Details(T)>>

- In the **TL1 Logs** tab, double-click the desired security log to view the log details.



Note:

Click the column heading of the query result to sort the result.

Other Operations

- ◆ Buttons

- ▶ Refresh: Obtains the latest data from the server end database and displays them in the client.
 - ▶ Query According to Template: Selects an existing template to query the logs matching the condition preset in the template.
 - ▶ 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 in the **TL1 Logs** dialog box to open the shortcut menu, which is described 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 server end database and displays them in the client.
- ▶ Template management: Manages the log query templates or edits / deletes the existing log query template. See [Managing TL1 Command Log Templates](#).
- ▶ Copy Cell: Edits / deletes the existing log template.
- ▶ Print: Prints out the operation logs.
- ▶ Export All Records: Exports all the operation logs as a TXT, XLS, CSV or HTML file to the specified directory.
- ▶ Export Selected Record: Exports the selected operation logs as a TXT, XLS, CSV or HTML file to the specified directory.

9.8 Managing Log Data

With the log saving function, the logs that are no longer needed can be deleted regularly or manually to avoid occupation of too many resources by the log information. The logs can also be exported as a file for you to view or isolate failures.

9.8.1 Managing the Log Forwarding Server

By setting the log forwarding server, users can forward the logs of the UNM2000 to other servers.

9.8.1.1 Viewing the Log Forwarding Server

View whether the log forwarding server meets the requirements.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. In the main menu, select **Security**→**Log Forwarding Server** to access the **Log Forwarding Server** tab, displaying the information of the current log forwarding server.
2. Click the buttons below the corresponding entry, or right-click the entry, and select operations such as **Modify**, **Start / Stop**, **Delete**, **Refresh**, **Copy Cell (K)**, **Print...**, or **Export**.

9.8.1.2 Adding a Log Forwarding Server

If the current log forwarding server cannot meet the requirements, you can add new log forwarding servers following the steps below.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. In the lower part of the **Log forwarding server** tab, click **Adding...** to open the **Log forwarding server** dialog box.
2. Set the parameters of the log forwarding server according to Table 9-5.

Table 9-5 Description on the Settings of the Log Forwarding Server

Parameter		Description
Server information	Server IP	Sets the IP address of the log forwarding server.
	Server port	Sets the port of the log forwarding server.
Protocol information	Protocol type	Sets the type of the transmission protocol. TCP and UDP can be selected, and the value should be consistent with the settings of the log forwarding server.
	Activate (U)	Selects whether to enable the server.
Log Information	Log level	<p>Sets the level of the log to be forwarded. The type is described as follows:</p> <ul style="list-style-type: none"> ◆ EMERG: The system is not available. ◆ ALERT: the event which must be handled at once. ◆ CRIT: the critical event. ◆ ERR: the error event. ◆ WARNING: the warning event. ◆ NOTICE: the common but important event. ◆ INFO: the useful information. ◆ DEBUG: the debug information.
	Log channel	<p>Sets the channel of the log to be forwarded. It should be consistent with the settings at the side of the log forwarding server. Its value includes:</p> <ul style="list-style-type: none"> ◆ KERN: the kernel log message. ◆ USER: the random user log message. ◆ MAIL: the mail system log message. ◆ DAEMON: the system daemon process log message. ◆ AUTH: the security management log message. ◆ SYSLOG: the log message of the log forwarding sever itself. ◆ LPR: the printer log message. ◆ NEWS: the news service log message. ◆ UUCP: the UUCP system log message. ◆ CRON: the CRON log message. ◆ AUTHPRIV: the private security management log message. ◆ FTP: the FTP daemon process log message. ◆ LOCAL0 to 7: reserved for local use.
	Log type	<p>Sets the type of the log to be forwarded. The type is described as follows:</p> <ul style="list-style-type: none"> ◆ System log ◆ NE log ◆ Security log ◆ Operation log

Table 9-5 Description on the Settings of the Log Forwarding Server (Continued)

Parameter		Description
Other Information	String filter	Sets the string. The log will be forwarded only when it complies with the string filtering conditions.
	Memo	Sets the remark information.

3. Click **OK**. The log forwarding server is added.

9.8.2 Setting the Overflow Save of Logs

When the alarm / event overflow save task is set, the UNM2000 will regularly check whether the alarm / event historical data in the database have met the preset conditions. If yes, the UNM2000 will save the alarm / event historical data automatically. The saved alarm / event history data will be deleted from the database.

Background Information

The default historical data overflow save task provided by the UNM2000 cannot be deleted. The user can modify the overflow save conditions of the corresponding task as required.

Prerequisite

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

Procedure

1. Select **System** → **Save Data** in the main menu to open the **Save the Data** tab.
2. In the left pane, select **Save History Data** → **Overflow Saving** → **Historical Overflow Save** to view the existing historical data overflow save task.
3. Select one of the following access methods to open the **Properties** of the corresponding overflow save task of alarm history.

No.	Access Method
1	Double-click the corresponding overflow save task in the right pane.
2	Right-click the corresponding overflow save task in the right pane and select Attribute from the shortcut menu.
3	In the left pane, click  next to the Overflow Saving , right-click the corresponding overflow save task and select Attribute from the shortcut menu.

4. See Table 9-6 for setting the properties of the overflow save task.

Table 9-6 Descriptions of the Overflow Save Task

Parameter		Description
Basic Information	Task name	The name of the overflow save task; read-only.
	Yes	Select this check box to start this task.
	Task type	The task execution cycle. The default setting is once every other day.
	Execution time	The execution time of the task.
	Begin Time	The start time of the task.
	End Time	The end time of the task.
Extend Information	Saving Mode	<ul style="list-style-type: none"> ◆ Select Save to File to save the historical data meeting the overflow save conditions to a file. You can select to save the historical data as a CSV file to the server's hard disk or in the FTP server. ◆ Select Delete and the historical data meeting the overflow save conditions are deleted directly.
	Overflow Border	The preset save proportion of the database when the save task is carried out as soon as the historical data have exceeded the maximum storage entry quantity or the threshold value.
	Capacity limit	The preset days of saving the historical data in the database when the save task is carried out.

5. After completing the settings, click **OK**.
6. Select the corresponding overflow save task in the left pane, and click **Execute Now** in the upper right pane. The execution result is shown in the lower right pane.

9.8.3 Setting the Manual Save of logs

The UNM2000 supports manual save of logs, so as to avoid capacity shortage of the database.

Background Information

The UNM2000 provides default manual save task of logs, which cannot be deleted. The user can modify the manual save conditions of the corresponding task as required.

Prerequisite

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

Procedure

1. Select **System**→**Save Data** in the main menu to open the **Save the Data** tab.
2. In the left pane, select **Save History Data**→**Save Manually**→**Save Log** to view the existing manual save task of logs.
3. Select one of the following access methods to open the **Properties** of the corresponding manual save task of data history.

No.	Access Method
1	Double-click the corresponding manual save task in the right pane.
2	Right-click the corresponding manual save task in the right pane and select Properties .
3	In the left pane, click  next to the Manual Dump , right-click the corresponding manual save task in the right pane and select Properties .

4. Modify the settings of the corresponding task as required in the **Properties** dialog box and click **OK**.
5. Select the corresponding manual save task in the left pane, and click **Execute now** in the upper right pane. The execution result is shown in the lower 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 and PON device capability.

- Managing Resource Statistical Templates
- 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
- Querying Cards by SN
- Querying the MDU Phone Number
- Querying the ONU RMS Error Information
- Querying the ONU Network Access Interception Logs

- Gateway Type Configuration
- Unauthorized ONU List
- Modifying ONU Names by Importing an Excel File

10.1 Managing Resource Statistical Templates

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, you can use the template directory without the need to set the conditions. The following introduces how to view the resource statistical templates already customized in the UNM2000.



Note:

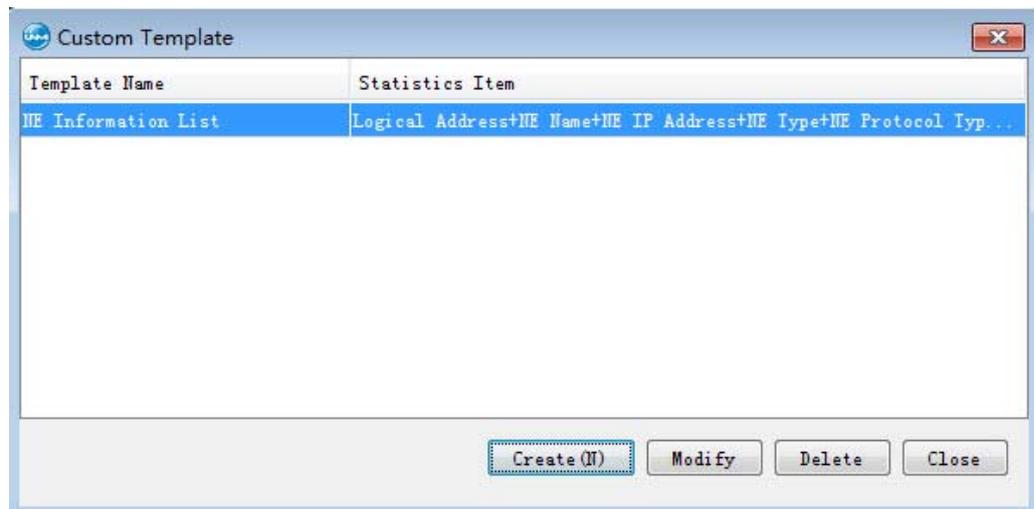
The following uses the NE resource statistical template as an example. You can follow the same procedures to view other templates with the only difference in the access method.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

