

iManager U2000 Unified Network Management System

V200R016C60

Product Description

Issue 11

Date 2018-11-30

HUAWEI TECHNOLOGIES CO., LTD.



Copyright © Huawei Technologies Co., Ltd. 2018. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
 Bantian, Longgang
 Shenzhen 518129
 People's Republic of China

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

Email: support@huawei.com

About This Document

Intended Audience

The *iManager U2000 Product Description* describes the network position, functions and features, system architecture and network applications of the U2000. The document also provides the reliability scheme and technical specifications of the U2000.

The intended audiences of this document are:

- Network planning engineers
- Data configuration engineers
- System maintenance engineers

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes in earlier issues.

Issue 11 (2018-11-30)

This issue is the eleventh release. Modify:

7.4 Alarm Management

Issue 10 (2018-08-15)

This issue is the tenth release. Modify:

- **4.1.2 CORBA NBI**

Issue 09 (2018-02-24)

This issue is the ninth release. Modify:

- **4.1 NBI**
- **11.4 Management Capabilities of Compatible Models**
- **11.3 Management Capabilities of Standard Delivery Models**
- **5.2.1 Hardware Configuration**
- **13.5 Introduction to the Reliability and Protection Solution**

- **4.1.2 CORBA NBI**

Issue 08 (2017-11-13)

This issue is the eighth release. Modify:

- **6.1.2 U2000 Deployment on Virtual Machines**
- **11.4 Management Capabilities of Compatible Models**
- **13.5 Introduction to the Reliability and Protection Solution**

Issue 07 (2017-09-27)

This issue is the seventh release. Modify:

- **6.1 Deployment Mode**
- **6.1.1 Single-Server System Deployment Mode**
- **6.1.2 U2000 Deployment on Virtual Machines**
- **5.1.2 Software Configurations**
- **5.2.1 Hardware Configuration**
- **13.3 Configuration Requirements**

Issue 06 (2017-07-28)

This issue is the sixth release. Modify:

- **5.1.1 Hardware Configuration**
- **6.1.2.1 Deployment Mode of the U2000 Virtual Machine Single-Server System**
- **11.1 U2000 Management Capability**
- **11.2.2 Equivalent NEs in the IP Domain**
- **11.3 Management Capabilities of Standard Delivery Models**
- **11.4 Management Capabilities of Compatible Models**
- **12.8 D-CCAP Series Equipment**
- **13.2 Network Structure**
- **13.3 Configuration Requirements**
- **13.7 Management Capability**

Issue 05 (2017-05-25)

This issue is the fifth release. Modify:

- **5.1.1 Hardware Configuration**
- **13.3 Configuration Requirements**

Issue 04 (2017-04-15)

This issue is the forth release. Modify:

- **5.1.1 Hardware Configuration**
- **11.4 Management Capabilities of Compatible Models**

Issue 03 (2017-03-30)

This issue is the third release. Modify:

11.4 Management Capabilities of Compatible Models

Issue 02 (2017-02-25)

This issue is the second release. Modify:

- **5.1.1 Hardware Configuration**
- **6.1.2.1 Deployment Mode of the U2000 Virtual Machine Single-Server System**
- **7.6 Performance Management**
- **11.4 Management Capabilities of Compatible Models**
- **12.2 WDM Series Equipment**
- **12.5 RTN Series Equipment**

Issue 01 (2016-11-28)

This issue is the initial release.

Contents

About This Document.....	ii
1 Product Overview.....	1
1.1 Network Position.....	1
1.1.1 Network Management Trend.....	1
1.1.2 Product Positioning.....	2
1.2 Product Characteristics.....	2
2 New Features.....	9
3 Software Architecture.....	13
4 External Interfaces.....	15
4.1 NBI.....	16
4.1.1 XML NBI.....	19
4.1.2 CORBA NBI.....	23
4.1.3 SNMP NBI.....	26
4.1.4 TL1 NBI for Access Equipment.....	26
4.1.5 Performance Text NBI.....	28
4.1.6 Customer OSS Test NBI for Access Equipment.....	28
4.2 SBI.....	29
5 Configuration.....	39
5.1 Physical Machine Scenario.....	39
5.1.1 Hardware Configuration.....	39
5.1.2 Software Configurations.....	41
5.2 Virtual Machine Scenario.....	44
5.2.1 Hardware Configuration.....	45
5.2.2 Software Configurations.....	51
5.3 Configuration of the U2000 Client.....	54
6 Networking and Application.....	55
6.1 Deployment Mode.....	55
6.1.1 U2000 Deployment on Physical Machines.....	58
6.1.1.1 Single-Server System Deployment Mode.....	58
6.1.1.2 Cold Backup Deployment Mode.....	59
6.1.1.3 Deployment of an HA System.....	62

6.1.2 U2000 Deployment on Virtual Machines.....	64
6.1.2.1 Deployment Mode of the U2000 Virtual Machine Single-Server System.....	64
6.1.2.2 Deployment Mode of the U2000 Virtual Machine Cold Backup System.....	67
6.1.2.3 Deployment Mode of the U2000 Virtual Machine Remote High Availability System.....	70
6.2 Networking Mode Between the U2000 and NEs.....	72
6.2.1 Inband Networking Mode.....	72
6.2.2 Outband Networking Mode.....	73
6.3 Application Scenarios of U2000 Management.....	74
6.3.1 Unified Management of Network Products.....	74
6.3.2 Single Metro Solution.....	76
6.3.3 Single Backhaul Solution.....	79
6.3.4 Single Backbone Solution.....	83
6.3.5 Single FTTx Solution.....	85
6.3.6 OptiCable D-CCAP Solution.....	91
7 Basic Functions.....	96
7.1 Overview of Functions and Features.....	97
7.2 Security Management.....	99
7.3 Topology Management.....	110
7.4 Alarm Management.....	117
7.5 Fault Diagnosis.....	140
7.6 Performance Management.....	144
7.7 Inventory Management.....	153
7.8 Log Management.....	156
7.9 Database Management.....	162
7.10 NE Communication Parameter Management.....	165
7.11 DCN Management.....	166
7.12 NE Software Management.....	167
7.13 Report Management.....	169
7.13.1 SDH Report.....	173
7.13.2 Microwave Report.....	178
7.13.3 WDM Statistic Report.....	184
7.13.4 MSTP Ethernet Report.....	192
7.13.5 PTN Statistic Report.....	193
7.13.6 Access Service Statistics Reports.....	197
7.13.7 Project Document Statistics Reports.....	210
7.14 System Monitoring.....	214
7.15 Network Management System Maintenance Suite.....	216
8 Network Feature Configuration and Management.....	218
8.1 MSTP Network Feature Management.....	219
8.1.1 MSTP NE Management.....	219
8.1.2 MSTP Protection Subnet Management.....	239
8.1.3 MSTP End-to-End Management.....	240

8.1.4 SDH ASON Network Management.....	248
8.2 WDM/OTN Network Feature Management.....	254
8.2.1 WDM/OTN NE Management.....	254
8.2.2 WDM/OTN NE (NA) Management.....	269
8.2.3 WDM/OTN Protection Subnet Management.....	278
8.2.4 WDM/OTN E2E Network Management.....	279
8.2.5 WDM ASON Network Management.....	286
8.3 RTN Network Feature Management.....	292
8.3.1 RTN NE Management.....	292
8.3.2 RTN Protection Subnet Management.....	306
8.3.3 End-to-End RTN Management.....	306
8.4 PTN Network Feature Management.....	310
8.4.1 PTN NE Management.....	310
8.4.2 E2E PTN Management.....	333
8.5 Router Feature and Switch Feature Management.....	338
8.5.1 Overview of Router and Switch Management.....	338
8.5.2 Network Deployment.....	340
8.5.2.1 IP Plug and Play.....	340
8.5.2.2 Router Management.....	341
8.5.2.3 Router V8 Management.....	349
8.5.2.3.1 Main Features of V8-based NE Management.....	350
8.5.2.3.2 Quick Search for V8 NE Explorer Parameters.....	351
8.5.2.4 Switch Management.....	351
8.5.2.5 Switch CE Management.....	353
8.5.2.6 Template Management.....	355
8.5.2.7 Node Redundancy Management.....	357
8.5.3 Service Deployment.....	357
8.5.3.1 Tunnel Service Management.....	357
8.5.3.2 VPN Service Management.....	358
8.5.3.3 IP Hard Pipe Service Management.....	360
8.5.4 Network Monitoring.....	361
8.5.4.1 Router Health Monitoring.....	361
8.5.4.2 AtomEngine Management.....	364
8.5.5 Network Diagnosis.....	368
8.5.5.1 IP Device Health Check.....	368
8.5.5.2 Diagnosis Management.....	368
8.5.5.3 IP Network TroubleShooting.....	369
8.6 Security NE Feature Management.....	371
8.6.1 Security NE Management.....	371
8.6.2 Network Security Management.....	375
8.6.3 Single-Point Web Configuration.....	376
8.6.4 Security VPN Service Management.....	377

8.7 FTTx Network Feature Management.....	378
8.7.1 OLT Management.....	378
8.7.2 ONU Management.....	396
8.7.3 Intelligent site management.....	411
8.8 D-CCAP Network Feature Management.....	412
8.9 MSAN Network Feature Management.....	418
8.9.1 MSAN Management.....	418
8.10 DSLAM Network Feature Management.....	433
8.10.1 DSLAM Management.....	433
8.11 BITS/RPS/EDFA Network Feature Management.....	441
8.11.1 BITS NE Management.....	441
8.11.2 RPS NE Management.....	442
8.11.3 EDFA NE Management.....	443
8.12 Third-Party NE Management.....	444
9 Reliability.....	459
9.1 Physical Machine Reliability and Protection Solution.....	459
9.2 Virtual Machine Reliability and Protection Solution.....	467
10 Performance Indicators.....	475
11 Management Capability.....	480
11.1 U2000 Management Capability.....	480
11.2 NE Equivalent Coefficient.....	483
11.2.1 Equivalent Coefficients of NEs in the Transport Domain.....	484
11.2.2 Equivalent NEs in the IP Domain.....	491
11.2.3 Equivalent NEs in the Access Domain.....	501
11.3 Management Capabilities of Standard Delivery Models.....	503
11.4 Management Capabilities of Compatible Models.....	506
12 Manageable NE.....	527
12.1 MSTP Series Equipment.....	528
12.2 WDM Series Equipment.....	538
12.3 WDM (NA) Series Equipment.....	549
12.4 Submarine Line Equipment.....	551
12.5 RTN Series Equipment.....	552
12.6 PTN Series Equipment.....	560
12.7 FTTx Series Equipment.....	567
12.8 D-CCAP Series Equipment.....	584
12.9 MSAN Series Equipment.....	586
12.10 DSLAM Series Equipment.....	587
12.11 BITS/iSite/EDFA Series Equipment.....	591
12.12 NE/ATN/CX/Multi-service gateways Series Equipment.....	592
12.13 R/AR Series Equipment.....	603
12.14 RM9000 Series Equipment.....	606

12.15 Switch Series Equipment.....	606
12.16 VoIP Gateway Equipment.....	611
12.17 Security Series Equipment.....	612
12.18 iCache Series Equipment.....	621
13 Distributed U2000 System.....	622
13.1 Solution Overview.....	623
13.2 Network Structure.....	624
13.3 Configuration Requirements.....	625
13.4 NBI Capabilities.....	631
13.5 Introduction to the Reliability and Protection Solution	634
13.6 Reliability Indicator.....	640
13.7 Management Capability.....	641
13.8 Performance Indicators.....	642
14 Standards and Protocols Compliance.....	646
A Glossary and Abbreviations.....	652

1 Product Overview

About This Chapter

This topic describes the position of the iManager U2000 unified network management system (U2000 for short) in the telecommunications management network (TMN) and the product characteristics.

1.1 Network Position

This topic focuses on the trends in network management and the position of the U2000 in the TMN hierarchy.

1.2 Product Characteristics

The U2000 improves its management capability, scalability, and usability to construct a unified and customer-oriented next-generation NMS.

1.1 Network Position

This topic focuses on the trends in network management and the position of the U2000 in the TMN hierarchy.

1.1.1 Network Management Trend

With the development of IT and IP technologies and the convergence of various industries (such as telecommunications, IT, media, and consumer electronic industries), the telecommunications industry has witnessed tremendous changes. Broadband services, mobile services, and network convergence have become the mainstream. Carriers' market orientation and business modes have also changed.

- The development of the all-IP architecture is a leading factor in the transition from the existing vertical network that is divided by technology and service to the flattened horizontal network.
- Improving user experience, lowering operation expenditure (OPEX), and improving efficiency are the driving forces for fixed-mobile convergence (FMC).
- Network convergence leads to operation and maintenance (O&M) convergence.

The U2000 is future-oriented and provides unified management of all-IP and FMC bearer and access equipment.

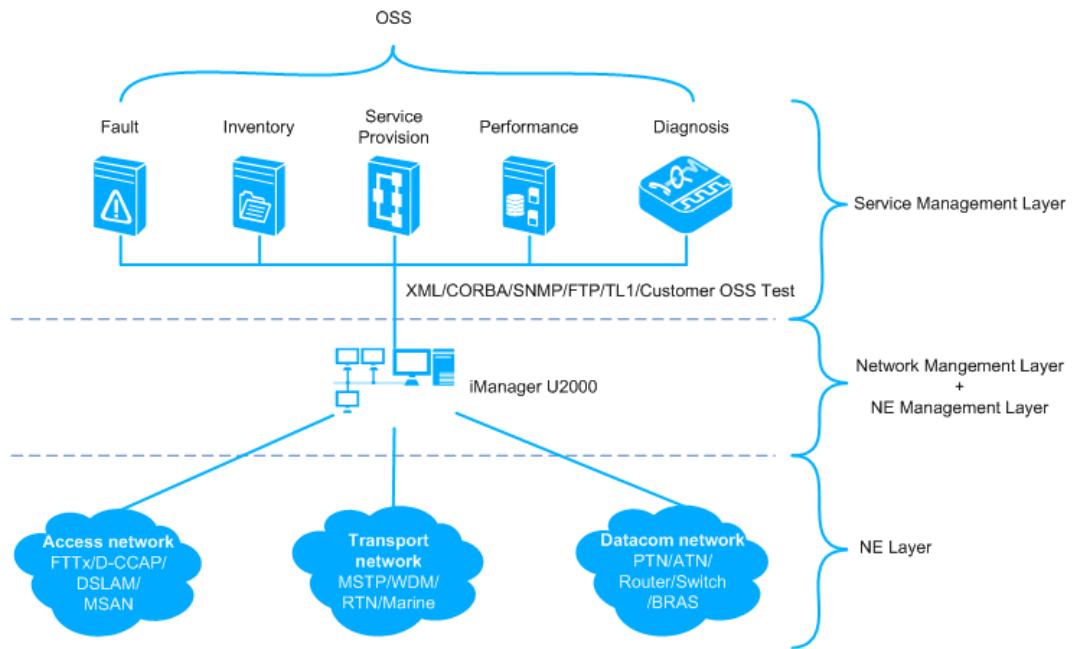
- The U2000 supports not only unified management of multi-domain equipment but also unified management at the element and network layers. The U2000 has revolutionized the layer-based management mode to meet the management requirements for transforming from the existing vertical network to the flattened horizontal network.
- The U2000 is a unified network management system (NMS) for multiple domains that aims to minimize O&M costs and to bring more network benefits to carriers.

1.1.2 Product Positioning

The U2000 is an equipment management system developed by Huawei. It is also a major future-oriented network management solution that provides powerful element management and network management functions.

In the TMN hierarchy, the U2000 is located at and supports all the functions of the element management and network management layers. **Figure 1-1** shows the position of the U2000 in the TMN hierarchy.

Figure 1-1 Position of the U2000 in the TMN hierarchy



1.2 Product Characteristics

The U2000 improves its management capability, scalability, and usability to construct a unified and customer-oriented next-generation NMS.

Unified and Abundant NBIs

The U2000 provides various operating support system (OSS) integration solutions with unified and abundant NBIs based on mainstream standards.