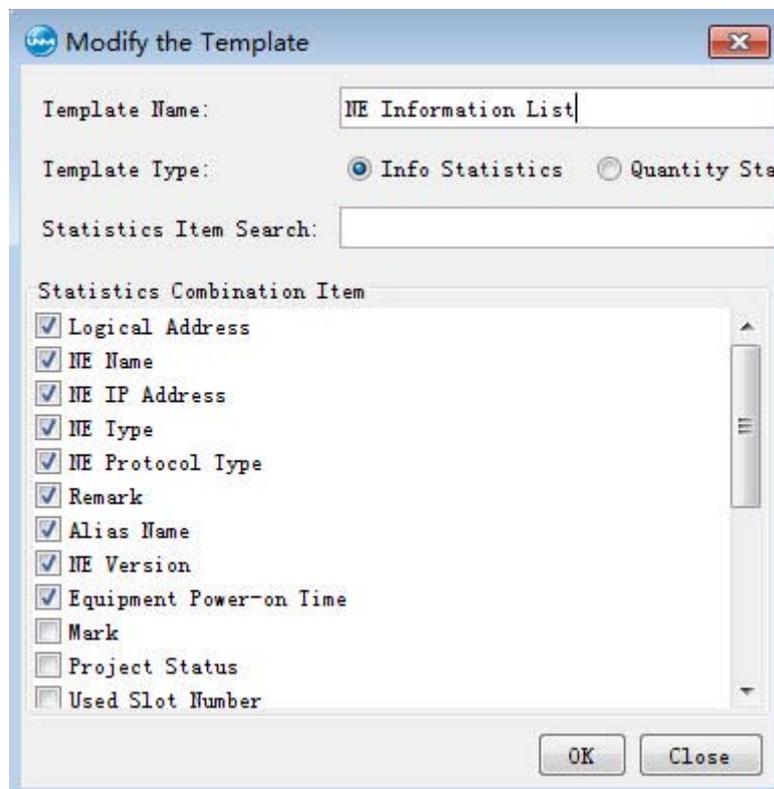
1. On the main menu select **Resources**→**Resource Statistics** and open the **Resource Statistics** tab.
2. In the left pane, Select **Resource Statistics**→**Physical Resource Statistics**→**NE Resource Statistics**.
3. In the **Statistical Template** drop-down list, select a statistical template.
4. Click **Custom** next to **Statistics Template** to open the **Custom Template** dialog box to view the existing statistical templates.



Other Operations

When the statistical items set in the template do not meet the requirements for resource statistics, you can modify the template.

1. Select the desired template entry, click **Modify** to open the **Modify the Template** dialog box.



2. Select the items according to the statistical range 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:

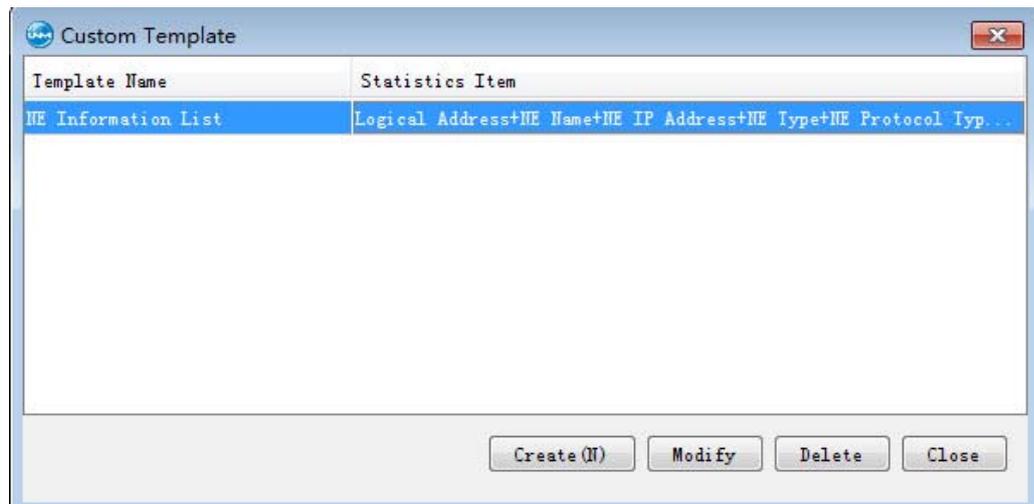
For **PON Device Capability Statistics**, only the default template can be used and no new one can be created.

Prerequisite

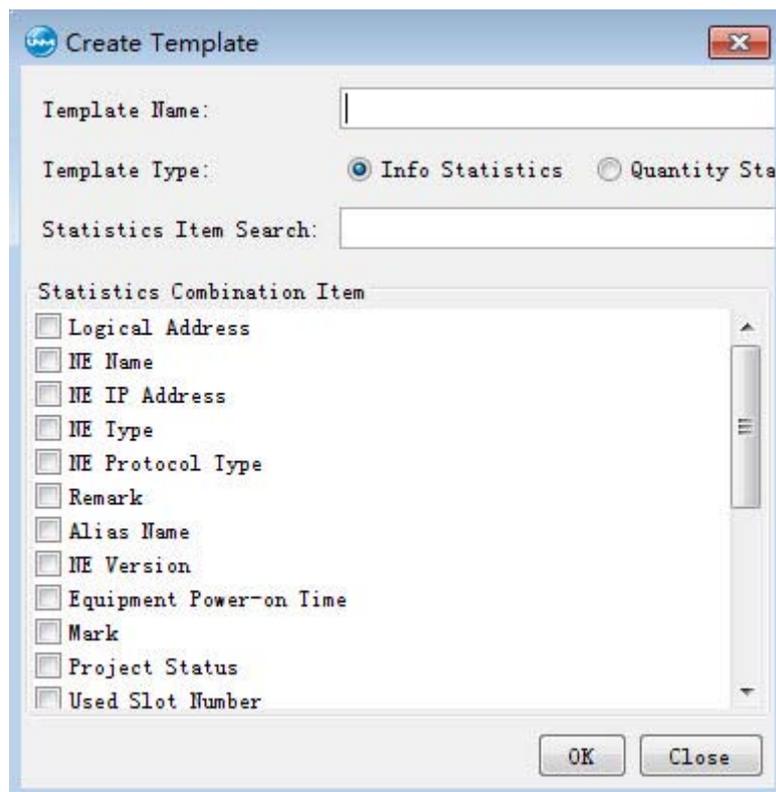
You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. On the main menu select **Resources**→**Resource Statistics** and open the **Resource Statistics** tab.
2. In the left pane, Select **Resource Statistics**→**Physical Resource Statistics**→**NE Resource Statistics**.
3. In the **Statistical Template** drop-down list, select a statistical template.
4. Click **Custom** next to **Statistics Template** to open the **Custom Template** dialog box to view the existing statistical templates.



- In the **Custom Template** dialog box, click **Create** to open the **Create Template** dialog box.



- 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

The user 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 authorities of **Inspector Group** or higher authorities.

Procedure

The procedures of gathering different physical resources are similar. The following uses the NE statistics as an example.

1. On the main menu select **Resources**→**Resource Statistics** and open the **Resource Statistics** tab.
2. In the left pane, Select **Resource Statistics**→**Physical Resource Statistics**→**NE Resource Statistics**.
3. In the **Statistical Template** drop-down list, select a statistical template.
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 address
peter	10.78.11.102	AN5116_02
peter	10.78.166.66	AN5516-01_GEPON
peter	10.78.188.198	AN5516-01_GEPON
peter	10.78.200.204	AN5006-20
peter	15	AN5006_15
peter	200	AN5516-01_GEPON
peter	30	AN5006-30
	5.5.5.5	AN5516_06_GEPON
Logical domain 1	a	AN5516-01_GEPON
Logical domain 1	b	VIRTUAL_NE
peter	test	AN5006-30

12 in total

statistical range... refresh stop

Other Operations

Right-click an entry in the statistical result and select **Copy the Cell**, **Print** or **Export** from the shortcut menu.

10.3 Resource Statistics of Other Types

Resource statistics of other types include statistics of ONU subscribers, local end VLANs, NE MGC services, ONU MGC services, device types, PON device capabilities, ONU WAN connection services, etc.



Note:

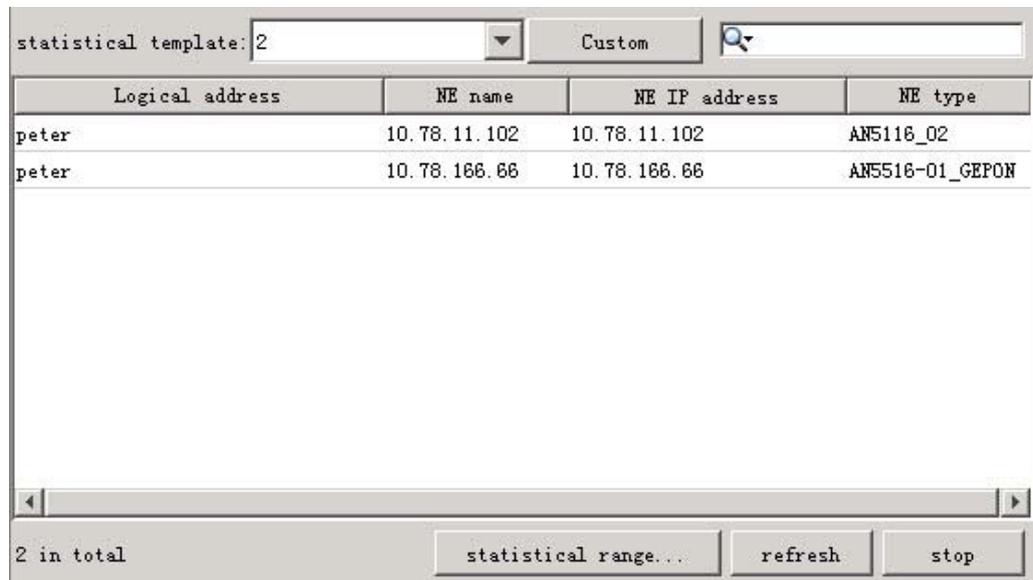
As the procedures for gathering statistics of resources of other types are similar, the following uses the ONU subscriber statistics as an example.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. On the main menu select **Resources**→**Resource Statistics** and open the **Resource Statistics** tab.
2. In the left navigation tree, select **Resource Statistics**→**Other Type Resource Statistics**→**ONU User Statistics**.
3. In the **statistical template** drop-down list, select a statistical template.
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
peter	10.78.11.102	10.78.11.102	AN5116_02
peter	10.78.166.66	10.78.166.66	AN5516-01_GEPON

Other Operations

Right-click an entry in the statistical result and select **Copy the Cell**, **Print** or **Export** from the shortcut menu.

10.4 Exporting Physical Resource Statistics

The user can export the physical resource statistical information to the configured FTP server as needed.

Background Information

The user can export physical resource statistical information, including NE resources, card resources, port resources, ONU resources, ONU port resources and MDU port resources.

Prerequisite

- ◆ The statistical template has been set. See [Customizing a Resource Statistical Template](#) for the setting method.
- ◆ The FTP server has been set. See [Setting the FTP Server](#) for the setting method.
- ◆ You have the authorities of **Inspector Group** or higher authorities.



Note:

The procedures of exporting different physical resource statistics are similar. In the following the NE resource statistics are exported as an example.

Procedure

1. On the main menu select **Resources**→**Resource Statistics** and open the **Resource Statistics** tab.
2. In the left navigation tree, select **Resource Export**→**Physical Resource Statistics**→**NE Resource Statistics** to view the existing export tasks.
3. Execute the following operations as required:
 - ▶ 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 when the execution result displays **Successful**.

- ▶ If the existing task has not met the requirements, → Step 4.
- 4. Add a physical resource statistical task.
 - 1) Right-click in the blank area of the GUI and select **Create** from the shortcut menu to open the **Add 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

Click a task and select the shortcut menus to delete, print, export or view the task.

10.5 Exporting Resource Statistics of Other Types

You can export statistical information of resources like the ONU subscribers, local end VLANs, MGC services, ONU MGC services, device types and ONU WAN connection services as needed.

Prerequisite

- ◆ The statistical template has been set. See [Customizing a Resource Statistical Template](#) for the setting method.
- ◆ The FTP server has been set. See [Setting the FTP Server](#) for the setting method.
- ◆ You have the authorities of **Inspector Group** or higher authorities.



Note:

The procedures of exporting resource statistics of other types are similar. In the following the ONU subscriber statistics are exported as an example.

Procedure

1. On the main menu select **Resources**→**Resource Statistics** and open 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 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

Click a task and select the shortcut menus to delete, print, export or view the task.

10.6 Example of Resource Statistics

The resource statistics of the UNM2000 can be used to manage the asset information of the devices in the entire network and important logical configuration information.

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 entire network timely via the resource management.

**Note:**

Taking the user preferences and use habit into consideration, the UNM2000 supports loading up to 20 thousand data entries and the excessive data will not be displayed. You can export the statistical records to view all the data.

Viewing the ONU Port Usage of a Specific NE

1. On the main menu, select **Resources** → **Resource Statistics**.
2. Select **Physical Resource Statistics** → **ONU Port Resource Statistics**.
3. Click **Custom** → **Create**. In the displayed **Create Template** dialog box, enter the template name, select template type and select the ONU port information entries to be included in the statistics. Then click **OK** to create the statistical template.

**Note:**

The template types are described as follows:

- ◆ **Info Statistics:** Gathers statistics of basic information of the statistical objects.
 - ◆ **Quantity Statistics:** Gathers quantity of types of the statistical objects.
-
4. Click **Statistics Range** to select the statistical object and then click **OK**.
 5. The **Resource Statistics** tab displays the ONU port usage set in the template.

Viewing the ONU Quantity of a Specified NE

1. On the main menu, select **Resources** → **Resource Statistics**.
2. Select **Physical Resource Statistics** → **ONU Resource Statistics**.
3. Click **Custom** → **Create**. In the displayed **Create Template** dialog box, enter the template name, select template type and select the ONU port information entries to be included in the statistics. Then click **OK** to create the statistical template.



Note:

The template types are described as follows:

- ◆ Info Statistics: Gathers statistics of basic information of the statistical objects.
 - ◆ Quantity Statistics: Gathers quantity of types of the statistical objects.
-
4. Click **Statistics Range** to select the statistical object and then click **OK**.
 5. The **Resource Statistics** tab displays the ONU quantity set in the template.

Viewing the VLAN Information

1. On the main menu, select **Resources**→**Resource Statistics**.
2. Select **Other Type Statistics**→**Local VLAN Statistics**.
3. Click **Custom**→**Create**. In the displayed **Create Template** dialog box, enter the template name, and select **Service Type**, **Service Name**, **Start VLAN** and **End VLAN**. Then click **OK** to create the statistical template.
4. Click **Statistics Range** to select the statistical object and then click **OK**.
5. The **Resource Statistics** tab displays the corresponding local end VLAN information.

10.7 Importing the ODN NSM Information

Creating the ODN view manually is inefficient and likely to generate errors. By importing the ODN NMS information, you can build the ODN network view quickly. After importing the information, the topology will display the relationship between NEs (OLT PON ports, splitters and ONUs), improving the maintenance efficiency.

Background Information

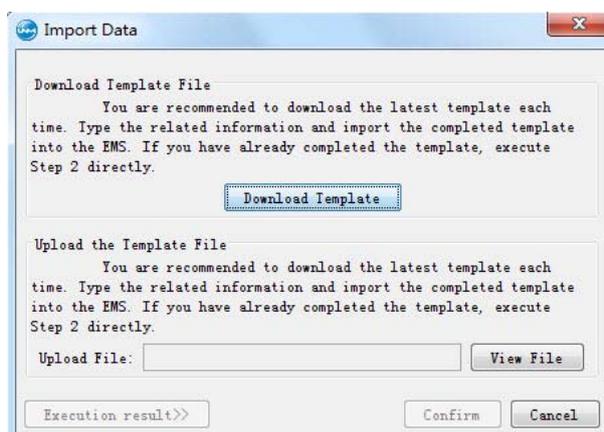
The ODN provides the optical transmission channel between the OLT and the ONU.

Prerequisite

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

Procedure

1. Select **Resource**→**Import ODN NMS Information** in the main menu.
2. Click **Open File** at the lower right corner of the window to open the **Import Data** window.



3. Click **Download Template** to save the ODN import information template to the local computer and enter the information according to the project requirement.



Note:

The items marked with an asterisk (*) are required. Either incorrect or missing input will lead to import failure.

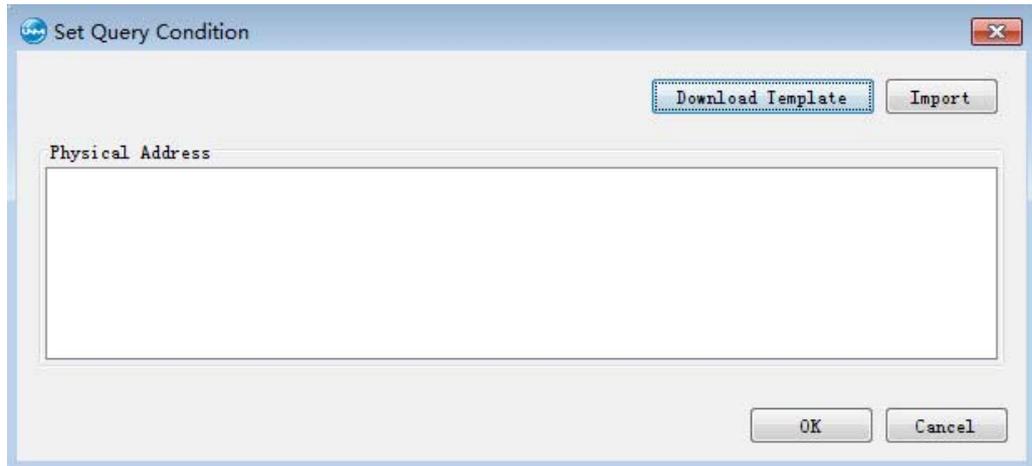
4. Click **View File** to select the file with ODN information entered, and then click **OK** to import the data.

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.