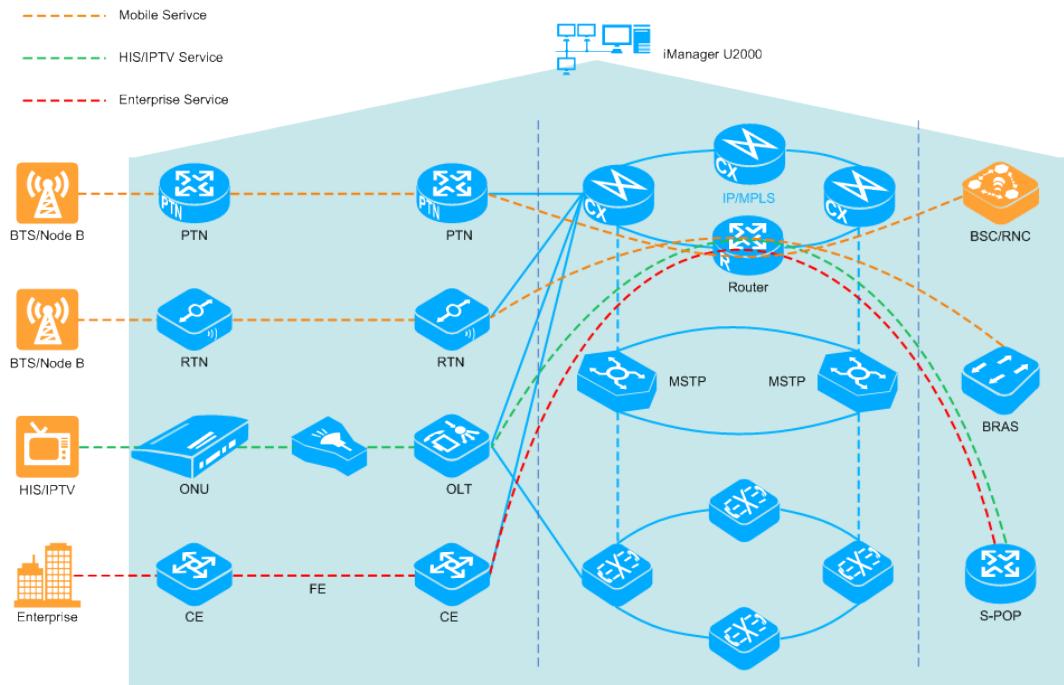
- Unified NBIs enable the U2000 to manage transport equipment, access equipment, IP equipment.
- Based on international standards, the NBIs of the U2000 are inexpensive to develop, economical to maintain, and easy to expand.
- Comprehensive NBIs (XML, CORBA, SNMP, TL1, TEXT, Customer OSS Test) address the needs for OSS integration.

Unified Network Management

The U2000 manages transport equipment, access equipment, IP equipment in a unified manner. Specifically, it manages Huawei MSTP, WDM, OTN, RTN, router, switch, ATN, PTN, MSAN, DSLAM, FTTx, firewall equipment and services.

In addition, the U2000 manages end-to-end (E2E) services, as shown in [Figure 1-2](#). The services include MSTP, WDM, RTN, PTN, ATN, Router, and Switch services.

Figure 1-2 Unified network management



NOTE

Services marked blue can be managed by the U2000 and services marked yellow cannot be managed by the U2000.

The U2000 is also capable of managing third-party equipment by obtaining equipment information directly through ICMP and SNMP protocols.

For details about the third-party equipment management function, see [Third-Party Router Management](#).

Multiple Operating Systems

The U2000 was developed based on Huawei's integrated management application platform (iMAP). The U2000 supports Sun workstations, PC servers, Sybase databases, SQL Server databases, Solaris, Windows, and SUSE Linux operating systems (OSs).

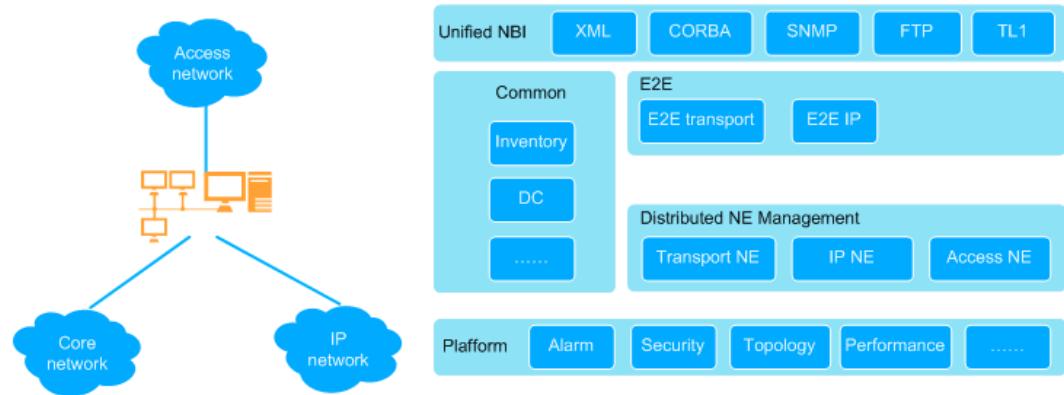
The U2000 is a standalone application that can be installed on a variety of OSs and databases. The U2000 provides high-end solutions for large-scale networks and low-cost solutions for common- and medium-scale networks.

Leading Scalable NMS Architecture

By adopting the mature and widely-used client/server (C/S) architecture, the U2000 supports distributed and hierarchical database systems, service processing systems, and client application systems. Modularized architecture is scalable so that the U2000 meets the management requirements of complex and large-scale networks, as shown in [Figure 1-3](#).

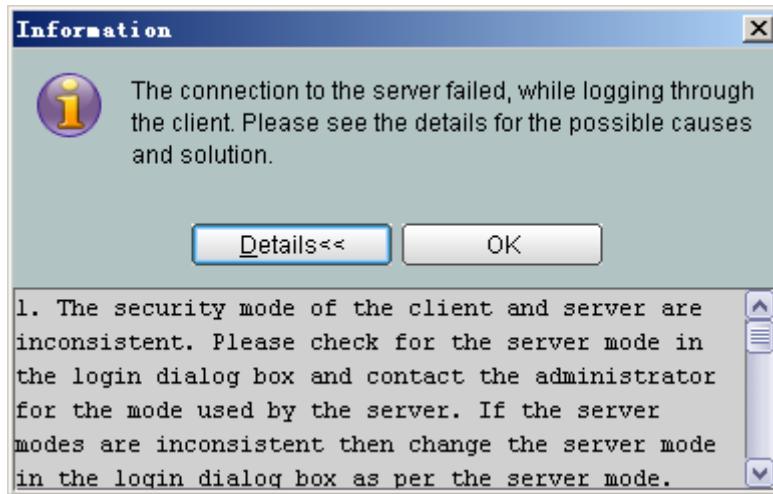
- The U2000 uses an object-oriented, multiprocessing, modularized, and component architecture design. The degree of coupling NE management components is reduced with this design, which means that the U2000 can increase its management capability from a single domain to multiple domains when the U2000 is installed multi-domain components.
- The U2000 can flexibly integrate different NBIs.
- The loose coupling framework supports independent maintenance of subsystems.
- The U2000 enables users to log in to a server at the same time from multiple clients. Users on different clients can view the same network data or custom network data, and operate the clients at the same time.

Figure 1-3 Modularized architecture



Friendly User Interface

- Fully considering users' operation habits, the U2000 provides alarm, topology, performance, security, and configuration management interfaces with the same graphical user interface (GUI) style.
- If any error operation is performed, the U2000 displays a friendly error message showing the cause and troubleshooting method.



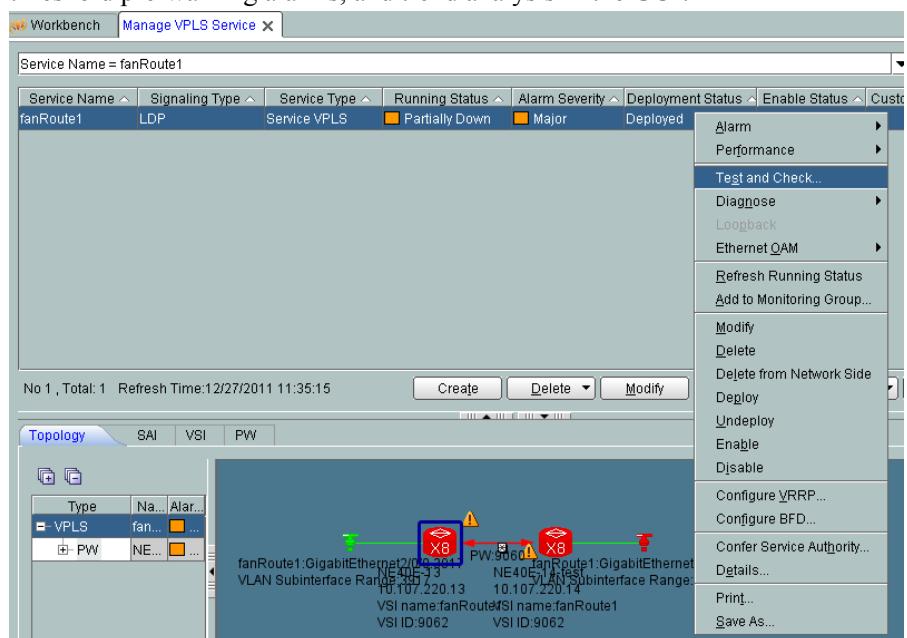
Visualized Management

- **Service supervision:**

- Supports service-centered visualized supervision and sorting affected services by alarm type.

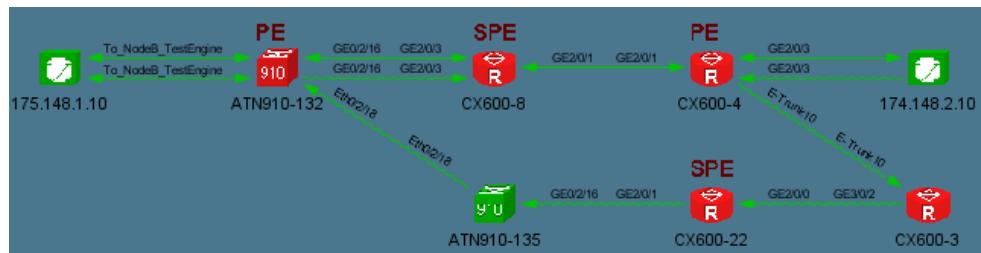
Sev...	Name	Alarm Source	Service Imp...
Major	MPLS Tunnel Failure	PTN6900-8-192	No
Critical	Link Down	PTN6900-8-192	No
Major	Static CR-LSP Down	PTN6900-8-192	No
Major	Static CR-LSP Down	PTN6900-8-192	No
Major	CES_LOSPKT_EXC	NE(126-243)	Yes
Critical	MPLS_TUNNEL_LOCV	PTN6900-8-192	No

- Provides a variety of detection and diagnostic methods to quickly check service connectivity and locate faults, and supports service-based performance query, threshold pre-warning alarms, and trend analysis in the GUI.



- **Visualized trails:**

- Displays trails in real time to solve the problem of invisible bearer path.
- Provides complete fault diagnosis methods based on trails, which facilitates fast network and service fault diagnosis.
- Supports the discovery of protection paths which cover five protection solutions on the live network, including primary/secondary PW, VPN FRR, VRRP, E-APS, and TE Hotstandby. Supports the discovery and display of primary and bypass paths, meeting the requirements for locating service switching faults.
- Supports hierarchical display of paths based on services, tunnels, routes, and links as well as the clear display of fault locations.
- Supports ME VPLS- and HVPLS-based path discovery and path-based visualization path locating.
- Automatically specifies the diagnosis process based on the MBB scenario and fault type (service interruption, service deterioration, or clock switching). A total number of 300 check items are provided to cover key MBB features, improving the precision and efficiency.
- Supports fault locating in the clock view.
- Supports fault locating eMBMS multicast.



- **Service deployment:**

- Provides templates to set service-related parameters once instead of repeated times.
- Supports bulk deployment of services, which increases configuration efficiency.
- Calculates static CR Tunnel routes and allocates labels automatically.

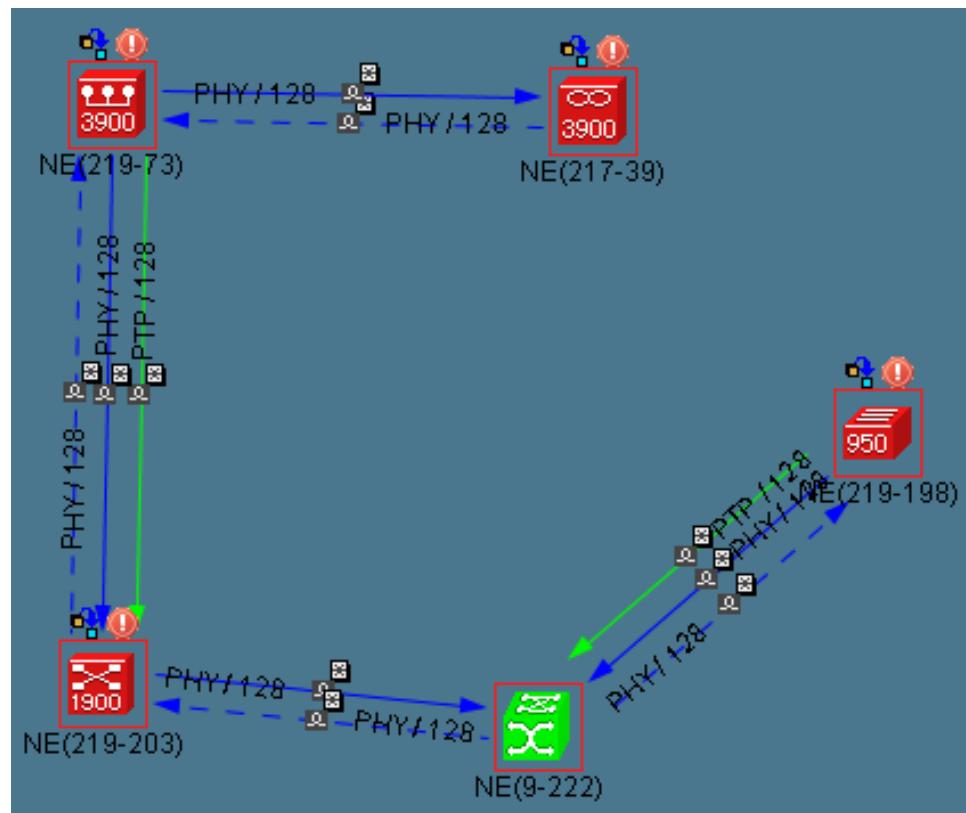
- **Object relationship:**

- Associates services with tunnels and tunnels with routes. Hierarchical object relationships explicitly represent the bearer relationships.
- Provides bearer relationships to quickly locate and rectify faults.

The screenshot shows the 'Check Result' interface. At the top, there is a table for 'Configuration' with fields for Source Device (NE40E-13), Source Equipment LSR ID (200.0.0.13), Source PWID (9060), Destination Equipment (NE40E-14-test), and Destination PWID (200.0.0.14). Below this is a message 'No 1 , Total: 1'. The main area is titled 'Check Result' with a warning icon. It displays a 'Check Path: By IP Route' between two nodes: NE40E-13 (200.0.0.13) and NE40E-14-test (200.0.0.14). The path consists of two segments: 2-0-0(GigabitEthernet2/0/0) 201.13.14.1 and 1-0-0(GigabitEthernet1/0/0) 201.13.14.2. Below the path diagram is a table titled 'Check Steps' with columns for 'Check Steps', 'Results', and 'Details'. The steps listed are: ICMP Ping From NE40E-13 To NE40E-14-test (Operation succeeded), LSP Ping (failed, NE40E-14-test host failed), VCCV Ping (failed, NE40E-14-test host failed), Check Tunnel Exist (failed, cannot find tunnel or E2E does not managed), Query Equipment LDP Session Information (Operation succeeded), Query LSP Information (Operation succeeded), and Service Configuration Check (Abnormal).

- **Network-wide clock:**

- Supports the automatic discovery of clocks (physical clock, PTP clock, ACR clock, PON clock and ATR clock).
- Provides the unified topology view of network-wide clocks and refreshes the tracking relationships and synchronization status of the clocks when faults occur.
- Monitors clock status and displays clock alarms, tracking relationships, and protection status in real time.



Cross-Domain E2E Service Provisioning

- Supports E2E TDM service provisioning and management across traditional microwave and MSTP networks, which shortens the time needed for network deployment and service provisioning on a large number of microwave services.
- Supports E2E packet service provisioning and management across IP microwave and PTN/Hybrid MSTP networks, which accelerates service provisioning in IP networks.
- Supports E2E management of ETH service, CES service, ATM service, MPLS tunnels, and PWs for PTN, MSTP, RTN, Switch, and NE series devices, to meet the development in the fixed market as it gets driven towards fixed-mobile convergence (FMC).
- Supports E2E service (ETH, CES, and ATM) provisioning across PTN and CX networks, and supports E2E management of MPLS tunnels and PWs, to meet the development in the mobile market as it gets driven towards FMC.
- Supports the GPON+IP topology where you can configure and manage ONU E-Line services in an E2E manner.
- Supports RTN+PTN and ATN+RTN+CX packet service provisioning.

2 New Features

This topic describes new features of the U2000 V200R016C60.

New Features in the IP Domain

- **Network Slice**
, Network slicing is developed to isolate bandwidth resources of different services such as mobile backhaul, group customer, and home broadband services and allow services of the same type to share bandwidth resources.
- **PTN (V8) as a Non-GNE**
The scenario where a V8 PTN NE functions a non-GNE outshines that where a V8 PTN NE functions a GNE in the following aspects:
 - NE management: A V8 PTN NE that functions as a GNE can access PTN NEs that do not function as GNEs.
 - DCN channel protection mechanism: The U2000 proactively detects channel faults and provides DCN protection.
 - Site deployment and network access efficiency: The efficiency improves greatly and the configuration is simplified.
 - Maintenance mechanism: Routes only between NEs and GNEs need to be maintained.
- **Seamless MPLS solution simplification**
Seamless MPLS service provisioning is simplified, improving the O&M solution competitiveness.
 - BGP routing policy configuration is simplified, and batch configuration of BGP peer is optimized.
 - Protection labels are automatically allocated for tail nodes.