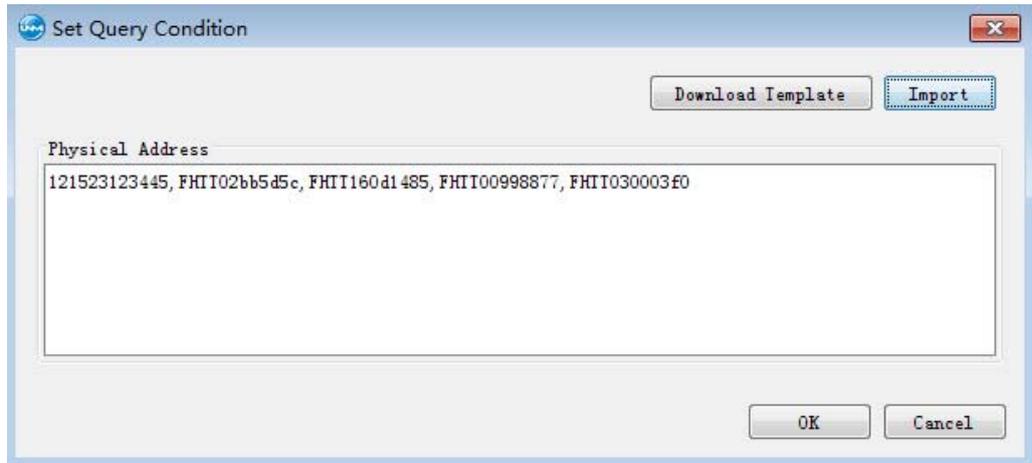


Note:

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.



- 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
PON[1]-ANS506-04-F1[33]	10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline
PON[1]-ANS506-04-F1[33]	10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline
PON[1]-ANS506-04-F1[33]	10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline
PON[1]-ANS506-04-F1[33]	10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline
PON[1]-ANS506-04-F1[33]	10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline
PON[1]-ANS506-04-F1[33]	10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline
PON[3]-ANS506-04-F1[1]	10.171.0.200	ANS506-04-F1	5	3	1	FHII030003f0	Online
PON[3]-ANS506-04-F1[1]	10.171.0.200	ANS506-04-F1	5	3	1	FHII030003f0	Online
PON[3]-ANS506-04-F1[1]	10.171.0.200	ANS506-04-F1	5	3	1	FHII030003f0	Online
PON[3]-ANS506-04-F1[1]	10.171.0.200	ANS506-04-F1	5	3	1	FHII030003f0	Online

- Select multiple entries in the query result list and right-click to select **ONU Deauthorization** to deauthorize multiple ONUs.

OLT IP	ONU Type	Slot Number	PON Number	ONU Number	Physical Address	Online Status	ONU Public IP
10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline	
10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline	
10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline	
10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline	
10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline	
10.171.0.200	ANS506-04-F1	5	1	33	FHII00998877	Offline	
10.171.0.200	ANS506-04-F1	5	3	1	FHII030003f0	Online	
10.171.0.200	ANS506-04-F1	5	3	1	FHII030003f0	Online	
10.171.0.200	ANS506-04-F1	5	3	1	FHII030003f0	Online	
10.171.0.200	ANS506-04-F1	5	3	1	FHII030003f0	Online	

Current Entry 1, selected 4 of 16 entries

10.9 Querying Cards by SN

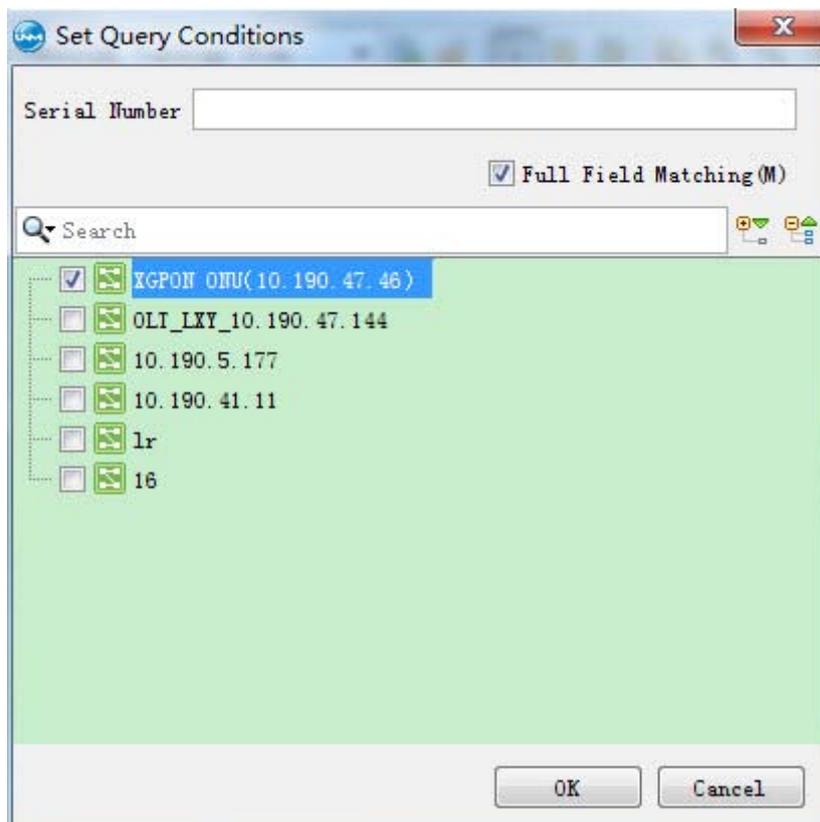
You can query the name and management IP address of the OLT where the card locates as well as the slot number of the card by serial number. You can query all OLT devices in the entire network.

Prerequisite

The SN 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 multiple OLT devices, as shown below:





Note:

- ◆ If you select **Full Field Matching**, enter the complete serial number of the card.
- ◆ If you do not select **Full Field Matching**, the fuzzy query is supported.

3. Click **OK**. The query result appears in the **Query Board by Serial Number**, as shown below:

NE Logic Address	NE Name	NE IP Address	Slot No	Board Type	Board Name	SN
OLT_LXY_10.190.47.144		10.190.47.144	3	GC8B	GC8B[3]	ABCDEFG1234567

10.10 Querying the MDU Phone Number

You can locate the corresponding card and port by the port phone number through the **Query MDU Phone Number** function. At present, it supports the SIP voice port query of the AN5006-20 and AN5006-30.

Prerequisite

The authority of the **Query MDU Phone Number** function has been assigned to you in the authority and domain division management.

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** (phone number of the port), as shown in Figure 10-1.

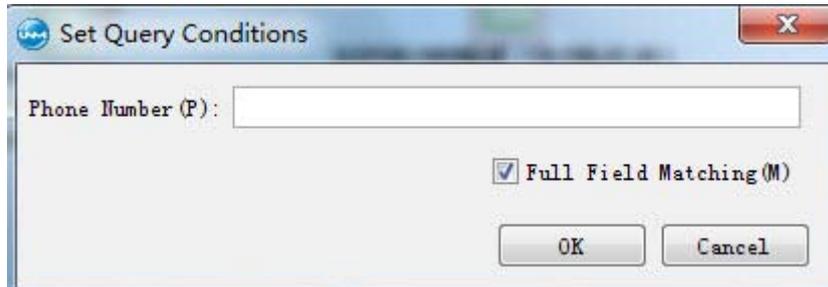


Figure 10-1 Setting the MDU Phone Number Query Conditions



Note:

- ◆ If you select **Full Field Matching**, enter the complete phone number.
- ◆ If you do not select **Full Field Matching**, the fuzzy query is supported.

3. Click **OK**. The query result appears in the **Query MDU Phone Number** tab, as shown in Figure 10-2.

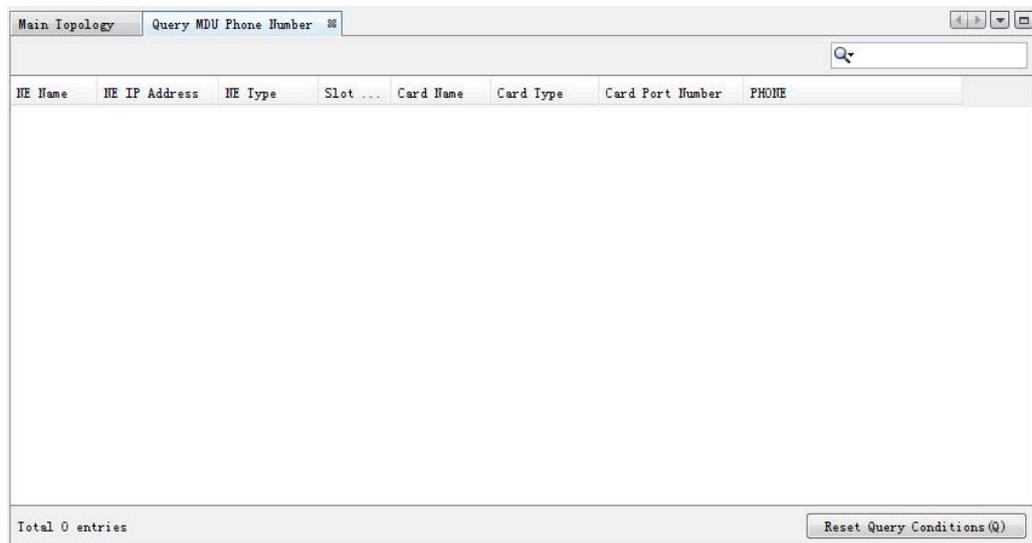


Figure 10-2 The Query MDU Phone Number Tab

10.11 Querying the ONU RMS Error Information

You can filter and query the ONU RMS failure information through the UNM2000 and print and export the content in the failure information table.

Prerequisite

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

Procedure

1. On the UNM2000 main menu, select **Resource**→**ONU RMS Error Information Query** to open the **Query ONU RMS Error Information** dialog box.

The screenshot shows a software dialog box titled "Query ONU RMS Error Information". It has two tabs: "Basic Information" (which is active) and "Advanced Information". Under "Basic Information", there are three main sections: 1. "Network Access Time Information" with "Start Date" (2016-08-02 14:35:16) and "End Date" (2016-08-09 14:35:16) fields, each with a calendar icon. 2. "Slot number and PON port number" with three input fields: "Slot Number:", "PON Number:", and "MDU ONU Slot Number:". Below these is a note: "Please enter a number or a number range separated by '-' or ','. For example, 1,3,7-10". 3. "MAC/SIN Information" with a "MAC/SIN:" input field and a note: "The physical address searching supports fuzzy matching (It only contains letters or numbers)...". At the bottom right, there are three buttons: "Reset", "OK", and "Close".

2. In the **ONU RMS Error Information** dialog box, set the query conditions, including **Basic Information** and **Advanced Information**.
3. Click **OK**. The **ONU RMS Error Information** tab lists the detailed failure information.

Other Operations

In the **ONU RMS Error Information** tab, right-click to **Print** or **Export** the selected entries.

10.12 Querying the ONU Network Access Interception Logs

You can filter and query the ONU network access interception logs through the UNM2000 and print and export the logs.

Prerequisite

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

Procedure

1. On the UNM2000 main menu, select **Resource**→**ONU Network Intercept Log Query** to open the **ONU Network Intercept Log Query** dialog box.

ONU Network Intercept Log Query

Basic Information | Advanced Information

Network Access Time Information

Start Date 2016-08-02 14:36:11 End Date 2016-08-09 14:36:11

Slot number and POH port number

Slot Number:

POH Number:

MDU ONU Slot Number:

Please enter a number or a number range separated by "-" or ",". For example, 1,3,7-10

MAC/SII Information

MAC/SII:

The physical address searching supports fuzzy matching (It only contains letters or numbers)...

Reset OK Close

2. In the **ONU Network Intercept Log Query** dialog box, set the query conditions, including **Basic Information** and **Advanced Information**.
3. Click **OK**. The **ONU Network Intercept Log** tab lists the log information.

Other Operations

In the **ONU Network Intercept Log Query** tab, right-click to **Print** or **Export** the selected entries.

10.13 Gateway Type Configuration

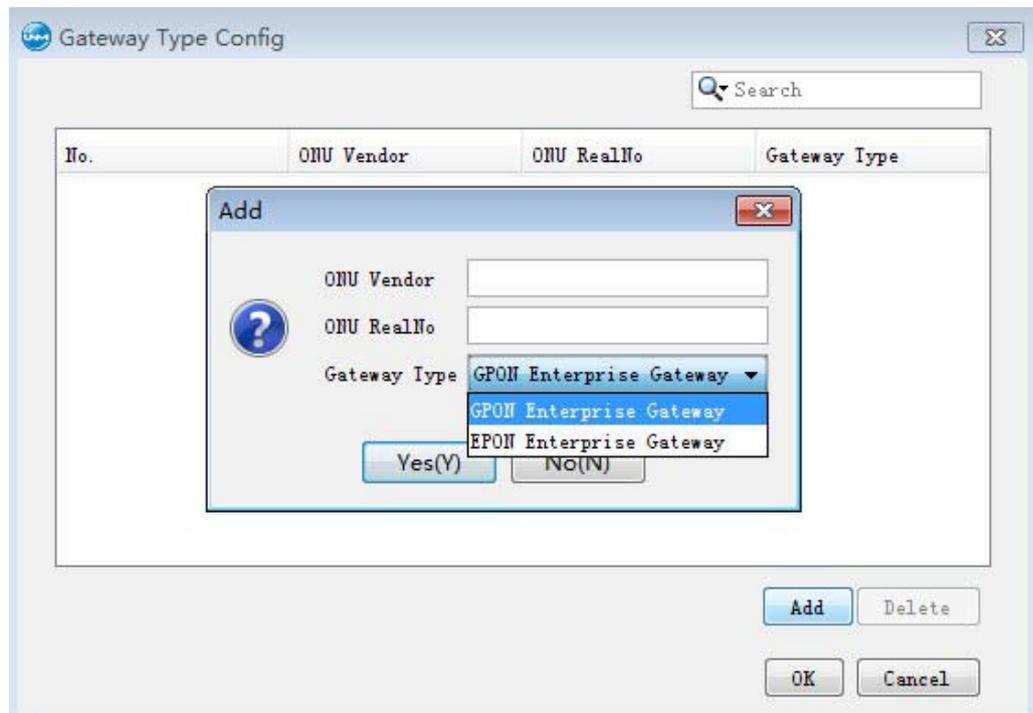
You can configure the gateway types, actual models and manufacturer names of ONU devices of different manufacturers so that the gateway types of the ONU devices can be identified when the resource management system delivers the network access configuration of enterprise gateway.

Prerequisite

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

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.

10.14 Unauthorized ONU List

You can obtain the information of all unauthorized ONUs under one or multiple OLTs through the UNM2000. The information of the unauthorized ONU includes the ONU slot number, PON port number, ONU physical address, logical ID and logical password.

Prerequisite

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

Procedure

1. Select **Resource**→**Unauthorized ONU List** from the UNM2000 main menu.
2. In the **Unauthorized ONU List** tab, click **Select the object**, as shown in Figure 10-3.

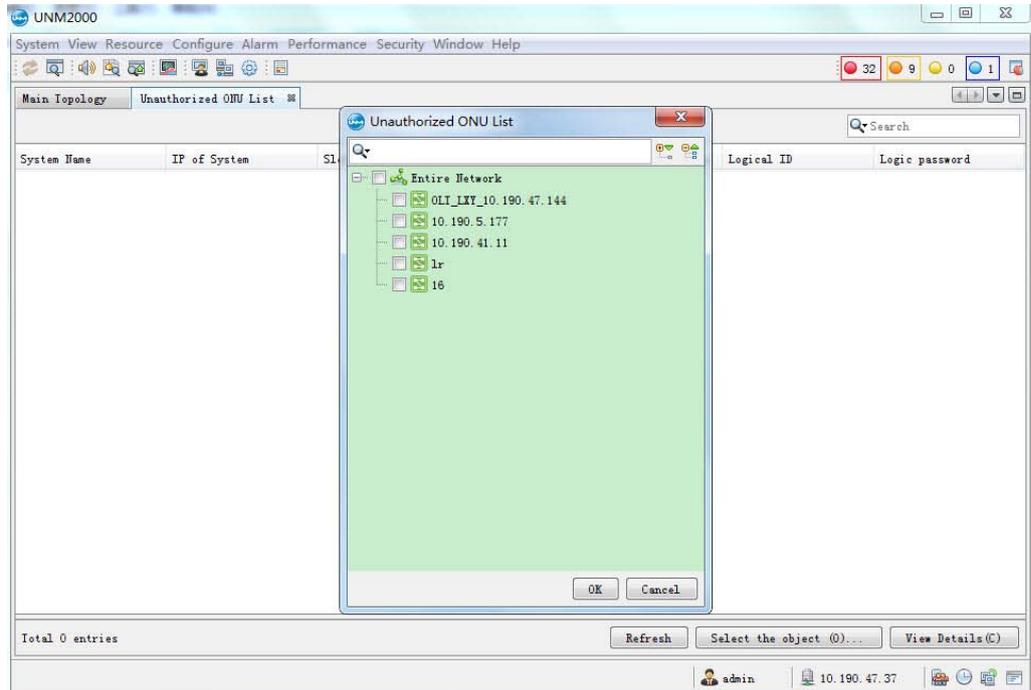


Figure 10-3 Unauthorized ONU List

3. In the **Unauthorized ONU List** dialog box, select the desired OLT and click **OK** to query the unauthorized ONUs.

10.15 Modifying ONU Names by Importing an Excel File

You can modify the names of ONUs in a batch manner by importing an Excel file.

Prerequisite

- ◆ The ONU names are planned.
- ◆ You have the authorities of **Operator Group** or higher authorities.

Procedure

1. Select **Resource**→**Modify ONU Names by Importing EXCEL** from the main menu.
2. Click **Open File** to open 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 data into the Excel file and save it.
5. Click **View File**, and select the configured Excel template to import it.
6. Click **OK** to write the data into the UNM2000.

11 Data Synchronization and Backup

In case multiple UNM2000 systems are used to manage NEs, modifying the NE configuring data in one of the UNM2000 will make the data in other UNM2000 inconsistent with the NE data. To ensure the consistency of the network data and NE data and the data security, the UNM2000 provides the data synchronization and backup.

- Managing Data Synchronization Tasks
- Data Backup

11.1 Managing Data Synchronization Tasks

Data synchronization refers to the synchronization of the equipment data with those in the UNM2000. Managing data synchronization tasks includes managing the software / hardware version update tasks, managing the configuration uploading tasks, and managing the NE automatic discovery task.

11.1.1 Managing Software / Hardware Version Update Tasks

The software / hardware version update refers to updating the software / hardware version of the equipment into the database of the network management system.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. In the left pane, select **Data Synchronization**→**Software and hardware version update task** to view the current software / hardware version update tasks.
3. Execute the following operations as required:
 - ▶ If the current tasks can meet the requirements, operate as follows: Right-click a task, and select **Execute now**, or select it and click the **Execute now** at the lower part of the tab to execute the software / hardware version update task.
 - ▶ Right-click the task, and perform the following operations: **Disabled (U)**, viewing and modifying **Properties**, etc.
4. Click a certain task in the left pane to view its object information, status, or failure cause.

11.1.2 Managing Configuration Uploading Tasks

In case of NE maintenance or NE upgrade / degrade, you need to back up the NE data to the UNM2000 server, client end or a third-party FTP server to avoid damage or loss of NE data caused by upgrade / degrade or accidental cause.