New Features in the Access Domain

- **D-CCAP O&M enhancement**
 - **EQAM Service Configurations**
Edge Quadrature Amplitude Modulation (EQAM) modulates videos of IP networks into QAM signals so that video data can now be carried on HFC networks. The existing CATV coaxial cable resources can be reused and no additional IP access network is required, reducing costs.

The built-in EQAM of a CMC supports Digital Video Broadcasting (DVB) services and Video On Demand (VOD) services.

- DVB service: The services are transmitted to OLTs through the D-CCAP upper-layer IP network. Media data in the IP format is modulated into RF signals on CMCs. DVB is similar to traditional wired broadcasting or television satellite broadcasting. Users have the same experience in watching DVB programs and traditional television programs. DVB standards are a combination of digital broadcasting standards including Digital Video Broadcasting-Satellite (DVB-S), Digital Video Broadcasting-Cable (DVB-C), and digital video broadcasting-terrestrial (DVB-T).

DVB-C video quality monitoring: You can query the input transport streams, output transport streams to monitor the program quality and collect statistics on packets at video stream forwarding points like CMCs, channels in real time. This implements E2E DVB-C video streams monitoring and fast diagnosis of video quality issues.

- Query input transport streams: Query the status information to verify that programs watched by users are sent to CMCs and check statistics on the program information of online transport streams, packet identifiers (PIPs), and EQAM DVB video domain input packets.
- Query output transport streams: Check information related to user programs and transport stream information based on CMCs or channels. Query the PIP packet parsing of output transport streams, including type, maximum rate, minimum rate, interference, CC errors, and associated programs. This allows you to determine whether a DVB program is normal and whether the program traffic has packet loss.
- VOD service: Idle downstream channels are set as EQAM channels for transporting video services. Users can view desired TV programs in real time based on the program list provisioned by the digital television system.
Check the VOD mapping information of a CMC to verify that program channels are normal. Check the output statistics of CMC channels to verify that the traffic of program transport streams is normal.
- Configure the location ID of a CMC. The U2000 delivers CMC location ID to STB through the packets in the video stream. Based on the packets, the STB obtains the association relationship connected to the CMC. Then the STB feeds back the association relationship to the STB and CMC network topology in the OSS system. In this manner, users can locate video faults to the faulty CMC.

- **Cable fault diagnosis**

- **CMC link health scoring:** To score CMC network quality based on its running data, allowing you to identify Top N deteriorated CMCs, detect potential faults in advance and help carriers achieve proactive O&M.
 - Network-wide CMCs are scored and ranked automatically every day, showing Top N deteriorated NEs.
 - The hourly network quality of each CMC is displayed, allowing you to pinpoint the time period when multiple CMs under a CMC are faulty.
 - CM KPIs during low-quality period are also displayed, allowing you to identify the branch where faults were introduced. KPIs include upstream and downstream SNR, upstream and downstream PWR, bit error, and flap. In this manner, the fault restoration efficiency is improved by 50%.

- **DOCSIS 3.1 PNM diagnosis:** The PNM standard test method is used to improve fault diagnosis precision.
 - Fault diagnosis of DOCSIS 3.1 networks is supported. The full coverage of fault information, remote fault analysis, and reduced site-visit time.
 - D-CCAP network faults including interface faults, line damage, component faults, and interference source diagnosis are covered.
 - The test methods are various, like comprehensive CMC upstream diagnosis, and comprehensive CM upstream diagnosis.
 - Comprehensive CMC upstream diagnosis: Perform multiple tests or single test for the upstream channel of a CMC, including tests on the impulsive noise, spectrum scanning, and histogram of CMC channels.
 - Comprehensive CM upstream diagnosis: Perform multiple tests or single test for the upstream channel of a CM, including impulsive noise, spectrum scanning, histogram, MER, and FEC tests of CM subcarriers.
- **Easy installation and maintenance through the MSO app**
 - DOCSIS 3.1 upstream frequency response: collects statistics and displays frequency response of upstream detection signals of CMCs sent by CMs from D3.1 channels so that maintenance personnel can analyze the attenuation and transmission capabilities of the upstream line between CMs and CMCs.
 - CMC diagnosis: The function can help the maintenance personnel to locate faults. This function is used to check the status of CMC NEs and performance indicators, as well as to query CM statistics, parameter details, frequency of the upstream and downstream channels, channel usage, EQAM channel and link details.
 - Downstream pilot: The function is used to configure multiple downstream pilot signals to be sent from a CMC channel. A hand-held meter receives the signals and calculates the line frequency response so that maintenance personnel can analyze the attenuation and transmission capabilities of the CMC downstream line.
- **Independent O&M of vANs:** vANs can be operated and maintained in a visualized, independent, efficient, and easy manner, achieving the same experience as that of managing physical OLTs

MA5800 V100R017C10 and later support vAN management. One physical device is virtualized into multiple logical devices by board or port. In this manner, you can flexibly schedule resources of access networks and deploy network functions as needed, meeting the requirements of independent network resources and independent O&M in multi-service, multi-carrier, and multi-industry scenarios. Visualized management is supported. In vAN views, you can create a VS, and view and manage the resource allocation of the VS. The management experience is the same at that of managing physical OLTs.

vANs meet intelligent operation requirements, for example, the multi-service scenario.

 - One OLT carrying multiple services: One physical OLT functions as multiple virtual OLTs to carry different services, saving space and power, and improving efficiency. In addition, you can use the open APIs to customize services on demand using Remote Serial Protocol (RSP).
 - Private line experience: Each virtual OLT has exclusive forwarding and control resources, ensuring private line priority.

- Domain-based management and easy maintenance: Different virtual OLTs are maintained by different teams, realizing end-to-end (E2E) maintenance.
- Secure resources: Physical resources are isolated, ensuring resource security for tenants.
- Resource sharing: vANs allow multiple carriers to share the infrastructure and independently maintain and manage their resources. vANs can also be leased to tenants like hotels and data centers in batches.

New Features for the Transport Domain

- MSOTN E2E scenarios are completed.
 - The VRP platform supports deployment of Layer 2 native Ethernet trails.
 - Asymmetric Layer1+Layer 2 E-Line services can be quickly provisioned.
- U2000 can expand MSTP lines to 40G without interrupting services.
- Low-rate 2M services support ASON and can be quickly provisioned and restored.

New Features for the Common Domain

Huawei FusionSphere cloud OS solution uses the OpenStack architecture. This solution implements virtualization of software and hardware in a data center and provides unified resource management and scheduling while ensuring openness and compatibility.

The following FusionSphere VM solutions have been added to the U2000 VM deployment solution:

- Single-server system (FusionSphere, E9000 server)
- HA system (FusionSphere, E9000 server)

NOTE

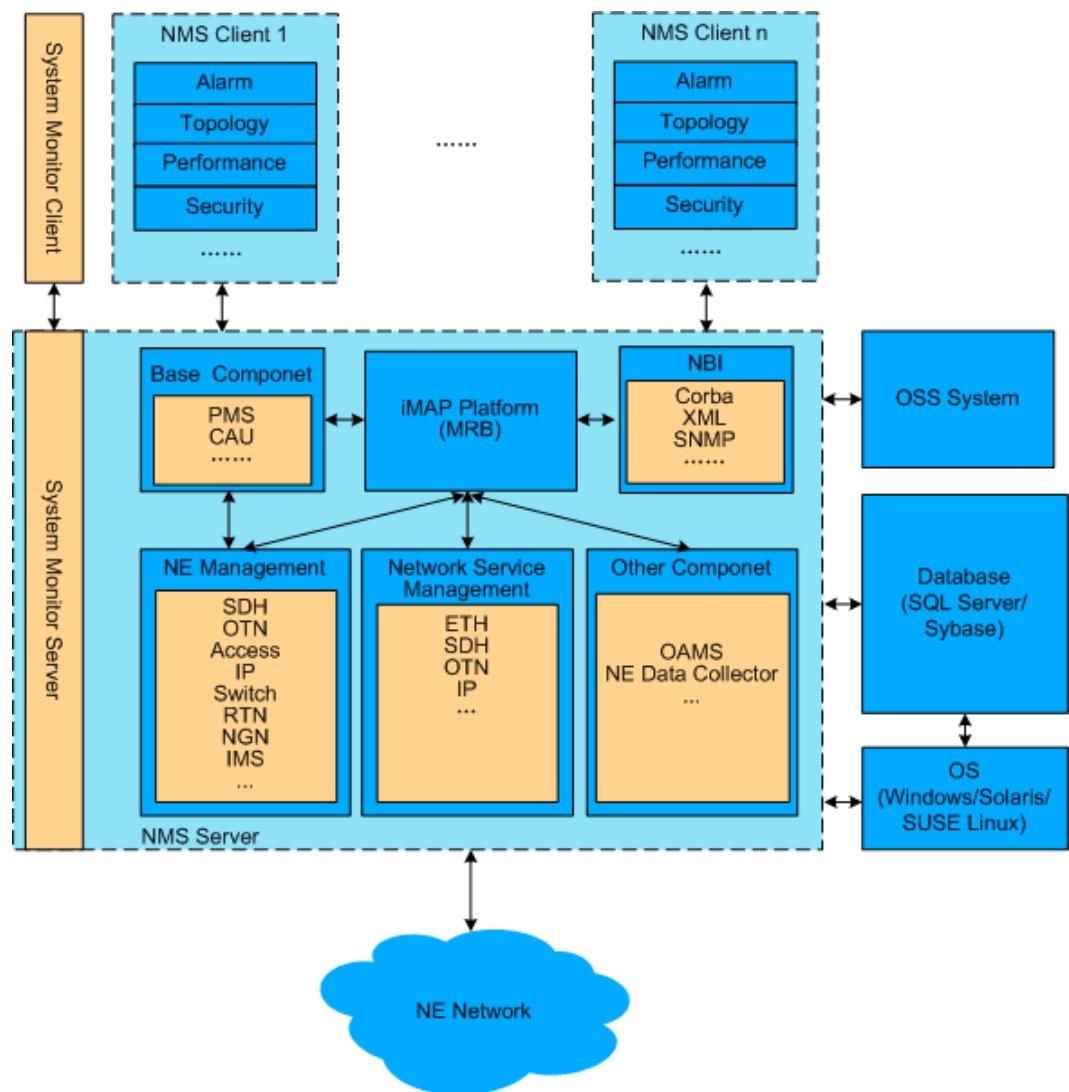
U2000 FusionSphere VM solution also supports the decoupling solution. Specifically, Huawei provides the U2000 FusionSphere VM installation solution when a user provides the FusionSphere virtualization environment. In this decoupling solution, as long as user-provided FusionSphere VMs meet the hardware configuration requirement of the U2000 FusionSphere VM solution, the U2000 can be installed on them, irrespective of the server used by bottom hardware.

3 Software Architecture

This topic describes the software architecture of the U2000 single-server system and U2000 HA system.

Figure 3-1 shows the structural relationships between the main modules of the U2000 system.

Figure 3-1 U2000 software architecture



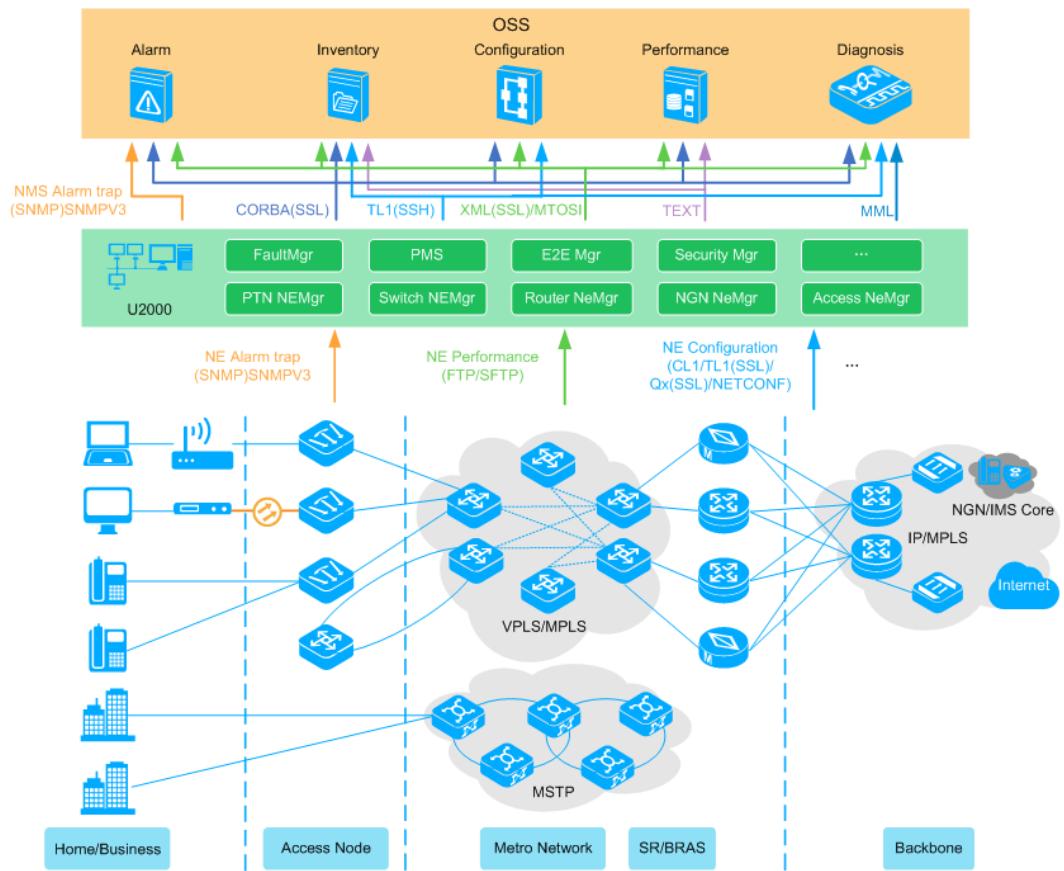
4 External Interfaces

About This Chapter

The U2000 offers abundant northbound interfaces (NBIs) that help to achieve unified management of transport, IP and access equipment; fast integration between OSSs and the U2000; and better quality of customer services. Currently, NBIs jointly developed by Huawei and mainstream OSS vendors are widely used by 90% of the top 50 carriers worldwide.

In addition to conventional NBIs such as TL1, SNMP, and CORBA NBIs, the U2000 offers the XML NBI that is based on MTOSI 2.0 standards. The XML NBI provides multiple extensible functions, including alarm management, inventory management, performance management, configuration management, and diagnostic tests. By using these interfaces, the U2000 can quickly and dynamically integrate with OSSs. [Figure 4-1](#) shows the functions of the external interfaces.

Figure 4-1 Functions of the external interfaces



4.1 NBI

The U2000 offers network monitoring information, such as the alarm, performance, and inventory information, for OSSs through northbound interfaces (NBIs). The NBIs support network management functions, such as service configuration and diagnostic tests. Through NBIs, the U2000 can integrate with different OSSs flexibly.

4.2 SBI

Using the southbound interface (SBI), the U2000 can connect to and manage NEs.

4.1 NBI

The U2000 offers network monitoring information, such as the alarm, performance, and inventory information, for OSSs through northbound interfaces (NBIs). The NBIs support network management functions, such as service configuration and diagnostic tests. Through NBIs, the U2000 can integrate with different OSSs flexibly.

The equipment of each product domain supports different NBI functions. For details, see the following tables.

Table 4-1 NBI functions supported by transport equipment

Interface	Feature	MSTP	Hybrid MSTP	WDM	OTN	Hybrid RTN (TDM)	TDM RTN	Packet RTN	PTN	Marine
XML (MTOSI)	Alarm	√	√	√	√	√	√	√	√	×
	Performance	√	√	√	√	√	√	√	√	×
	Inventory	√	√	√	√	√	√	√	√	×
	Configuration	√	√	√	√	√	√	√	√	×
CORBA	Alarm	√	√	√	√	√	√	√	√	√
	Performance	√	√	√	√	√	√	√	√	√
	Inventory	√	√	√	√	√	√	√	√	√
	Configuration	√	√	√	√	√	√	√	√	×
SNMP	Alarm	√	√	√	√	√	√	√	√	×
Performance NBI	Performance	√	√	√	√	√	√	√	√	×

Table 4-2 NBI functions supported by access equipment

Interface	Feature	MSAN/DSLAM		FTTx		D-CCAP
		Narrowband Port	Broadband Port	FTTH	FTTB/C	
XML (MTOSI)	Alarm	√	√	√	√	×
	Performance	×	×	√	√	×
	Inventory	√	√	√	√	×
	Configuration	√	√	√	√	×

Interface	Feature	MSAN/DSLAM		FTTx		D-CCAP
		Narrowband Port	Broadband Port	FTTH	FTTB/C	
CORBA	Alarm	√	√	√	√	√
SNMP	Alarm	√	√	√	√	√
Performance text NBI	Performance	√	√	√	√	√
TL1	Diagnosis	√	√	√	√	√
	Inventory	√	√	√	√	√
	Configuration	√	√	√	√	×
Customer OSS test	Diagnosis	√	√	×	×	×

Table 4-3 NBI functions supported by IP equipment

Interface	Feature	NE Series	CX Series	Switch	BRAS	ATN	Security Series	PTN
XML (MTOSI)	Alarm	√	√	√	√	√	×	√
	Performance	√	√	×	×	√	×	√
	Inventory	√	√	√	√	√	×	√
	Configuration	√	√	√	√	√	×	√
CORBA	Alarm	√	√	√	√	√	×	√
SNMP	Alarm	√	√	√	√	√	√	√
Performance text NBI	Performance	√	√	√	√	√	×	√

Supported	√
-----------	---

Not supported	×
---------------	---

4.1.1 XML NBI

This topic describes the U2000 XML NBI functions.

Technical Specifications

Table 4-4 Performance indicators of the XML NBI

Item	Indicator
Number of OSS connections received concurrently	10
Delay of response to XML request	<ul style="list-style-type: none">When querying a small amount of data (for example, the number of returned managed element is smaller than 1000) from the U2000, the XML interface returns all information within three seconds (when the CPU usage is lower than 50%). When querying from NEs, however, the XML interface spends more time, depending on the network and NE statuses.When querying a large quantity of alarms, the XML interface handles at least 100 alarms per second.
Alarm notification processing capability	More than 60 records per second when 3 OSSs are connected
Alarm notification transmission delay	Shorter than 10s when 3 OSSs are connected
Maximum invocation concurrency of the XML interfaces that involve a large amount of data (including getInventory, getInventoryIterator, and executeCLI)	1
Size of an SOAP request packet	500,000 characters

Transport

Complying with the TMF MTOSI 2.0 series standards, the XML NBI enables the U2000 to provide unified alarm, performance, inventory, and configuration management on transport equipment for OSSs.

The XML NBI supports the following functions:

- **Alarm management**

- Alarm reporting
- Synchronization of active alarms
- Alarm acknowledgment
- Alarm unacknowledgment
- Alarm clear
- Collection of alarm statistics
- **Performance management**
 - Query of historical performance data
 - Query of current performance data
 - Reporting of performance threshold-crossing events
 - Query of performance threshold-crossing events
 - PTN performance instance management (creation, deletion, suspension, enabling, and query)
- **Inventory management**
 - Query of physical inventory, such as NEs, subracks, slots, boards, and physical ports
 - Query of logical inventory, such as logical ports, fibers or cables, cross-connections, and trails
 - Export of inventory data
 - Report of changes in inventory
- **Configuration management**
 - E2E WDM trail management, including creating, deleting, activating, deactivating, and modifying E2E WDM trails
 - E2E OTN trail management, including creating, deleting, activating, deactivating, and modifying E2E OTN trails
 - MS OTN E2E EPL/EPlan/TrunkLink/SDH trail management (creation, deletion, activation, and deactivation)
 - MS OTN E2E PWE3/VPLS trail management (creation, deletion, activation, deactivation, and modification)
 - MSTP+ E2E PWE3/VPLS trail management (creation, deletion, activation, deactivation, and modification)
 - Hybrid MSTP trail management, including creating, deleting, activating, deactivating, and modifying E2E Hybrid MSTP trails
 - E2E EoO/EoW trail management, including creating, deleting, activating, and deactivating E2E EoO or EoW trails
 - Link (fiber and Layer 2 link) management, including creating and deleting link
 - Per-NE-based services management for L2VPN/L3VPN/NativeEth of PTN/RTN, including creating, deleting, activating, deactivating, and modifying service
- **Protection group management**
 - SNCP protection (query and switching)
 - NE tunnel APS (creation, deletion, query, and switching)
 - SDH MSP (query and switching)
 - WDM OCP or OLP (query and switching)

- NE protection (query and switching)
- E2E tunnel APS (TNP) management (query, creation, and deletion) of Hybrid MSTP NEs

Access

Complying with the TMF MTOSI 2.0 series standards, the XML NBI enables the U2000 to provide unified alarm, performance, inventory, and configuration management on access equipment for OSSs. **Table 4-4** lists the performance indicators of the XML NBI.

The XML NBI supports the following functions:

- **Alarm management**
 - Alarm reporting
 - Synchronization of active alarms
 - Alarm acknowledgment
 - Alarm unacknowledgment
 - Alarm clear
 - Collection of alarm statistics
 - TCA synchronization
- **Performance management**
 - Query of historical performance data
- **Inventory management**
 - Query of IP DSLAM inventory (ADSL ports, SHDSL port, templates)
 - Query of GPON physical inventory such as NEs, slots, boards, and physical ports
 - Query of GPON logical inventory such as VLANs and services
 - Query of TL inventory (fibers/cables)
 - Query of QoS templates
 - Query of service ports
 - Querying RU information
 - Querying ANCP information (including ADSL and VDSL2)
- **Configuration management**
 - FTTH (GPON) service creation, modification, deletion, activation, and deactivation
 - FTTB/FTTC (GPON) service creation, modification, deletion, activation, and deactivation
 - xDSL configuration (including ADSL and VDSL2)
 - Service port management (creation, deletion, activation, and deactivation)
 - RU management (creation, deletion, modification)
 - ANCP information configuration (including ADSL and VDSL2)
- **Access diagnosis management**
 - xDSL port test (including ADSL and VDSL2)
 - Port loopback
 - OAM detection
 - ONT management

In addition, the U2000 supports the XML NBI that complies with the SOAP protocol in the access domain to provide functions such as VDSL2, GPON, service port, and multicast configuration and inventory queries for the OSS in a customized manner. For the details, see [4.1.4 TL1 NBI for Access Equipment](#). If an office requires the XML interface for interconnection, contact Huawei engineers to customize the wsdl files and documents based on the customer's service requirements.

Table 4-5 lists the performance indicators of the XML NBI.

Table 4-5 Performance indicators of the XML NBI

Item	Specification
Maximum number of OSS connections that can be received at one time	15
Processing capability for requesting commands of XML	10 per second (only for configuration commands)
Response time for requesting commands of XML	Within two minutes (excluding test commands)

IP

Complying with the TMF MTOSI 2.0 series standards, the XML NBI enables the U2000 to provide unified alarm, performance, inventory, configuration, diagnostic test, and protection group management on IP equipment for OSSs.

The XML NBI supports the following functions:

- **Alarm management**
 - Alarm reporting
 - Synchronization of active alarms
 - Alarm acknowledgment
 - Alarm unacknowledgment
 - Alarm clear
 - Collection of alarm statistics
 - Synchronization of correlative alarms
- **Performance management**
 - Query of historical performance data
 - Query of performance threshold-crossing events
 - Performance instance management, including creating, deleting, enabling, suspending, and querying performance instances
- **Inventory management**
 - Query of physical inventory, such as NEs, subracks, slots, boards, and physical ports
 - Query of logical inventory such as logical ports, fibers or cables, tunnels, and services

- Export of inventory data and reporting of changes in inventory
- QoS management (query, creation, deletion, apply, and unapply)
- **Configuration management**
 - Provisioning of tunnel resources (TE Tunnel, static CR Tunnel, Static Tunnel)
 - Provisioning of service resources (ATM PWE3, CES PWE3, Ethernet PWE3, VPLS, L3VPN, and PWSwitch)
- **Diagnostic test management**
 - Management of MDs, MAs, MEPs, MIPs, and RMEPs based on 802.1ag, 802.3ah, and Y.1731 standards
 - CC, LB, and LT tests
 - Management of test suites and test cases
 - BFD session management, including creating, deleting, binding, and unbinding BFD sessions
 - OAM statistics management (query, creation, and execution)
- **Protection group management**
 - E-trunk management, including creating, deleting, and querying E-trunks
 - E-APS management, including creating, deleting, and querying E-APS protection groups

4.1.2 CORBA NBI

This topic describes the U2000 CORBA NBI functions.

Technical Specifications

The U2000 CORBA interface has the following technical specifications.

- The CORBA interface can handle 100 reporting notifications every second.
- For settings that are not applied to NEs, the CORBA interface is able to handle most of them within two seconds. For settings that are applied to NEs, the CORBA interface is able to handle most of them within five seconds.
- When querying a small amount of data (for example, the number of returned managed objects is smaller than 1000) from the U2000, the CORBA interface returns all information within five seconds. When querying from NEs, however, the CORBA interface spends more time, depending on the network and NE statuses.
- When querying a large quantity of alarms, the CORBA interface handles at least 100 alarms per second.
- Maximum concurrency limitations:
 - The maximum invocation concurrency of the CORBA NBI is 4. If the number of invocations exceeds 4, the invocations are queued.
 - For interfaces that involve a large amount of data, such as getAllEquipment and getHistoryPMDData, it takes a long time for the U2000 server to process the interface invocations. The number of concurrent interface invocations is small. Therefore, single-thread serial invocation is recommended. Otherwise, an error indicating a fully loaded task may be reported.

NOTICE

- In the U2000 servers of different configurations, the preceding technical specifications are different.
- The alarm handling capability of the CORBA NBI depends on many factors, such as alarm quantity on the live network, and CPU performance and memory size of the server. At the same time, the CORBA NBI sends alarms synchronously, that is, another alarm will not be sent until the OSS receives the previous alarm and responds to the CORBA NBI. Therefore, the network stability between the U2000 and the OSS and the handling capability of the OSS will affect the alarm handling capability of the U2000.
- If an alarm storm occurs, the CORBA NBI will possibly reach its handling limit. The CORBA NBI can report a maximum of 1,000,000 alarms within one hour. To ensure the stability of the system, the CORBA NBI will discard some alarms if the alarm quantity exceeds 1,000,000. You are recommended to handle network faults instantly if an alarm storm occurs. Also, the OSS is suggested to synchronize alarms actively at proper times, for example, when the system is idle.

Transport

Complying with the TMF MTNM V3.5 series standards, the CORBA NBI enables the U2000 to provide unified alarm and inventory management. The CORBA NBI also enables the U2000 to provide service configuring, performance, diagnostic test, and protection group management for transport equipment.

The CORBA NBI supports the following functions:

- **Alarm management**
 - Alarm reporting
 - Synchronization of active alarms
 - Alarm acknowledgment
 - Alarm unacknowledgment
 - Alarm clear
- **Performance management**
 - Query of historical performance data
 - Query of current performance data
 - Reporting of performance threshold-crossing events
 - Query of performance threshold-crossing events
- **Inventory management**
 - Inventory change notification reporting
 - Query of physical inventory, such as NEs, subracks, slots, boards, and physical ports
 - Query of logical inventory, such as logical ports, fibers or cables, cross-connections, and trails
- **Configuration management**
 - Provisioning of E2E services (SDH, WDM, OTN, MSTP, ASON, and RTN) in the transport domain

- Provisioning of per-NE-based services (SDH, WDM, OTN, MSTP, and PTN) in the transport domain
- Provisioning of per-NE-based services for tunnels (MPLS tunnels and IP tunnels)
- Provisioning of per-NE-based services (ATM PWE3, CES PWE3, Ethernet PWE3, VPLS and PW Switch)
- Provisioning of E2E services for tunnels(Only for PTN) (Static-CR Tunnel)
- Provisioning of E2E services(Only for PTN) (CES PWE3, Ethernet PWE3)
- **Diagnostic test management (RTN and PTN)**
 - Port loopback and alarm insertion
 - Ethernet CC, LB, and LT tests
 - OAM management for MPLS LSP, PW, PWE3 and VPLS services
- **Protection group management (SDH, WDM, OTN, PTN, RTN, Hybrid MSTP)**
 - Board protection, including querying protection groups and performing switching
 - Port protection, including querying protection groups and performing switching
 - Subnetwork connection protection (SNCP) protection, including querying protection groups and performing switching
 - Tunnel APS protection, including creating, deleting and querying Tunnel APS protection groups
 - E2E tunnel APS (TNP) management (query, creation, and deletion)

Access

Complying with the TMF MTNM V3.5 series standards, the CORBA NBI enables the U2000 to provide unified alarm management.

The CORBA NBI supports the following functions:

- **Alarm management**
 - Alarm reporting
 - Synchronization of active alarms
 - Alarm acknowledgment
 - Alarm unacknowledgment
 - Alarm clear

IP

Complying with the TMF MTNM V3.5 series standards, the CORBA NBI enables the U2000 to provide unified alarm management.

The CORBA NBI supports the following functions:

- **Alarm management**
 - Alarm reporting
 - Synchronization of active alarms
 - Alarm acknowledgment
 - Alarm unacknowledgment
 - Alarm clear

4.1.3 SNMP NBI

Complying with the SNMP v1/v2c/v3 standard, the SNMP NBI enables the U2000 to provide unified alarm management for OSSs.

Technical Specifications

Table 4-6 Performance Indicators for the SNMP NBI

Indicator	Description
Maximum number of concurrent OSS connections	10
Alarm forwarding efficiency	No less than 60 alarms per second (for three OSS connections)
Alarm forwarding delay	Less than 10 seconds (three OSS connections)
SNMP request response delay	Less than 5 seconds (CPU usage is less than 50%)

Function

The SNMP NBI supports the following functions:

- Alarm reporting
- Synchronization of active alarms
- Alarm acknowledgment
- Alarm unacknowledgment
- Alarm clear
- Heartbeat alarm reporting
- Setting of alarm filter criteria
- Alarm maintenance status reporting

4.1.4 TL1 NBI for Access Equipment

Complying with the GR 831 standard, the TL1 NBI enables the U2000 to provide service provisioning (xDSL, xPON, broadband, and narrowband services) and inventory query in the access domain for OSSs.

The TL1 NBI supports the functions of service provisioning, inventory query and diagnosis test functions, and uses the default port 9819.

Performance Indicators

Table 4-7 Performance indicators of the TL1 NBI

Item	Specification
Maximum number of OSS connections that can be received at one time	<ul style="list-style-type: none"> ● Common- and medium-sized networks: 20 <ul style="list-style-type: none"> - Service provisioning: 15 - Inventory query: 2 - Diagnosis test: 3 ● Large- and ultra large-sized networks: 30 <ul style="list-style-type: none"> - Service provisioning: 20 - Inventory query: 2 - Diagnosis test: 8 <p>NOTE For details about the mapping between the network scale and server configurations, see 5.1.1 Hardware Configuration.</p>
Processing capability for requesting commands of TL1	10 per second (only for configuration commands)
Response time for requesting commands of TL1	Within two minutes (excluding test commands)

Function

The TL1 NBI supports the following functions:

- **Service provisioning**
 - Provisioning of xDSL (ADSL, G.SHDSL, and VDSL2) services
 - Provisioning of G.fast services
 - Provisioning of multicast services
 - Provisioning of xPON (GPON and EPON) services
 - Provisioning of CNU services
 - Provisioning of CM services
 - Management of VLANs
 - Management of Ethernet ports
 - Management of service ports
 - Management of PVCs
 - Provisioning of voice (VoIP, PSTN, ISDN, and SPC) services
 - Management of ACL&QoS and HQoS
- **Inventory query**
 - Querying various resources, such as devices, xDSL (including ADSL, G.SHDSL, and VDSL2 resources), G.fast, video, xPON (including GPON and EPON resources), CNU, CM, VLAN, Ethernet, service port, PVC, voice (VoIP, PSTN, ISDN, and SPC), ACL&QoS, and HQoS resources

- Notification of resource changes
- **Diagnostic test**
 - Line Test
 - ETH OAM

4.1.5 Performance Text NBI

The Performance Text NBI enables the U2000 to export performance statistics for OSSs. The U2000 exports performance statistics to a specified FTP server for analysis.

Technical Specifications

Table 4-8 Indicators of the U2000

Item	Indicator
Maximum number of connected OSSs	<ul style="list-style-type: none">● As the FTP client, the U2000 transmits files to one OSS only.● As the FTP server, the U2000 can be visited by a maximum of three OSSs.

Function

The Performance Text NBI supports the following functions:

- Generates the performance text file in a unified format (*.csv).
- Exports the performance text file based on the collection period (the period can be 5, 10, 15, 30, 60, 360, or 1440 minutes).
- Exports the performance text file at the scheduled time (5, 10, 15, 30, 60, 360, or 1440 minutes, the time must be longer than the collection period).
- Specifies the start time to export the performance text file.
- Checks data integrity of the performance text file. If the performance text file fails to be generated, the data will be saved to the performance text file which will be generated in the next period. (SDH, WDM and OTN performance data does not support this function.)
- Transmits the performance text file to the specified FTP or SFTP server.
- Exports the performance text file by indicator.
- Specifies the start time to delete the performance text file.
- Clears earlier performance text file periodically.
- Specifies the number of data records in a single file.

4.1.6 Customer OSS Test NBI for Access Equipment

The customer OSS test NBI includes two types of NBI: narrowband line test NBI and ADSL line test NBI. Narrowband line test NBI provides tests on narrowband access devices (lines and terminals). ADSL line test NBI provides query on ADSL ports, and line capture and line release on ADSL lines.

Performance Indicators

Item	Specification
Maximum number of connections	64 clients
Connection duration	After a connection is set up, if the client does not send a command in one hour, the connection is automatically disconnected.