The configuration upload tasks can be used to upload the configuration data on the device to the UNM2000 database, ensuring the consistency of the data in the UNM2000 and the data on the device.

11.1.2.1 Viewing Configuration Uploading Tasks

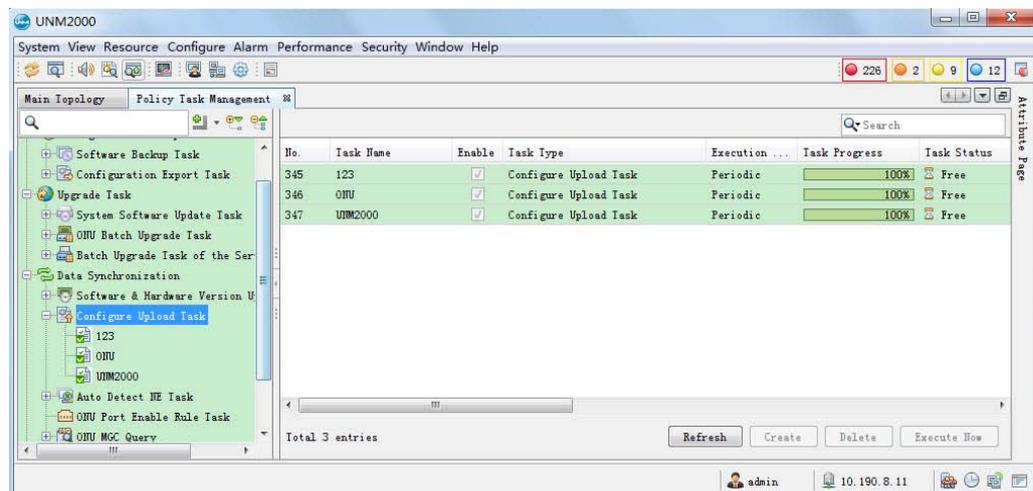
By viewing the configuration uploading tasks, you can check whether the execution time and object of the device configuration uploaded to the UNM2000 database meet the requirements for data synchronization.

Prerequisite

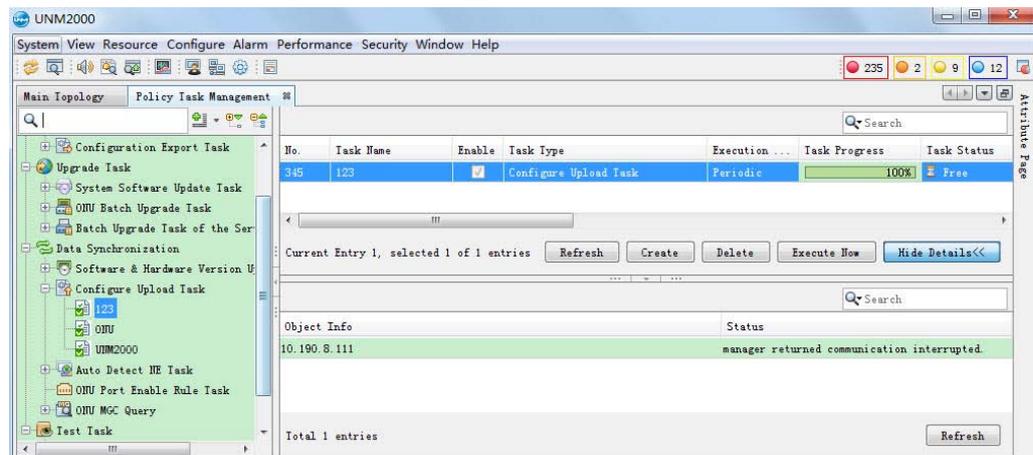
You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. In the left pane, select **Data Synchronization**→**Configure uploading task** to view the current configuration uploading tasks.



3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its object information and status.



Other Operations

In the right policy, right-click the desired task and select the corresponding shortcut menu to **Delete** / **Disabled** the task or view / modify **Properties**, etc.

11.1.2.2 Adding a Configuration Uploading Task

When the existing configuration uploading tasks do not meet the data synchronization requirements, you can create configuration export tasks according to your needs.

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. Right-click **Configure Upload Task** in the left pane or right-click in the right pane and select **Create** to open the dialog box.
3. Set the related parameters in the **Basic information** and **Object source** tabs, and click **OK** after completing the settings. Then the added tasks will be displayed in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name**: of other tasks. This can improve the setting efficiency.

- Click the desired task in the left pane to view its object information and status.

11.1.2.3 Executing a Configuration Uploading Task

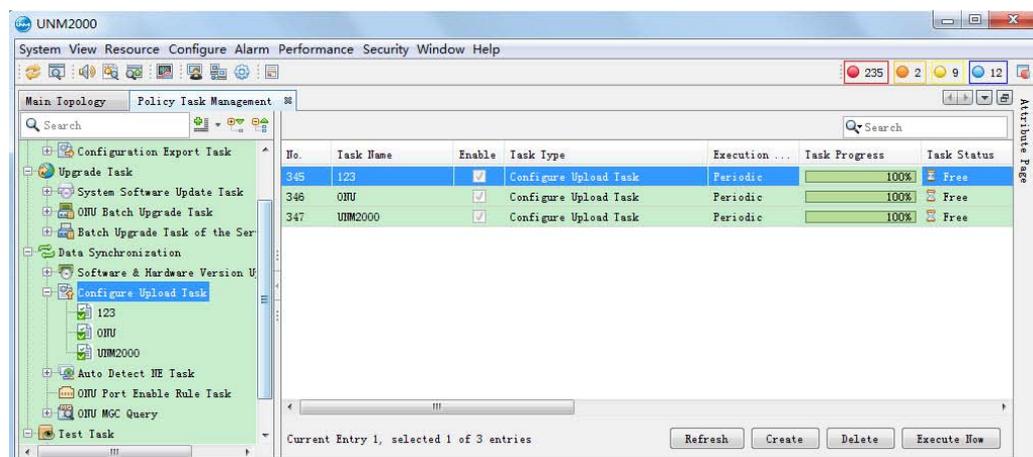
You can execute the configuration uploading tasks to timely synchronize the configuration data on the device to the UNM2000 database, so as to ensure the security and accuracy of the UNM2000 data.

Prerequisite

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

Procedure

- In the main menu, select **System** → **Policy Task Management** to open the **Policy Task Management** window.
- In the left pane, select **Data Synchronization** → **Configure uploading task** to view the current configuration uploading tasks.



3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its **Object Information** and **Status** and check whether the configuration uploading task meets your requirements.
4. Right-click the desired task and select **Execute Now**, or click the task and click **Execute Now** at the lower right corner of the tab to execute the configuration upload task.

11.2 Data Backup

To ensure the security of the NE data, you can back up the NE data and restore it when critical failures occur in the network. Managing configuration backup tasks includes managing the software backup tasks and managing the configuration exporting tasks.

11.2.1 Managing Software Backup Tasks

The following introduces how to view, create and execute the software backup tasks of the card.

11.2.1.1 Viewing Software Backup Tasks

The following introduces how to view the software backup tasks.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. In the left pane, select **Configuration Backup**→**Software Backup Task** to view the existing software backup tasks.
3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its object information and status.

Other Operations

In the right pane, right-click the desired task and select the corresponding shortcut menu to **Delete / Disabled** the task or view / modify **Properties**, etc.

11.2.1.2 Adding a Software Backup Task

When the existing software backup tasks do not meet the backup requirements, you can create software backup tasks according to your needs.

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** 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** after completing the settings. Then the added tasks will be displayed in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name**: of other tasks. This can improve the setting efficiency.

4. Click a certain task in the left pane, and users can view its object information and status.

11.2.1.3 Executing a Software Backup Task

The following introduces how to execute a software backup task.

Prerequisite

- ◆ The FTP server is configured. See [Setting the FTP Server](#).
- ◆ The file transmission service between the client end and the server end runs normally.
- ◆ You have the authorities of **Maintainer Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. In the left pane, select **Configuration Backup**→**Software Backup Task** to view the existing software backup tasks.
3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its **Object Information** and **Status** and check whether the software backup task meets your requirements.
4. Right-click the desired task and select **Execute Now**, or click 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

The following introduces how to view, add and execute the export tasks of data already backed up.

11.2.2.1 Viewing Configuration Export Tasks

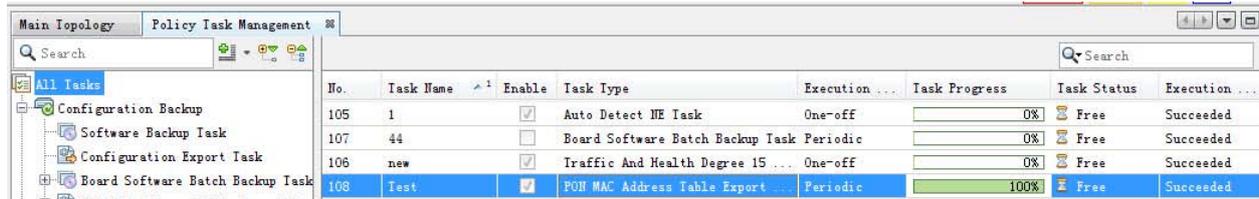
By viewing the configuration export tasks, you can confirm whether the exported data information should be saved to an external location.

Prerequisite

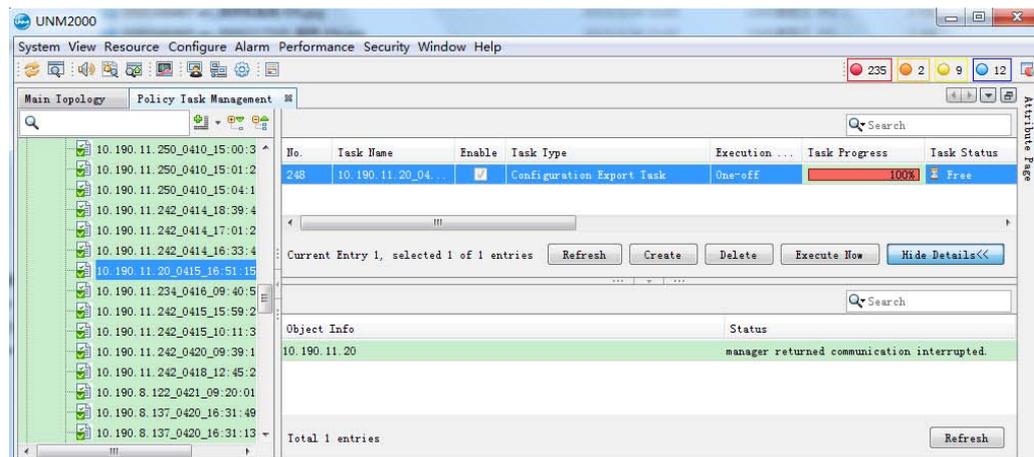
You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. In the left pane, select **Configuration Backup**→**Configuration Export Task** to view the existing configuration export tasks.



3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its object information and status.



Other Operations

In the right pane, right-click the desired task and select the corresponding shortcut menu to **Delete** / **Disabled** the task or view / modify **Properties**, etc.

11.2.2.2 Creating a Configuration Export Task

When the existing configuration export tasks do not meet the backup requirements, you can create configuration export tasks according to your needs.

Prerequisite

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

Procedure

1. In the main menu, select **System**→**Policy Task Management** 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** after completing the settings. Then the added tasks will be displayed in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name:** of other tasks. This can improve the setting efficiency.

4. Click a certain task in the left pane, and users can view its object information and status.

11.2.2.3 Executing a Configuration Export Task

The following introduces how to execute the configuration export task.

Prerequisite

- ◆ The FTP server is configured. See [Setting the FTP Server](#).
- ◆ The file transmission service between the client end and the server end runs normally.
- ◆ You have the authorities of **Maintainer Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.

2. In the left pane, select **Configuration Backup**→**Configuration Export Task** to view the existing configuration export tasks.
3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its **Object Information** and **Status** and check whether the configuration export task meets your requirements.
4. Right-click the desired task and select **Execute Now**, or click the task and click **Execute now** at the lower right corner of the tab to execute the configuration export task.

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 Software Backup Tasks

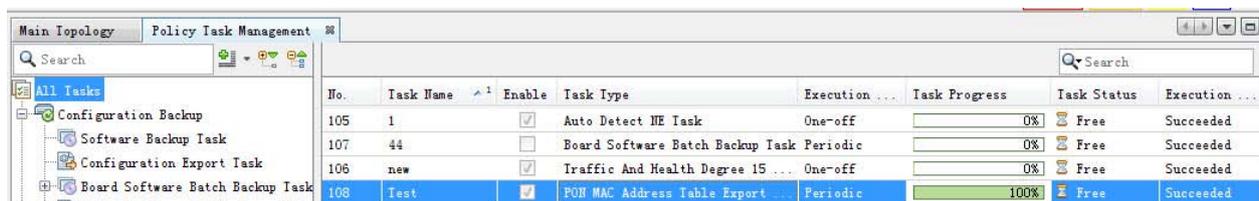
You can add or delete software backup tasks.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. In the left pane, select **Configuration Backup**→**Board Software Batch Backup Task** to view the existing configuration export tasks.



No.	Task Name	Enable	Task Type	Execution ...	Task Progress	Task Status	Execution ...
105	1	<input checked="" type="checkbox"/>	Auto Detect NE Task	One-off	0%	Free	Succeeded
107	44	<input type="checkbox"/>	Board Software Batch Backup Task	Periodic	0%	Free	Succeeded
106	new	<input checked="" type="checkbox"/>	Traffic And Health Degree 15 ...	One-off	0%	Free	Succeeded
108	Test	<input checked="" type="checkbox"/>	PON MAC Address Table Export ...	Periodic	100%	Free	Succeeded

3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its object information and status.

Other Operations

In the right pane, right-click the desired task and select the corresponding shortcut menu to **Delete / Disabled** the task or view / modify **Properties**, etc.

11.2.3.2 Adding a Software Backup Task

When the existing software backup tasks do not meet the backup requirements, you can create software backup tasks according to your needs.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

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.
3. Click **Create** in the right pane to open the dialog box.

The screenshot shows a dialog box titled "Create Board Software Batch Backup Task". It has three tabs: "Basic information", "Object source", and "Extend information". The "Basic information" tab is selected. The dialog contains the following fields and controls:

- Task name:** An empty text input field.
- Enable:** A checked checkbox.
- Task Type:** Three radio buttons: "One time", "Every" (selected), and "Every week". The "Every" option is set to "1 day(s)". There is also an "Every month, Day:" option with a "1" in a spinner box.
- Execution time:** A time selection field showing "10:08:33".
- Start time:** A date and time selection field showing "2016-06-13 10:08:23".
- End time:** A checkbox labeled "End time:" followed by a date and time selection field showing "2016-06-13 10:08:23".
- Buttons:** "Copy from other tasks...", "Create", "OK", and "Cancel".

4. Set the parameters in the **Basic information**, **Object source**, and **Extend information** tabs as required, and click **OK** after completing the settings. Then the added tasks will be displayed in the task list.



Note:

Click the **Copy from Other Task** button, and users can copy all settings except for the **Task name**: of other tasks. This can improve the setting efficiency.

5. Click a certain task in the left pane, and users can view its object information and status.

11.2.3.3 Executing a Software Backup Task

The following introduces how to execute a software backup task.

Prerequisite

- ◆ The FTP server is configured. See [Setting the FTP Server](#).
- ◆ The file transmission service between the client end and the server end runs normally.
- ◆ You have the authorities of **Maintainer Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. In the left pane, select **Configuration Backup**→**Board Software Batch Backup Task** to view the existing tasks.
3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its **Object Information** and **Status** and check whether the configuration export task meets your requirements.
4. Right-click the desired task and select **Execute Now**, or click the task and click **Execute now** at the lower right corner of the tab to execute the configuration export task.

11.2.4 Managing MAC Address Table Export Tasks of PON Ports

The following introduces how to view, create and execute the MAC address table export tasks of PON ports.

11.2.4.1 Viewing MAC Address Table Export Tasks of PON Ports

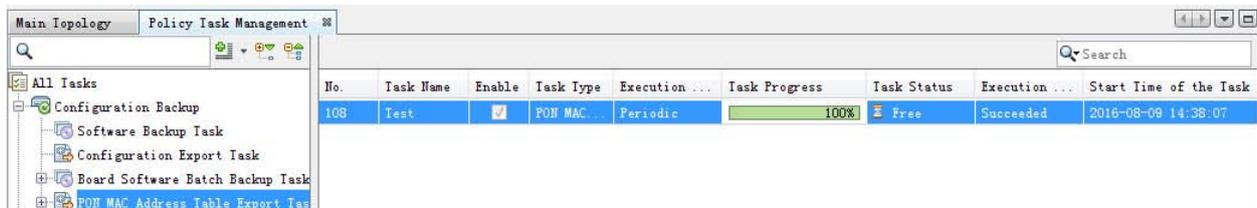
By viewing MAC address table export tasks of PON ports, you can decide whether to add or delete the tasks.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.
2. In the left pane, select **Configuration Backup**→**PON MAC Address Table Export Task** to view the existing configuration export tasks.



3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its object information and status.

Other Operations

In the right pane, right-click the desired task and select the corresponding shortcut menu to **Delete / Disabled** the task or view / modify **Properties**, etc.

11.2.4.2 Creating MAC Address Table Export Tasks of PON Ports

When the existing tasks do not meet the backup requirements, you can create MAC address table export tasks of PON ports according to your needs.

Prerequisite

You have the authorities of **Inspector Group** or higher authorities.

Procedure

1. Select **System**→**Policy Task Management** from the main menu to open the **Policy Task Management** tab.
2. Select **Configuration Backup**→**PON MAC Address Table Export Task** in the left pane.
3. Click **Create** in the right pane to open the dialog box.