Function

The customer OSS test NBI supports the following functions:

- **Narrowband line test NBI**
 - Dial tone test for POTS users
 - Feed voltage test for POTS users
 - Loop current test for POTS users
 - Line test for POTS users
 - Ringing test for POTS users
 - DTMF or pulse test for POTS users
 - Howler tone test for POTS users
 - Circuit test for ISDN users
 - Line test for ISDN users
 - NT1 terminal test for ISDN users
 - Narrowband line capture test
 - Narrowband line release test
 - Ringing current voltage test
 - Stopping a test
- **ADSL line test NBI**
 - Query of the information about an ADSL user port
 - Control of the DSLAM test bus
 - Loopback diagnostic tests performed at the central office end on the user port
 - OAM test

4.2 SBI

Using the southbound interface (SBI), the U2000 can connect to and manage NEs.

Table 4-9 SBI functions supported by transport equipment

SBI Type	Interface Description	supported equipment
Qx	A Qx interface is a private communication interface simplified based on ITU-T Q3 interface regulations and works in compliance with the standard TCP/IP management protocol. It can transmit data through in-band DCC/ECC or out-band communication medium and features fewer costs, standard structure, and high efficiency. The U2000 automatically adapts to different protocol types.	All transport product
TFTP/FTP/ SFTP	<p>TFTP, FTP, and SFTP are TCP/IP-based network management protocols at the application layer and are dependent on the UDP protocol.</p> <ul style="list-style-type: none"> ● Trivial File Transfer Protocol (TFTP) is a simple and low-overhead protocol (as compared with FTP and SFTP) used to upload and download files. The TFTP protocol does not support password configuration and transfers file contents in plain text. ● File Transfer Protocol (FTP) is a set of standard protocols used for transferring files on networks. The FTP protocol transfers passwords and file contents in plain text. ● SSH FTP (SFTP) uses the SSH protocol to provide secure file transfer and processing. For data backup using the SFTP protocol, passwords and data are encrypted during transmission. <p>Transport NEs use the DC to implement functions such as NE upgrades, backup, and patch installation.</p>	All transport product
Syslog	<p>The Syslog SBI serves as an interface for the U2000 to receive system logs from NEs. With the Syslog SBI, the U2000 can manage NE logs.</p> <p>Transport NEs support NE security logs and running logs.</p>	All transport product (PTN 6900 series NEs do not support NE security logs.)
Netconf	<ul style="list-style-type: none"> ● The NETCONF protocol is used to manage configuration data and network devices. This protocol is designed to supplement the SNMP and Telnet protocols for network configuration. ● The NETCONF protocol defines a simple mechanism for installing, manipulating, and deleting the configurations of network devices. NETCONF uses XML-based data encoding for the configuration data and protocol messages. In an automatic network configuration system, NETCONF plays a crucial role. 	Only OptiX OSN 9600/9800 series based on the VRP8 platform support this interface.

SBI Type	Interface Description	supported equipment
TL1	The TL1 interfaces comply with GR-811-CORE and GR-831-CORE.	Only NAWDM and NANGWDM NEs support.

Table 4-10 SBI functions supported by IP equipment

SBI Type	Interface Description	NE Series	CX Series	Switch	BRA	ATN	Security Series
SNMP	<p>SNMP is a TCP/IP-based network management protocol at the application layer. SNMP uses the UDP protocol at the transmission layer. Through the SNMP SBI, the U2000 can manage network equipment that supports agent processes.</p> <p>The U2000 supports the SNMP SBI that complies with SNMP v1, SNMP v2c, and SNMP v3. Through the SNMP SBI, the U2000 can connect to equipment. The SNMP SBI supports basic management functions such as auto-discovery of network devices, service configuration, data synchronization, fault management, and performance management.</p>	√	√	√	√	√	√

SBI Type	Interface Description	NE Series	CX Series	Switch	BRA	ATN	Security Series
Telnet/ STelnet	<p>The Telnet and STelnet SBIs are a basic type of interface used for remote login to and management of NEs. The Telnet and STelnet SBIs address the disadvantages of the SNMP SBI and allow the U2000 to provide more management functions.</p> <ul style="list-style-type: none"> ● Telnet is a TCP/IP-based network management protocol at the application layer. Through the Telnet SBI, users can log in to an NE in the CLI and run commands directly in the CLI to maintain and configure the NE. Using the TCP protocol at the transmission layer, the Telnet protocol provides services for network communication. The Telnet protocol transmits communication data in plain text, which is not secure. ● STelnet provides secure Telnet services based on SSH connections. Providing encryption and authentication, SSH protects NEs against attacks of IP address spoofing. 	√	√	√	√	√	√

SBI Type	Interface Description	NE Series	CX Series	Switch	B R A S	A T N	Secur ity Serie s
TFTP/FTP/SFTP	<p>TFTP, FTP, and SFTP are TCP/IP-based network management protocols at the application layer and are dependent on the UDP protocol.</p> <ul style="list-style-type: none"> ● Trivial File Transfer Protocol (TFTP) is a simple and low-overhead protocol (as compared with FTP and SFTP) used to upload and download files. The TFTP protocol does not support password configuration and transfers file contents in plain text. ● File Transfer Protocol (FTP) is a set of standard protocols used for transferring files on networks. The FTP protocol transfers passwords and file contents in plain text. ● SSH FTP (SFTP) uses the SSH protocol to provide secure file transfer and processing. For data backup using the SFTP protocol, passwords and data are encrypted during transmission. <p>Routers and switches whose VRP version is 5.7 or later use the TFTP, FTP, or SFTP SBI to synchronize data with the U2000. IP NEs use the DC to implement functions such as NE upgrades, backup, and patch installation.</p>	√	√	√	√	√	√
Syslog	The Syslog SBI serves as an interface for the U2000 to receive system logs from NEs. With the Syslog SBI, the U2000 can manage NE logs. IP NEs support Syslog running logs.	√	√	√	√	√	√
ICMP	ICMP is a network-layer protocol. It provides error reports and IP datagram processing messages that will be sent back to the source. ICMP is usually used as an IP-layer or higher-layer protocol and ICMP packets are usually encapsulated in IP data packets for transmission. Some ICMP packets carry error packets that will be sent back to NEs.	√	√	√	√	√	√

SBI Type	Interface Description	NE Series	CX Series	Switch	B R A S	A T N	Secur ity Serie s
Netconf	<ul style="list-style-type: none"> ● The NETCONF protocol is used to manage configuration data and network devices. This protocol is designed to supplement the SNMP and Telnet protocols for network configuration. ● The NETCONF protocol defines a simple mechanism for installing, manipulating, and deleting the configurations of network devices. NETCONF uses XML-based data encoding for the configuration data and protocol messages. In an automatic network configuration system, NETCONF plays a crucial role. <p>NOTE Only routers based on the VRP8 platform support this interface.</p>	√	√	×	×	×	×

Table 4-11 SBI functions supported by access equipment

SBI Type	Interface Description	MSA N/ DSL AM	FTTx			D- CC AP
			OLT	MD U	ONT	
SNMP	<p>SNMP is a TCP/IP-based network management protocol at the application layer. SNMP uses the UDP protocol at the transmission layer. Through the SNMP SBI, the U2000 can manage network equipment that supports agent processes.</p> <p>The U2000 supports the SNMP SBI that complies with SNMP v1, SNMP v2c, and SNMP v3. Through the SNMP SBI, the U2000 can connect to equipment. The SNMP SBI supports basic management functions such as auto-discovery of network devices, service configuration, data synchronization, fault management, and performance management.</p>	√	√	√	×	√

SBI Type	Interface Description	MSA N/ DSL AM	FTTx			D- CC AP
			OLT	MD U	ONT	
Telnet/ STelnet	<p>The Telnet and STelnet SBIs are a basic type of interface used for remote login to and management of NEs. The Telnet and STelnet SBIs address the disadvantages of the SNMP SBI and allow the U2000 to provide more management functions.</p> <ul style="list-style-type: none"> ● Telnet is a TCP/IP-based network management protocol at the application layer. Through the Telnet SBI, users can log in to an NE in the CLI and run commands directly in the CLI to maintain and configure the NE. Using the TCP protocol at the transmission layer, the Telnet protocol provides services for network communication. The Telnet protocol transmits communication data in plain text, which is not secure. ● STelnet provides secure Telnet services based on SSH connections. Providing encryption and authentication, SSH protects NEs against attacks of IP address spoofing. 	✓	✓	✓	✗	✓

SBI Type	Interface Description	MSA N/ DSL AM	FTTx			D- CC AP
			OLT	MD U	ONT	
TFTP/FTP /SFTP	<p>TFTP, FTP, and SFTP are TCP/IP-based network management protocols at the application layer and are dependent on the UDP protocol.</p> <ul style="list-style-type: none"> ● Trivial File Transfer Protocol (TFTP) is a simple and low-overhead protocol (as compared with FTP and SFTP) used to upload and download files. The TFTP protocol does not support password configuration and transfers file contents in plain text. ● File Transfer Protocol (FTP) is a set of standard protocols used for transferring files on networks. The FTP protocol transfers passwords and file contents in plain text. ● SSH FTP (SFTP) uses the SSH protocol to provide secure file transfer and processing. For data backup using the SFTP protocol, passwords and data are encrypted during transmission. <p>Access NEs use the TFTP, FTP, or SFTP SBI to synchronize data with the U2000, and use the DC to implement functions such as NE upgrades, backup, and patch installation.</p>	✓	✓	✓	✓	✓
Syslog	The Syslog SBI serves as an interface for the U2000 to receive system logs from NEs. With the Syslog SBI, the U2000 can manage NE logs. Access NEs support Syslog operation logs.	✓	✓	✓	✗	✓

SBI Type	Interface Description	MSA N/ DSL AM	FTTx			D- CC AP
			OLT	MDU	ONT	
ICMP	ICMP is a network-layer protocol. It provides error reports and IP datagram processing messages that will be sent back to the source. ICMP is usually used as an IP-layer or higher-layer protocol and ICMP packets are usually encapsulated in IP data packets for transmission. Some ICMP packets carry error packets that will be sent back to NEs.	✓	✓	✓	✗	✓
TR069	TR069 is also called the CPE WAN Management Protocol. It defines a set of automatic negotiation and interaction protocols between a CPE and an auto-configuration server (ACS) to implement automatic terminal configuration, upgrade, and remote centralized management.	✗	✗	✗	✓	✗

Supported	✓
Not supported	✗

5 Configuration

About This Chapter

The U2000 can be installed and deployed directly on the OS or virtual OS of a physical machine. Deployment of the U2000 on a physical machine or a virtual machine requires certain hardware resources. This topic describes the corresponding software logical structure and hardware/software configuration requirements for deployment of the U2000 on a physical machine or a virtual machine.

5.1 Physical Machine Scenario

For a physical machine, the operating system (OS) is installed on hardware directly. There is no virtualization software layer between the OS and hardware. The U2000 supports installation and deployment on different physical servers.

5.2 Virtual Machine Scenario

A virtual machine (VM) is a software-emulated computer system that provides a complete set of hardware functions but runs in a completely isolated environment. In the U2000 VM solution, the operating system (OS) is installed on a VM and a virtualization software layer exists between the OS and hardware. The VM solution enables applications to run in systems that are independent of each other, significantly improving the working efficiency. The U2000 supports installation and deployment on different virtual servers.

5.3 Configuration of the U2000 Client

This topic describes the requirements for software and hardware configuration of the U2000 client.

5.1 Physical Machine Scenario

For a physical machine, the operating system (OS) is installed on hardware directly. There is no virtualization software layer between the OS and hardware. The U2000 supports installation and deployment on different physical servers.

5.1.1 Hardware Configuration

This topic describes the hardware configuration requirements for the U2000 physical machines server.

Configuration Principles

When planning the hardware configurations of the U2000 server, observe the following principles:

- Select proper hardware configurations according to the network scale, capacity expansion plan, hardware costs, and other information. The hardware configurations cannot be lower than that required by the network scale. For example, a common-scale network can use the hardware configurations for a large-scale network, but a large-scale network cannot use the hardware configurations for a common-scale network.
- If an HA system deployment scheme is used, select the same hardware configurations for the primary and secondary sites.
- Configure independent uninterruptible power supply (UPS) for the NMS server. This can avoid some serious problems such as hardware damage, system restoration failure, and data loss caused by abnormal power failure.

Configuration Requirements

Table 5-1 lists the standard hardware delivery configurations for physical machines of this version. The hardware configurations are the same for single-server systems, cold backup systems and HA (Veritas) systems of different network scales. When the U2000 is re-used, **Table 11-7** lists compatible models in the transport and IP domain and **Table 11-8** lists compatible models in the access domain.

Table 5-1 Mappings between network scales and hardware configurations of physical servers

Network Scale	Server (SUSE Linux-Supported)
Small-scale network: less than 500 equivalent NEs	RH2288H V3 <ul style="list-style-type: none">● CPU: 2 x Xeon 6-core 2.4 GHz● Memory: 64 GB● Hard disk: 8 x 600 GB
Common-scale network: 500-2000 equivalent NEs	RH2288H V3 <ul style="list-style-type: none">● CPU: 2 x Xeon 6-core 2.4 GHz● Memory: 64 GB● Hard disk: 8 x 600 GB <p>NOTE When only access-domain NEs are managed, the server also supports management of a medium-scale network.</p>
Medium-scale network: 2000-6000 equivalent NEs	RH5885H V3 <ul style="list-style-type: none">● CPU: 4 x Xeon 10-core 2.0 GHz● Memory: 64 GB● Hard disk: 8 x 600 GB <p>NOTE When only access-domain NEs are managed, the server also supports management of a large-scale network.</p>

Network Scale	Server (SUSE Linux-Supported)
Large-scale network: 6000-15000 equivalent NEs	<p>RH5885H V3+disk array</p> <ul style="list-style-type: none"> ● CPU: 4 x Xeon 10-core 2.0 GHz ● Memory: 128 GB ● Hard disk: 2 x 600 GB <p>NOTE When only access-domain NEs are managed, the server also manages 20000 equivalent NEs.</p>
Super-large-scale network: 15000-30000 equivalent NEs	<p>RH5885H V3 + disk array</p> <ul style="list-style-type: none"> ● CPU: 4 x E7-8860 18-Core 2.2 GHz ● Memory: 256 GB ● Hard disk: 2 x 600 GB

Table 5-2 Configurations of physical machine disk array

Hardware Configuration Item	Disk Array Hardware Version	Capacity
Delivered: OceanStor 5500 V3	-	48 GB memory, 12 x 600 GB
Compatible: OceanStor S3900 NOTE An M200 controller enclosure is delivered with disk arrays.	V100R005C02 V100R002C00	16 GB memory, 12 x 600 GB

5.1.2 Software Configurations

This topic describes the software that can be configured for the U2000 server, including system software and NMS software, and introduces the logical structure of software on the server.

Software Configuration Requirements

The software for the U2000 physical machines server is as follows:

- System software: It includes the operating system software and database software. [Table 5-3](#) lists the configuration standards for the system software.
- High availability software: It refers to the Veritas software that is applicable to only the high availability system. [Table 5-4](#) lists the high availability software.
- NMS software: It refers to the U2000 developed by Huawei.



The U2000 supports only the OS in Simple Chinese or English.

Table 5-3 OS and database software supported by the U2000

Item	Software Platform	OS Software	Database Software
Delivered software platform	x86 (Linux 64 bit)	SUSE Linux Enterprise Server 11 SP3	SYBASE 15.7 with EBF26397 + SP138
Compatible software platform	x86 (Windows 64 bit)	Windows Server 2008 R2 Standard with SP1 NOTE <ul style="list-style-type: none"> ● The server OS can identify a memory with the size only of 32 GB or lower. If the physical memory of the server exceeds 32 GB, the OS can be installed properly, but only 32 GB memory can be identified and used. ● The U2000 specific to Windows has been restricted since V200R015C50 and will gradually reach EOS. 	MS SQL Server 2008 SP3 Standard
	SPARC (Solaris 64 bit)	Solaris 10 (8/11) + Patch 29.0.1	SYBASE 15.7 with EBF26390 + SP138
	SPARC (Solaris 64 bit)	Solaris 10 (available for upgrade only)	SYBASE 15.0.3 or SYBASE 15.5 (available for upgrade only)
	x86 (Linux 64bit)	SUSE Linux Enterprise Server 10 SP4 (available for upgrade only)	SYBASE 15.5 (available for upgrade only)
Software platform no longer supported	x86 (Windows 32 bit)	Windows Server 2003 R2 Enterprise with SP2	MS SQL Server 2000 SP4 Standard
		Windows 2000 Server	MS SQL Server 7.0 or SQL Server 2000
	SPARC (Solaris 32 bit)	Solaris 8	SYBASE 12.0or SYBASE 12.5
	x86 (Linux 64 bit)	SUSE Linux 10 SP1or SUSE Linux 10 SP2	SYBASE 12.5

Table 5-4 High availability software

Platform	High Availability Software
Solaris	<ul style="list-style-type: none">● Compatible configurations: Veritas 7.1● Compatible configurations: Veritas 6.1 + patch 6.1.1, Veritas 6.0.1 + patch 6.0.5 and Veritas 5.1 + SP1RP4
SUSE Linux	<ul style="list-style-type: none">● Delivered configurations: Veritas 7.1● Compatible configurations: Veritas 6.1 + patch 6.1.1, Veritas 6.0.1 + patch 6.0.5 and Veritas 5.1 + SP1RP4

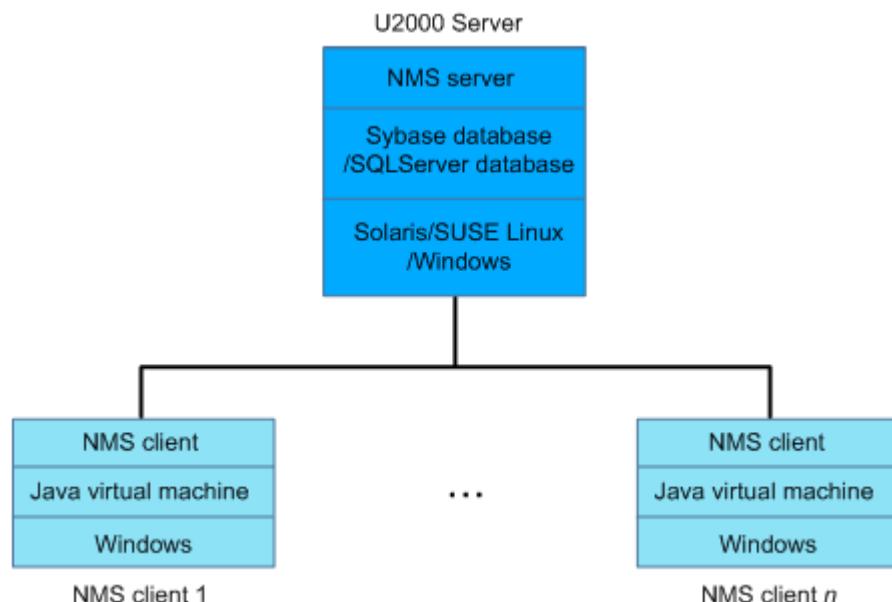
Table 5-5 U2000 software

Configuration Item	Typical Configuration
U2000 software	Installation DVD-ROM or installation software package

Logical Structure of Software

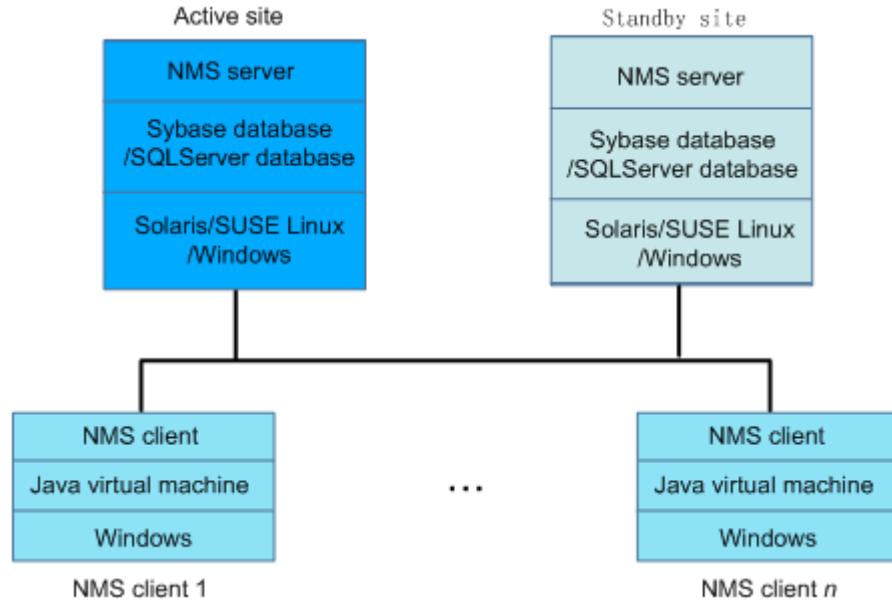
[Figure 5-1](#) shows the software logical structure of the U2000 single-server system.

Figure 5-1 Software logical structure of the U2000 single-server system



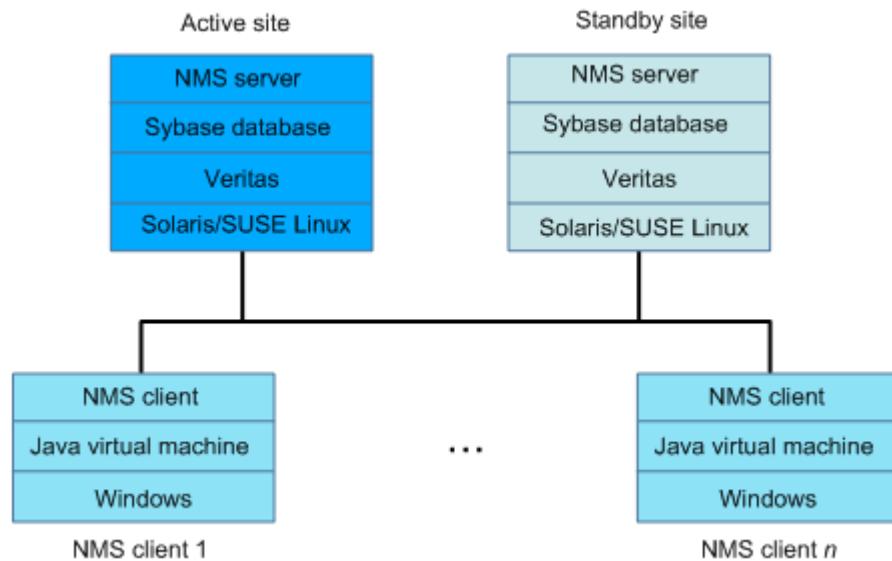
[Figure 5-2](#) shows the structure relationship of the U2000 cold backup system.

Figure 5-2 Software logical structure of the U2000 cold backup system



The U2000 HA system (Veritas Hot Standby) supports Solaris and SUSE Linux. [Figure 5-3](#) shows the software logical structure.

Figure 5-3 Veritas hot standby HA system software architecture



5.2 Virtual Machine Scenario

A virtual machine (VM) is a software-emulated computer system that provides a complete set of hardware functions but runs in a completely isolated environment. In the U2000 VM solution, the operating system (OS) is installed on a VM and a virtualization software layer

exists between the OS and hardware. The VM solution enables applications to run in systems that are independent of each other, significantly improving the working efficiency. The U2000 supports installation and deployment on different virtual servers.

5.2.1 Hardware Configuration

The U2000 can be installed and run on the virtual server of a blade server that is virtualized through VMware or FusionSphere. This topic describes the hardware configuration requirements for the U2000 virtual machines server.

Configuration Principles

When planning the hardware configurations of the U2000 server, observe the following principles:

- Select proper hardware configurations according to the network scale, capacity expansion plan, hardware costs, and other information. The hardware configurations cannot be lower than that required by the network scale. For example, a common-scale network can use the hardware configurations for a large-scale network, but a large-scale network cannot use the hardware configurations for a common-scale network.
- If an HA system deployment scheme is used, select the same hardware configurations for the primary and secondary sites.
- Configure independent uninterruptible power supply (UPS) for the NMS server. This can avoid some serious problems such as hardware damage, system restoration failure, and data loss caused by abnormal power failure.

Configuration Requirements

The standard hardware delivery configurations for the virtual machine solution are E9000 blade servers. The U2000 also supports a decoupling solution, that is, users provide a virtualization environment and Huawei provides a U2000 installation solution.

Table 5-6 Configurations of the E9000 blade server

Item	Configuration
E9000 blade server	In the scenario where a single blade manages no more than 15,000 equivalent NEs, the configurations of each CH242 V3 blade are as follows: <ul style="list-style-type: none">● CPU: 4 x 14-core 2.0GHz CPUs● Memory: 192 GB● Hard disk: 2 x 600 GB
	In the scenario where a single blade manages no more than 30,000 equivalent NEs, the configurations of each CH242 V3 blade are as follows: <ul style="list-style-type: none">● CPU: 4 x 18-core 2.2GHz CPUs● Memory: 256 GB● Hard disk: 2 x 600 GB

Item	Configuration
Disk Array	<p>Delivered: OceanStor 5500 V3 48 GB memory, 24 x 900 GB</p> <p>Compatible: OceanStor S3900 16 GB memory, 24 x 900 GB</p> <p>An M200 controller enclosure is delivered with disk arrays.</p> <p>Hardware version: V100R005C02 or V100R002C00.</p>

Table 5-7 lists the minimum hardware configurations for a single virtual machine when the E9000 blade server solution or decoupling solution is used. The specifications in the table are the default configurations of U2000 for delivery. The decoupling solution requires that the network bandwidth between servers and storage devices is 10 Gbps.

 **NOTE**

- The CPU virtualization ratio must be disabled, that is, the number of virtual CPUs (vCPUs) that can be allocated on a physical host cannot exceed the number of physical CPUs on the host. Otherwise, the U2000 performance will be downgraded.

The CPU virtualization ratio is a proportion of **physical CPUs** to **vCPUs**. For example, if 32 physical CPUs are available and the virtualization ratio is 1:5, the number of vCPUs that can be allocated is 160 (32 x 5). At this moment, the vCPU performance will be downgraded.

- The memory virtualization ratio must be disabled, that is, the size of virtual memory that can be allocated on a physical host cannot exceed the size of physical memory on the host. Otherwise, the U2000 performance will be downgraded.

The memory virtualization ratio is a proportion of **physical memory size** to **virtual memory size**. For example, if 32 GB physical memory is available and the virtualization ratio is 1:5, the size of virtual memory that can be allocated is 160 GB (32 GB x 5). At this moment, the virtual memory performance will be downgraded.

Table 5-7 Mappings between network scales and hardware configurations of a single virtual machine

Network Scale	VMware/FusionSphere Virtual Machine Of Single-Server System	VMware/FusionSphere Virtual Machine Of Remote High Availability System
Small-scale network: less than 500 equivalent NEs	<ul style="list-style-type: none"> ● Virtual CPU per VM: 64-bit, 4-core 2 GHz or higher ● Virtual memory per VM: 16 GB or higher ● Virtual disk space per VM: 400 GB or higher ● VMware: Physical disk's reserved space per VM: 960 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for cloning (virtual disk space} \times 1.2) + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$</p> <ul style="list-style-type: none"> ● FusionSphere: Physical disk's reserved space per VM: 400 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space}$</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 1000 	-

Network Scale	VMware/FusionSphere Virtual Machine Of Single-Server System	VMware/FusionSphere Virtual Machine Of Remote High Availability System
Common-scale network: 500-2000 equivalent NEs	<ul style="list-style-type: none"> ● Virtual CPU per VM: 64-bit, 8-core 2 GHz or higher ● Virtual memory per VM: 32 GB or higher ● Virtual disk space per VM: 400 GB or higher ● VMware: Physical disk's reserved space per VM: 960 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for cloning (virtual disk space} \times 1.2) + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$ </p> ● FusionSphere: Physical disk's reserved space per VM: 400 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space}$ </p> ● Disk IOPS (Input/Output Operations Per Second): 1000 	<ul style="list-style-type: none"> ● Virtual CPU per VM: 64-bit, 8-core 2 GHz or higher ● Virtual memory per VM: 32 GB or higher ● Virtual disk space per VM: 1050 GB or higher. Three hard disks are involved. Their capacities are 300 GB, 650 GB, and 100 GB. ● VMware: Physical disk's reserved space per VM: 1260 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$ </p> ● FusionSphere: Physical disk's reserved space per VM: 1050 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space}$ </p> ● Disk IOPS (Input/Output Operations Per Second): 1000

Network Scale	VMware/FusionSphere Virtual Machine Of Single-Server System	VMware/FusionSphere Virtual Machine Of Remote High Availability System
Medium-scale network: 2000-6000 equivalent NEs	<ul style="list-style-type: none"> ● Virtual CPU per VM: 64-bit, 16-core 2 GHz or higher ● Virtual memory per VM: 32 GB or higher ● Virtual disk space per VM: 400 GB or higher ● VMware: Physical disk's reserved space per VM: 960 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for cloning (virtual disk space} \times 1.2) + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$ </p> ● FusionSphere: Physical disk's reserved space per VM: 400 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space}$ </p> ● Disk IOPS (Input/Output Operations Per Second): 1000 	<ul style="list-style-type: none"> ● Virtual CPU per VM: 64-bit, 16-core 2 GHz or higher ● Virtual memory per VM: 32 GB or higher ● Virtual disk space per VM: 1050 GB or higher. Three hard disks are involved. Their capacities are 300 GB, 650 GB, and 100 GB. ● VMware: Physical disk's reserved space per VM: 1260 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$ </p> ● FusionSphere: Physical disk's reserved space per VM: 1050 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space}$ </p> ● Disk IOPS (Input/Output Operations Per Second): 1000

Network Scale	VMware/FusionSphere Virtual Machine Of Single-Server System	VMware/FusionSphere Virtual Machine Of Remote High Availability System
Large-scale network: 6000-15000 equivalent NEs	<ul style="list-style-type: none"> ● Virtual CPU per VM: 64-bit, 32-core 2 GHz or higher ● Virtual memory per VM: 64 GB or higher ● Virtual disk space per VM: 600 GB or higher ● VMware: Physical disk's reserved space per VM: 1440 GB <p>NOTE</p> <p>Physical disk's reserved space = Virtual disk space + Space reserved for cloning (virtual disk space x 1.2) + Space reserved for snapshots (virtual disk space x 0.2)</p> <ul style="list-style-type: none"> ● FusionSphere: Physical disk's reserved space per VM: 600 GB <p>NOTE</p> <p>Physical disk's reserved space = Virtual disk space</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 1600 	<ul style="list-style-type: none"> ● Virtual CPU per VM: 64-bit, 32-core 2 GHz or higher ● Virtual memory per VM: 64 GB or higher ● Virtual disk space per VM: 1400 GB or higher. Three hard disks are involved. Their capacities are 300 GB, 1000 GB, and 100 GB. ● VMware: Physical disk's reserved space per VM: 1680 GB <p>NOTE</p> <p>Physical disk's reserved space = Virtual disk space + Space reserved for snapshots (virtual disk space x 0.2)</p> <ul style="list-style-type: none"> ● FusionSphere: Physical disk's reserved space per VM: 1440 GB <p>NOTE</p> <p>Physical disk's reserved space = Virtual disk space</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 1600

Network Scale	VMware/FusionSphere Virtual Machine Of Single-Server System	VMware/FusionSphere Virtual Machine Of Remote High Availability System
Super-large-scale network: 15000-30000 equivalent NEs	<ul style="list-style-type: none"> Virtual CPU per VM: 64-bit, 42-core 2 GHz or higher Virtual memory per VM: 128 GB or higher Virtual disk space per VM: 600 GB or higher VMware: Physical disk's reserved space per VM: 1440 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for cloning (virtual disk space} \times 1.2) + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$</p> <ul style="list-style-type: none"> FusionSphere: Physical disk's reserved space per VM: 600 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space}$</p> <ul style="list-style-type: none"> Disk IOPS (Input/Output Operations Per Second): 3000 	<ul style="list-style-type: none"> Virtual CPU per VM: 64-bit, 42-core 2 GHz or higher Virtual memory per VM: 128 GB or higher Virtual disk space per VM: 1400 GB or higher. Three hard disks are involved. Their capacities are 300 GB, 1000 GB, and 100 GB. VMware: Physical disk's reserved space per VM: 1680 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$</p> <ul style="list-style-type: none"> FusionSphere: Physical disk's reserved space per VM: 1440 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space}$</p> <ul style="list-style-type: none"> Disk IOPS (Input/Output Operations Per Second): 3000

5.2.2 Software Configurations

This topic describes the software that can be configured for the U2000 virtual machines server, including virtual software, system software and NMS software, and introduces the logical structure of software on the server.

Software Configuration Requirements

The software for the U2000 server is as follows:

- Virtual machine software: The VM software that supports installation of U2000 includes VMware and FusionSphere, as shown in [Table 5-8](#) and [Table 5-9](#).
- System software: It includes the operating system software and database software. [Table 5-8](#) lists the configuration standards for the system software.
- High availability software: It refers to the Veritas software that is applicable to only the high availability system. [Table 5-10](#) lists the high availability software.
- NMS software: It refers to the NMS software developed by Huawei. For details about the NMS software, see the U2000.



The U2000 supports only the OS in Simple Chinese or English.