The screenshot shows a dialog box titled "Create PON MAC Address Table Export Task". It has three tabs: "Basic information", "Object source", and "Extend information". The "Basic information" tab is selected. The fields are as follows:

- Task name: [Empty text box with a red asterisk]
- Enable:
- Task Type: One time, Every (1 day(s)), Every week (Monday), Every month, Day: (1)
- Execution time: 02:00:00
- Start time: 2016-06-13 10:16:01
- End time: 2016-06-13 10:16:01

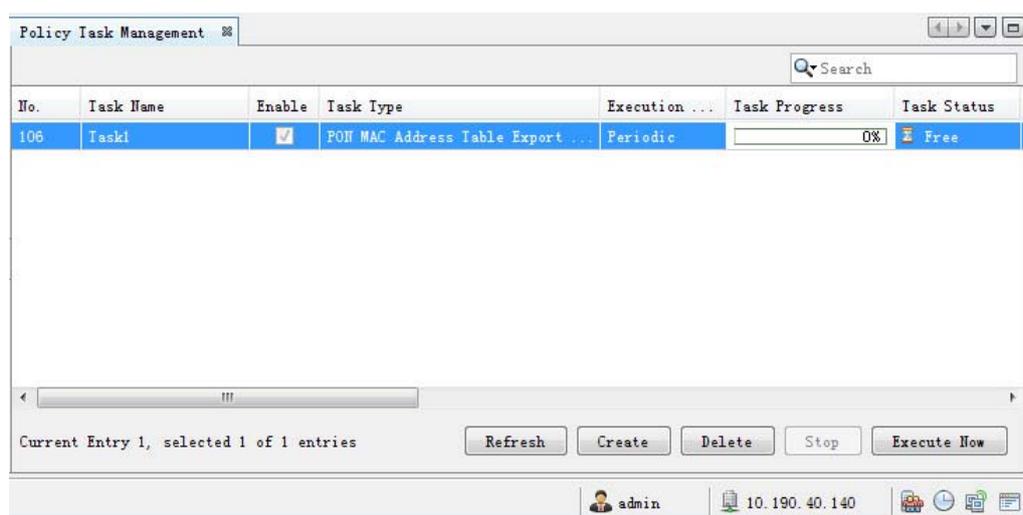
Buttons at the bottom: "Copy from other tasks...", "Create", "OK", "Cancel".

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 certain task in the left pane, and users can view its object information and status.

11.2.4.3 Executing MAC Address Table Export Tasks of PON Ports

The following introduces how to execute the MAC address table export tasks of PON ports.

Prerequisite

- ◆ The FTP server is configured. See [Setting the FTP Server](#).
- ◆ The file transmission service between the client end and the server end runs normally.
- ◆ You have the authorities of **Maintainer Group** or higher authorities.

Procedure

1. In the main menu, select **System**→**Policy Task Management** to open the **Policy Task Management** window.

2. In the left pane, select **Configuration Backup**→**PON MAC Address Table Export Task** to view the existing tasks.
3. In the right pane, right-click the desired task entry and select **View** from the shortcut menu to view its **Object Information** and **Status** and check whether the configuration export task meets your requirements.
4. Right-click the desired task and select **Execute Now**, or click the task and click **Execute now** at the lower right corner of the tab to execute the configuration export task.

12 Application Scenario

The following introduces several common application scenarios of the UNM2000.

- Alarm Management
- Performance Management
- Authorization and Domain Division
- Guaranteeing Device Configuration

12.1 Alarm Management

The alarm management module monitors the faults and abnormalities generated during the device operation in real time. Besides, it provides detailed information of the alarms and analysis tools supporting quick fault isolation and troubleshooting.

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. To query each alarm record, you can check the alarm logs.

- ◆ Alarm history: The removed current alarms are added into the alarm history after the preset delay time has expired.

The alarm history will be transferred to 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 Descriptions

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 Descriptions

Operation	Description	Related Function
Preset alarm parameters	Presets the alarm parameters, including alarm sound, automatic synchronization policy, history alarm definition, etc.	For setting alarm relevant parameters, see Setting Alarm Related Parameters .
Monitor alarms	Obtains the alarm information by monitoring the alarms.	For viewing current alarms, see Viewing Current Alarms .
		For viewing the alarm history, see Viewing Alarm History .
		For viewing reported alarms, see Viewing the Reported Alarms .
		For viewing alarm logs, see Viewing Alarm Logs .
		For viewing the alarm log statistics, see Viewing Statistical Data of the Alarm Logs .
		For viewing the alarm statistics, see Viewing Alarm Statistics .
Monitor alarms	You can obtain accurate alarm information via alarm synchronization which ensures consistency between the alarms displayed at the network management system side and occurring at the device side.	For alarm synchronization, see Synchronizing Alarms .
	The user can customize alarm names and levels according to maintenance requirements, for easier management and alarm monitoring.	For customizing alarm names, see Customizing Alarm Names . For customizing alarm levels, see Customizing Alarm Levels .

Table 12-1 Alarm Operation Descriptions (Continued)

Operation	Description	Related Function
	To make sure that the staff will be informed immediately when a fault occurs, the alarm notification method should be set beforehand, such as the alarm prompt tone, alarm report rules, and remote alarm notification rules.	For managing remote alarm notification, see Remote Alarm / Event Notification .
		For turning on / off the alarm sound, see Enabling / Disabling the Audio Alarm .
		For settings alarm reporting rules, see Viewing Alarm Reporting Rules .
Collect the failure information and analyze the failure cause	Collects failure relevant information and analyzes failure causes by viewing alarm details, locating alarms and viewing related alarms.	For viewing alarm details, see Viewing Alarm Details .
		For isolating the alarm, see Locating Alarms .
		For locating alarms, see Viewing Related Alarms .
		For outputting alarm information, see Exporting Alarms .
		View root / derivative alarms.
Eliminate failures	See the related manuals of the corresponding NEs and handling suggestions in the alarm details to eliminate the failure that triggers the alarm.	For viewing 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 .
	During maintenance, commissioning or provisioning, a large number of alarms may be reported. The user can filter the alarms by setting alarm mask to focus on the important ones only.	For filtering alarms, see Filtering Alarms .
		For managing alarm mask rules, see Viewing Alarm Filter Rules .
		For setting project alarm filtering, see Setting the Project Alarm Filter .

Table 12-1 Alarm Operation Descriptions (Continued)

Operation	Description	Related Function
Confirming alarms	If an alarm is confirmed, the alarm is processed.	For confirming alarms, see Confirming Alarms .
Record the alarm maintenance experience	After handling the alarms, you can record the alarm maintenance experience in the alarm library.	For editing alarm maintenance experience, see Editing Alarm Maintenance Experience . For managing alarm maintenance experience, see Managing Maintenance Experience .
Save alarm history data	Saving alarm history data can improve the NE running efficiency.	For managing historical data save, see Managing Alarm / Event Data .

12.2 Performance Management

The following introduces the performance management function, which helps the user understand the service operation status during a period of time.

Background Information

The performance data includes the real-time performance data, current performance data and performance history data.

- ◆ **Current performance:** The current 15-minute performance and the latest one to sixteen 15-minute performance. The performance data is not stored in the database.
- ◆ **Real-time performance:** The performance data that are collected and displayed in a real-time manner. The collection cycle can be set to 10 seconds or 30 seconds, and the collection period can be set to 15 minutes, 30 minutes, 1 hour or 24 hours. The performance data is not stored in the database.
- ◆ **Performance history:** The performance data that are saved in the database according to the performance collection task.

Performance Operation Descriptions

The UNM2000 provides abundant performance management functions. The user can refer to Table 12-2 and choose the corresponding function to monitor the NE service operation status effectively.

Table 12-2 Performance Operation Descriptions

Operation	Description	Related Function
Enable the NE performance classification	As there are a large number of performance indexes and performance data, the performance classification function is disabled by default. Therefore, the user should enable the NE performance classification switch before querying the NE performance data.	-
Manage the performance collection	The user can collect performance data or monitor the performance quality with the function of performance collection task.	For managing the performance collection task, see Managing Performance Collection Task .
	The user can set the performance parameters of the performance collection task quickly by managing the performance index set.	For managing performance index sets, see Managing Performance Index Sets .
	The user 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, see Managing Performance Threshold Sets .

Table 12-2 Performance Operation Descriptions (Continued)

Operation	Description	Related Function
Monitor the performance data	You can obtain the performance data using the performance monitoring function.	For viewing the current performance, see Viewing the Current Performance .
		For viewing the real-time performance, see Viewing the 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 Comparison of Performance Data .
Save performance history data	Saving performance history data can improve the NE running efficiency.	For managing historical data save, see Managing Performance Data .

12.3 Authorization and Domain Division

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

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 authorities respectively.

Procedures

1. Create object sets.

According to area division, create object set A and object set B. Add the devices of Area A and Area B to the members of object set A and object set B.

Refer to [Creating an Object Set](#) to create the object sets.

2. Create operation sets.

Use 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 specific operations of creating the operation set, see [Adding an Operation Set](#).

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
Supervisor 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

Refer to [Creating User Groups](#) for specific steps of creating the 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.
- ▶ According to the working shifts of the staff, set the login time ranges.

- ▶ Set the users' user groups. If six user groups A, B, C, D, E, and F are to be created, refer to Table 12-4. After being assigned with a user group, the user will be authorized with the management domain and operational authorities 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 and limit the IP address range accessible to the user.

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 sudden accidents like device fault, disconnection between the network management system and the device, shut-off of the power supply system, which may impact the service restoration, the UNM2000 provides several functions to guarantee the device configuration.

Backing up System Configuration

- ◆ When the user needs to compare the device configuration with the configuration in the network management database, the user can perform configuration synchronization and check whether every configuration is consistent. If not, the user can manually synchronize the device configuration to the database, or from the database to the device. For detailed operation steps, see [Configuration Synchronization](#).

- ◆ To avoid device fault, the user can set the execution cycle to automatically upload the device configuration to the network management database periodically. This helps restore the configuration quickly after the device fault is recovered. For detailed operation steps, see [Managing Configuration Uploading Tasks](#).
- ◆ To avoid fault occurring on the device and the network management server at the same time, the user can set the execution cycle to automatically export the device configuration periodically and save to another FTP server. This ensures the device configuration will not be lost. For detailed operation steps, see [Managing Configuration Export Tasks](#).

Backing up the Software

To avoid device software upload failure, the user can set the execution cycle to automatically back up the device software periodically to the FTP server. This helps recover the device software quickly. For detailed operation steps, see [Managing Software Backup Tasks](#).

13 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	Resource 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