Table 5-8 OS and database software supported by the U2000

Item	Software Platform	OS Software	Database Software
Delivered software platform	VMware ESXi 6.5	SUSE Linux Enterprise Server 11 SP3	SYBASE 15.7 with EBF26397 + SP138
	FusionSphere 6.1	SUSE Linux Enterprise Server 11 SP3	SYBASE 15.7 with EBF26397 + SP138
Compatible software platform	VMware ESXi 5.5	SUSE Linux Enterprise Server 10 SP4 (available for upgrade only)	SYBASE 15.5 (available for upgrade only)

Table 5-9 Software configurations of the vSphere Web Client

OS	Browser
Windows	<ul style="list-style-type: none"> ● Mozilla Firefox 34 to 49 ● Google Chrome 39 to 53
Mac OS	<ul style="list-style-type: none"> ● Mozilla Firefox 34 to 49 ● Google Chrome 39 to 53

Table 5-10 High availability software

Platform	High Availability Software
SUSE Linux	<ul style="list-style-type: none"> ● Delivered configurations: Veritas 7.1 ● Compatible configurations: Veritas 6.1 + patch 6.1.1, Veritas 6.0.1 + patch 6.0.5 and Veritas 5.1 + SP1RP4

Table 5-11 U2000 software

Configuration Item	Typical Configuration
U2000 software	Installation DVD-ROM or installation software package

Logical Structure of Software

Install VMware or FusionSphere on the server and configure multiple virtual servers. After the SUSE Linux OS is installed on these virtual servers, install and deploy the U2000. The

U2000 cannot be installed and deployed on the Windows or Solaris OS of a virtual machine. The following figures show the software logical structure of each U2000 VM scheme.

Figure 5-4 Software logical structure of the U2000 single-server VM scheme

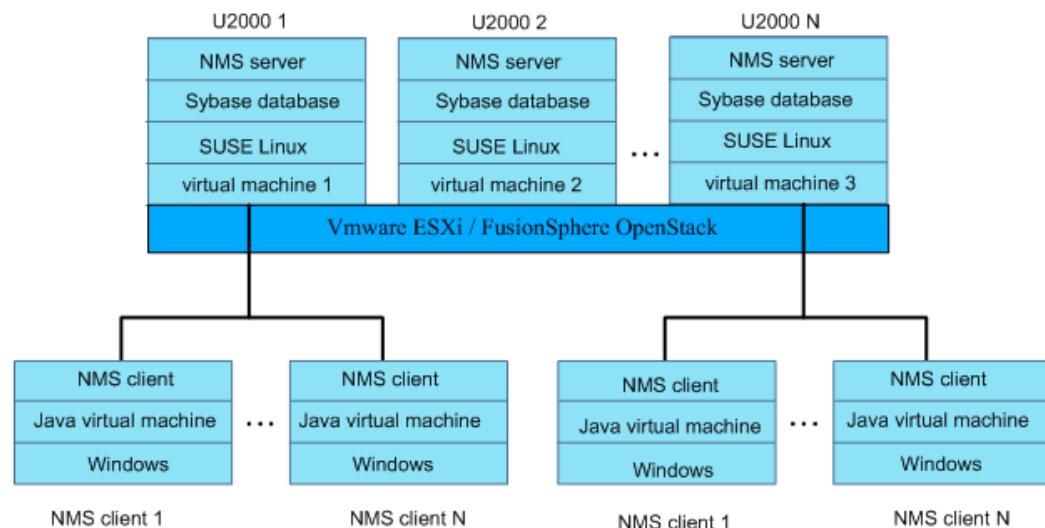
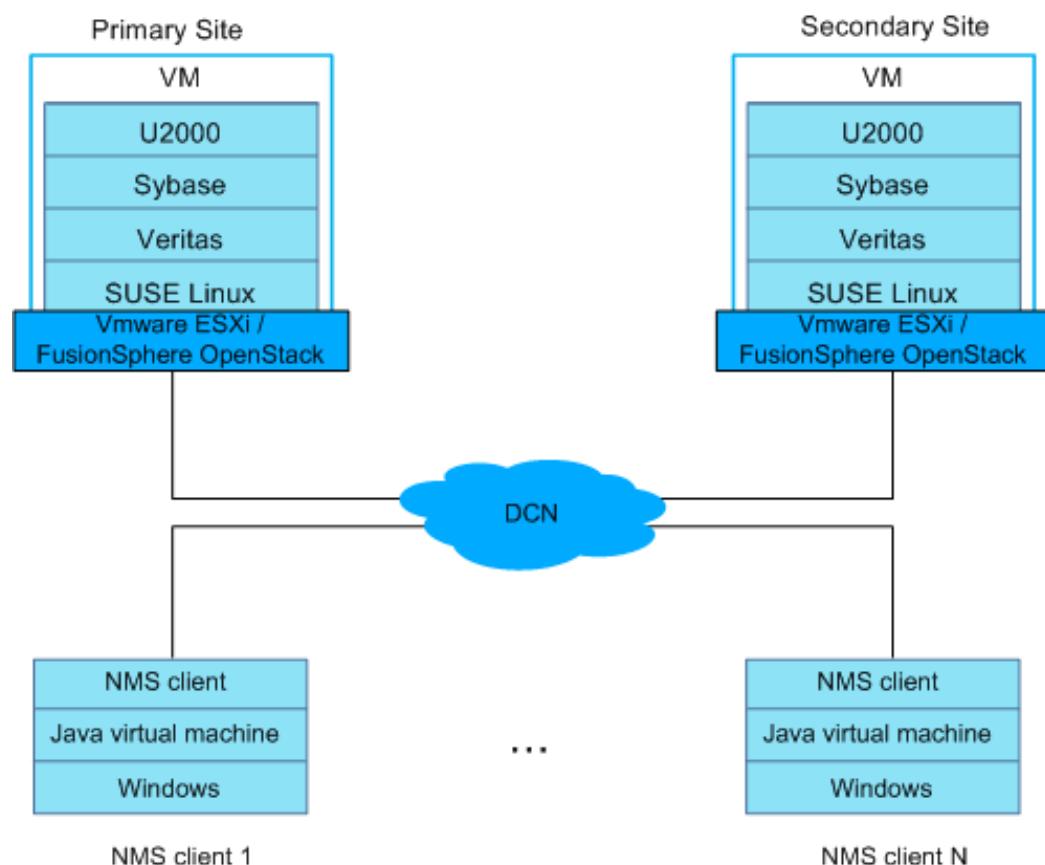


Figure 5-5 Software logical structure of the U2000 HA VM scheme



5.3 Configuration of the U2000 Client

This topic describes the requirements for software and hardware configuration of the U2000 client.

The U2000 client can be installed on Windows. Currently, it cannot be installed on SUSE Linux or Solaris.

The U2000 software can be installed on the OS only with the simplified Chinese or English version instead of other language versions.

Table 5-12 shows the hardware and software configuration.

Table 5-12 Software and hardware configurations for the U2000 client

Platform	Hardware Configuration	Software Configuration	Browser Version
Windows	Minimal configuration requirements: Intel E2140: (dual-core) (1.6 GHz or greater); memory (2 GB or greater)	Recommended OS: <ul style="list-style-type: none">● Windows 10 Professional (64-bit version)● Windows 10 Professional (32-bit version)● Windows 7 Professional (64-bit version)● Windows 7 Professional (32-bit version) Compatible OS: <ul style="list-style-type: none">● Windows Server 2008 R2 Standard (64-bit version)● Windows Server 2012 R2 Standard (64-bit version)	<ul style="list-style-type: none">● Firefox17.X ESR, Firefox24.X ESR or Firefox31.X ESR● IE11(32-bit version)● IE10(32-bit version)● IE9(32-bit version)● U2000 MSO Web client: Chrome 46/47 (recommended browser), IE10 and later versions

6 Networking and Application

About This Chapter

The U2000 provides a unified network-wide management solution for transport, access, IP networks. In addition, the U2000 provides standard external interfaces to integrate with the operating support system (OSS), thereby meeting the management requirements of large-scale networks.

[6.1 Deployment Mode](#)

You can formulate a U2000 deployment scheme based on the network scale, deployment platform, and reliability requirements.

[6.2 Networking Mode Between the U2000 and NEs](#)

The U2000 adopts the widely used C/S (client/server) architecture. In such architecture, the client and the server communicate by means of a LAN or WAN. The U2000 server communicates with managed NEs in inband or outband networking mode. Faults on the U2000 have no impact on networks between managed NEs and services on these NEs.

[6.3 Application Scenarios of U2000 Management](#)

This topic describes typical application scenarios of U2000 management.

6.1 Deployment Mode

You can formulate a U2000 deployment scheme based on the network scale, deployment platform, and reliability requirements.

Table 6-1 provides information about the deployment modes of the U2000.

Table 6-1 Deployment modes of the U2000

Deployment Platform	NMS Deployment Scheme	Supported Platform	Disaster Tolerance Capability	Networking Complexity	Maximum Network Scale
Physical machine	Deployment mode of a single-server system	<ul style="list-style-type: none"> ● Windows ● Solaris ● SUSE Linux 	Low	Simple	<ul style="list-style-type: none"> ● The Windows-based system supports a medium-scale network (a maximum of 6,000 equivalent NEs). ● The Solaris-based system supports an ultra-large-scale network (a maximum of 20,000 equivalent NEs). ● The SUSE Linux-based system supports an ultra-large-scale network (a maximum of 30,000 equivalent NEs).
	Deployment mode of cold backup	<ul style="list-style-type: none"> ● Windows ● Solaris ● SUSE Linux 	Medium	Minor	<ul style="list-style-type: none"> ● The Windows-based system supports a medium-scale network (a maximum of 6,000 equivalent NEs). ● The Solaris-based system supports an ultra-large-scale network (a maximum of 20,000 equivalent NEs). ● The SUSE Linux-based system supports an ultra-large-scale network (a maximum of 30,000 equivalent NEs).

Deployment Platform	NMS Deployment Scheme	Supported Platform	Disaster Tolerance Capability	Networking Complexity	Maximum Network Scale
	Deployment mode of high availability (HA) system	<ul style="list-style-type: none"> ● Solaris ● SUSE Linux 	High	Complex	<ul style="list-style-type: none"> ● The Solaris-based system supports an ultra-large-scale network (a maximum of 20,000 equivalent NEs). ● The SUSE Linux-based system supports an ultra-large-scale network (a maximum of 30,000 equivalent NEs).
Virtual machine	Deployment mode of a single-server system	<ul style="list-style-type: none"> ● VM ware +SUSE Linux ● FusionSphere +SUSE Linux 	Medium	Minor	A Super-large-scale network (a maximum of 30,000 equivalent NEs)
	Deployment mode of cold backup	<ul style="list-style-type: none"> ● VM ware +SUSE Linux ● FusionSphere +SUSE Linux 	Medium	Minor	A Super-large-scale network (a maximum of 30,000 equivalent NEs)

Deployment Platform	NMS Deployment Scheme	Supported Platform	Disaster Tolerance Capability	Networking Complexity	Maximum Network Scale
	Deployment mode of HA system	<ul style="list-style-type: none">● VM ware +SUSE Linux● FusionSphere +SUSE Linux	High	Complex	A Super-large-scale network (a maximum of 30,000 equivalent NEs)

6.1.1 U2000 Deployment on Physical Machines

The U2000 can be installed and deployed on a physical machine. The specific deployment modes include single-server system deployment, cold backup deployment, and high availability (HA) deployment.

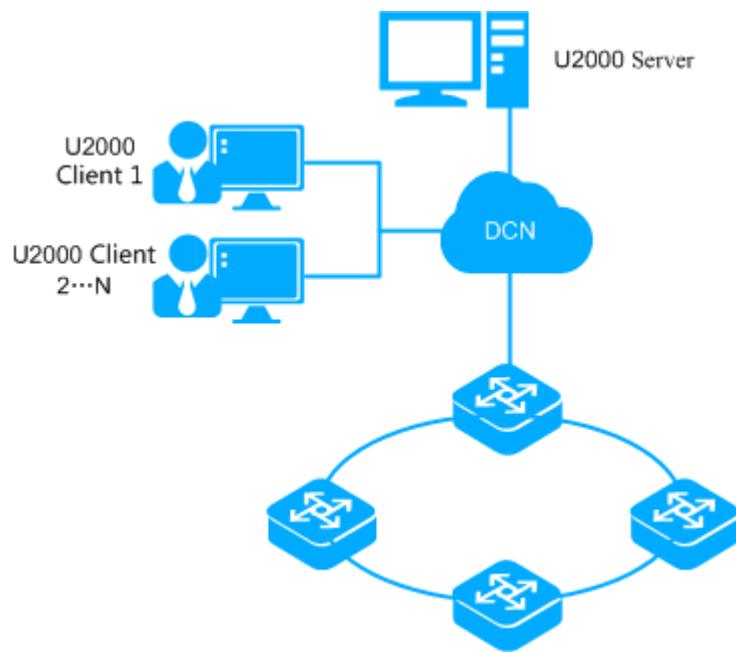
6.1.1.1 Single-Server System Deployment Mode

For the deployment mode of a single-server system, there is only one U2000 server where all processes run. Multiple clients are allowed to connect to and perform operations on the U2000 server.

A single-server system is easy to deploy and cost effective. However, it is not vulnerable to risks and not good at high availability. If a high availability solution is required, you are advised to use the U2000 high availability system deployment solution.

The single-server system is deployed on Windows, Solaris, or SUSE Linux, and supports single-server multiple-client networking schemes. The clients and the server are connected by means of LAN or WAN, as shown in [Figure 6-1](#).

Figure 6-1 Centralized deployment of the single-server system

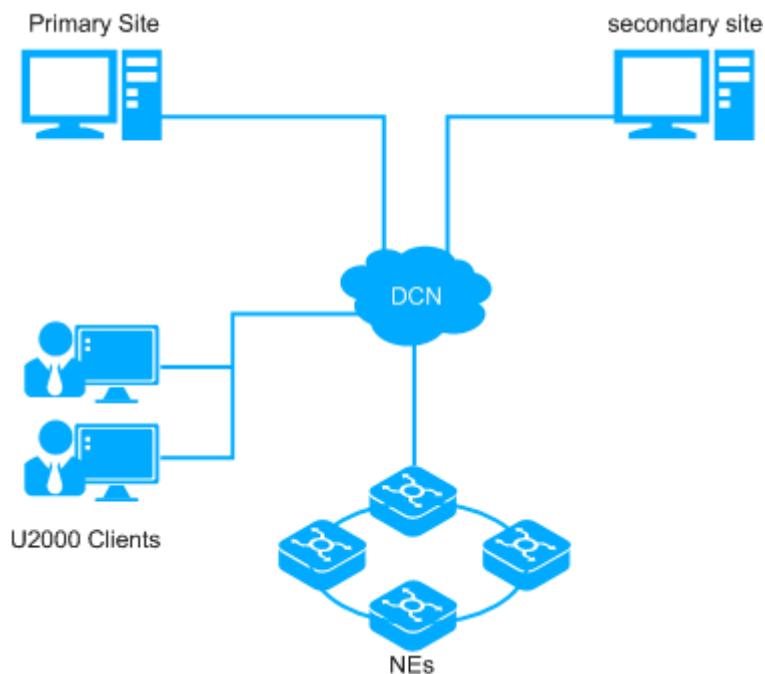


6.1.1.2 Cold Backup Deployment Mode

In the cold backup solution, two single server U2000 systems with the same version, deployment domain, language, OS type, server time, and time zone are deployed. One system is run on the primary site and the other is run on the secondary site.

Figure 6-2 show the deployment Mode.

Figure 6-2 Cold Backup Deployment Mode



- In normal conditions, the primary site provides the network management functions. The network management process and maintenance tool on the secondary site are standby while the database is running. The primary site backs up the network management data periodically, and the secondary site obtains the backup file from the primary site at regular intervals.
- If the U2000 on the primary site fails, the U2000 on the secondary site starts immediately to provide network management functions.

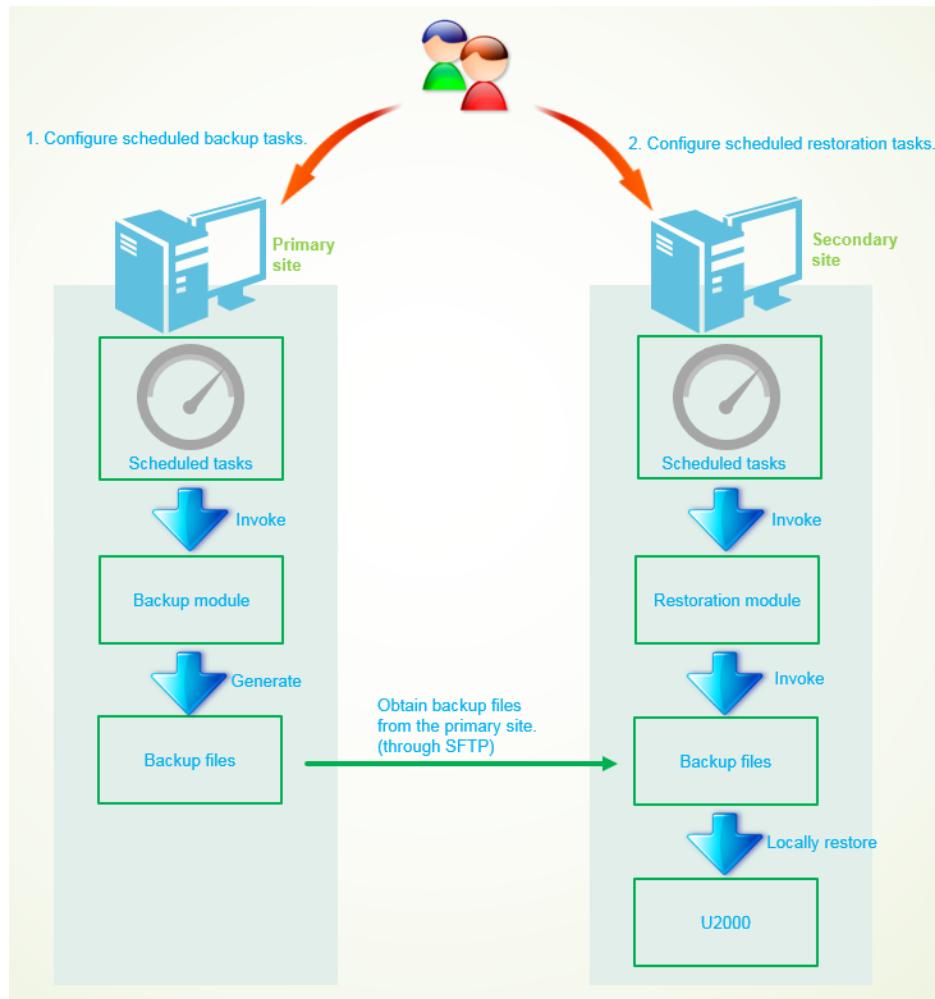
 **NOTE**

- The backup object is the entire database, including the custom data at the U2000 side (excluding the custom options of the system), network layer trail data, NE-side configuration data, alarm data and performance data. In addition, a backup is created for the structure of the entire database, all database tables (including the system tables and the user tables), table structure, and stored procedures. The personal information (including personal name, phone numbers and addresses) on the U2000 and all user names and passwords are also backed up. Therefore, you are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the personal data of users is fully protected.
- The following data is not backed up when you back up the U2000 database:
 - The data that is not saved at the NE side, that is, the data that cannot be uploaded.
 - The custom options of the system. For example, font, color setting, and audio setting.

The fast restoration scheme for the U2000 cold backup system supports manual and automatic backup and restoration. If you use manual backup and restoration, you need to manually start the backup or restoration task each time. If you use automatic backup and restoration is used, you only need to configure a scheduled backup and a scheduled restoration task. The automatic backup and restoration is recommended.

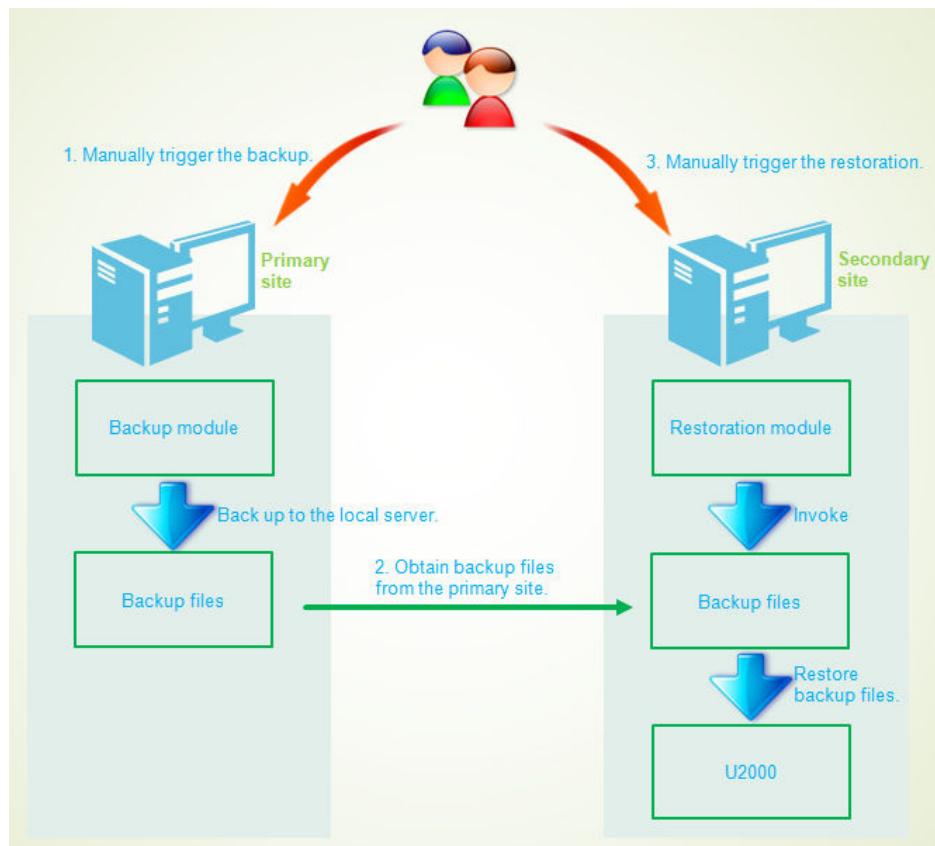
- Automatic backup and restoration scheme: To automatically back up and restore data, you need to configure scheduled backup tasks on the primary site and automatic restoration tasks on the secondary site. The process is as follows:
 - a. On the secondary site, install a single server U2000 whose version, deployment domain, language and database username are the same as those on the primary site.
 - b. Configure scheduled backup tasks on the primary site. The backup files are generated through backup modules and stored on the primary site.
 - c. Configure scheduled restoration tasks on the secondary site. Obtain the backup files through SFTP from the primary site and restore the files on the secondary site.
 - d. When the primary site malfunctions, start the U2000 on the secondary site to fast restore the U2000.

Figure 6-3 Automatic backup and restoration scheme



- Manual backup and restoration scheme: The manual backup and restoration scheme requires a cold backup tool to back up and restore data. The process is as follows:
 - a. On the secondary site, install a single server U2000 whose version, deployment domain, language and database username are the same as those on the primary site.
 - b. Use a cold backup tool to back up the U2000 data on the primary site as backup files and store the files on the primary site.
 - c. Copy the backup files from the primary site to the secondary site, and use the cold backup tool to restore the files on the secondary site.
 - d. Start the U2000 on the secondary site.

Figure 6-4 Manual backup and restoration scheme



6.1.1.3 Deployment of an HA System

This topic describes the principles and networking of the deployment scheme for the high availability (HA) system.

The U2000 is responsible for the management of networks, NEs, and services. A large number of key data is saved on the U2000. Based on the significance of the U2000, it must be an HA system that can run for a 7 x 24 basis and take measures to prevent and handle various disasters. In addition, the U2000 can recover the running of the system and services in time after a disaster occurs. The HA disaster recovery scheme adopts the physical redundancy backup scheme to ensure the automatic startup of the standby system when the software and hardware are faulty. The U2000 provides two HA solutions.

U2000 HA system (Remote)

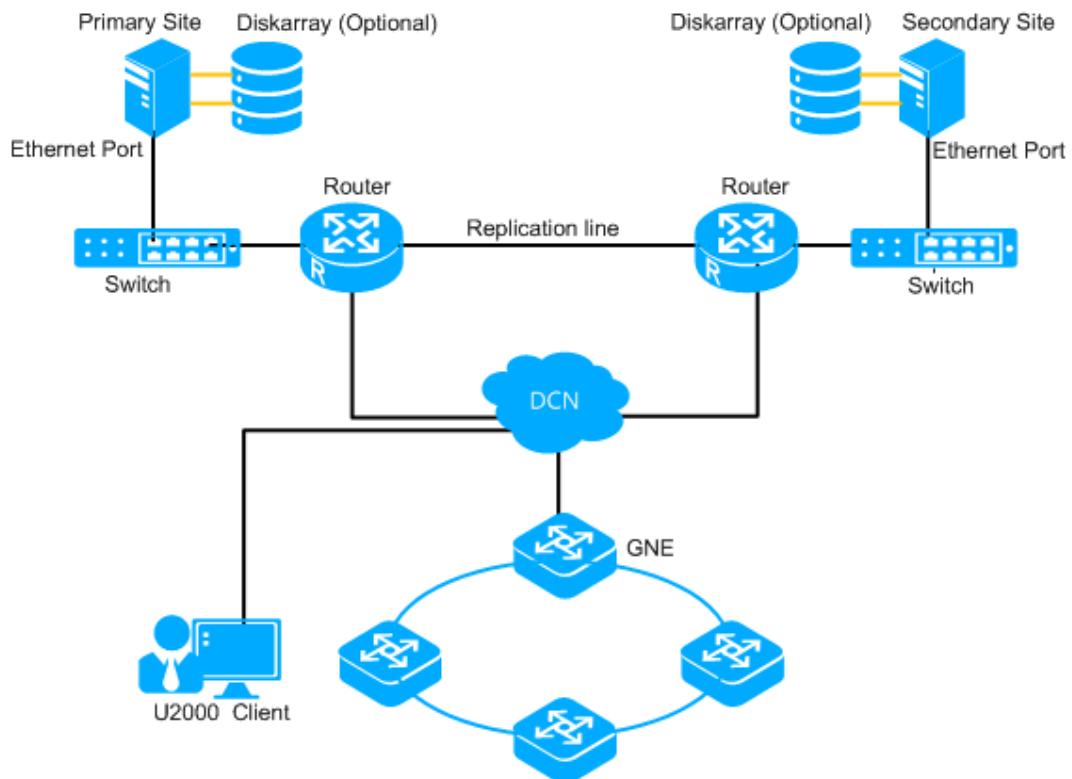
U2000 HA system (remote) solution consists of the primary and secondary sites. The primary and secondary sites can be deployed both on SUSE Linux and Solaris. This solution supports the access and operations on multiple clients. You can deploy the servers of the primary and secondary sites on either the same location or different locations, but the hardware configurations of the primary and secondary sites must be the same. **Figure 6-5** shows the networking diagram of the solution.

The U2000 HA system uses Veritas technology to achieve real-time data synchronization between the primary and secondary sites and to dynamically monitor the operating status of the U2000. If the primary site fails, services are automatically switched to the secondary site.

 **NOTE**

Configure disk arrays according to the number of managed equivalent NEs.

Figure 6-5 Networking diagram for the HA system solution (remote)

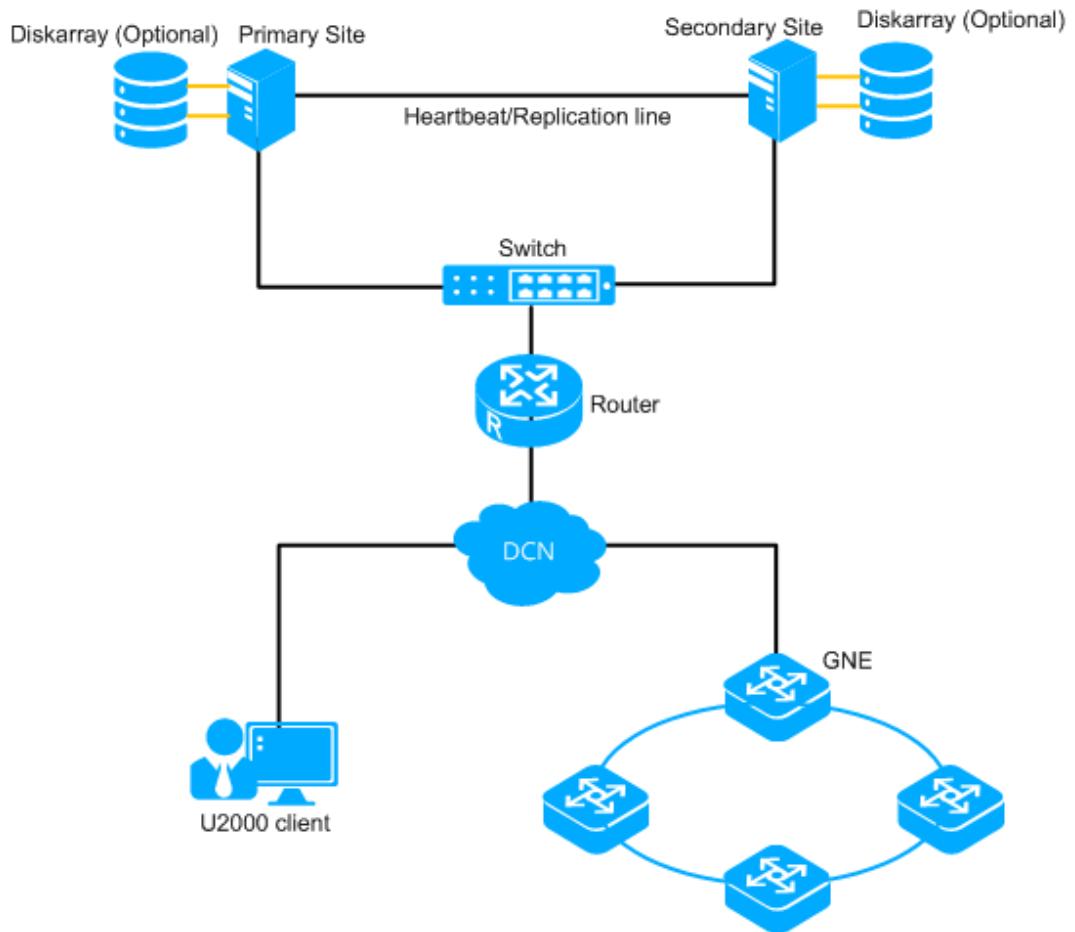


HA System Solution (Local)

The U2000 HA system (local) solution consists of the primary and secondary sites. The primary and secondary sites can be deployed only on SUSE Linux. This solution supports the access and operations on multiple clients. You can deploy the servers of the primary and secondary sites on the same location to ensure that the hardware configurations of the primary and secondary sites are the same. **Figure 6-6** shows the networking diagram of the solution.

The U2000 HA system uses Veritas technology to achieve real-time data synchronization between the primary and secondary sites and to dynamically monitor the operating status of the U2000. If the primary site fails, services are automatically switched to the secondary site.

Figure 6-6 Networking diagram for the HA system solution (local)



6.1.2 U2000 Deployment on Virtual Machines

The U2000 can be installed and deployed on a virtual machine (VMware or FusionSphere). The specific deployment modes include virtual machine single-server deployment mode, virtual machine cold backup deployment mode and virtual machine high availability (HA) deployment mode.

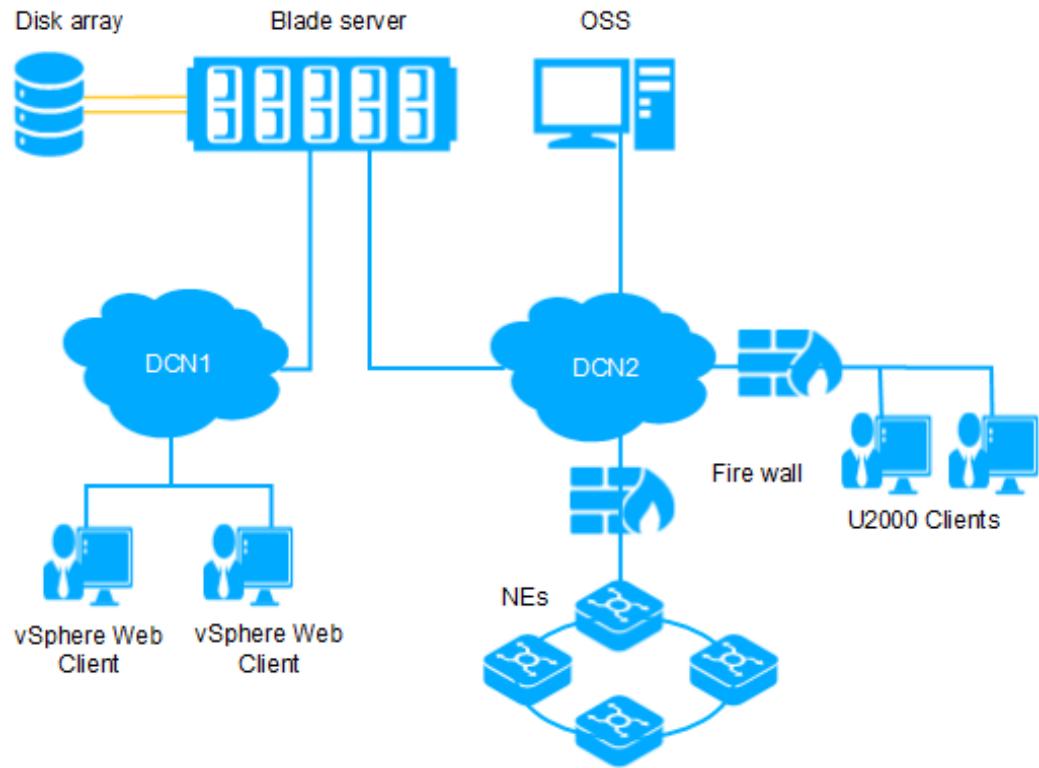
6.1.2.1 Deployment Mode of the U2000 Virtual Machine Single-Server System

The U2000 can be installed and runs on VMware or FusionSphere virtual machines (VMs). This topic describes the networking and principles of the U2000 Virtual Machine Single-Server System deployment solution.

Single-Server System (VMware, blade Server)

Figure 6-7 lists the single-server system (VMware, blade server) networking.

Figure 6-7 Single-server system (VMware, blade server) networking

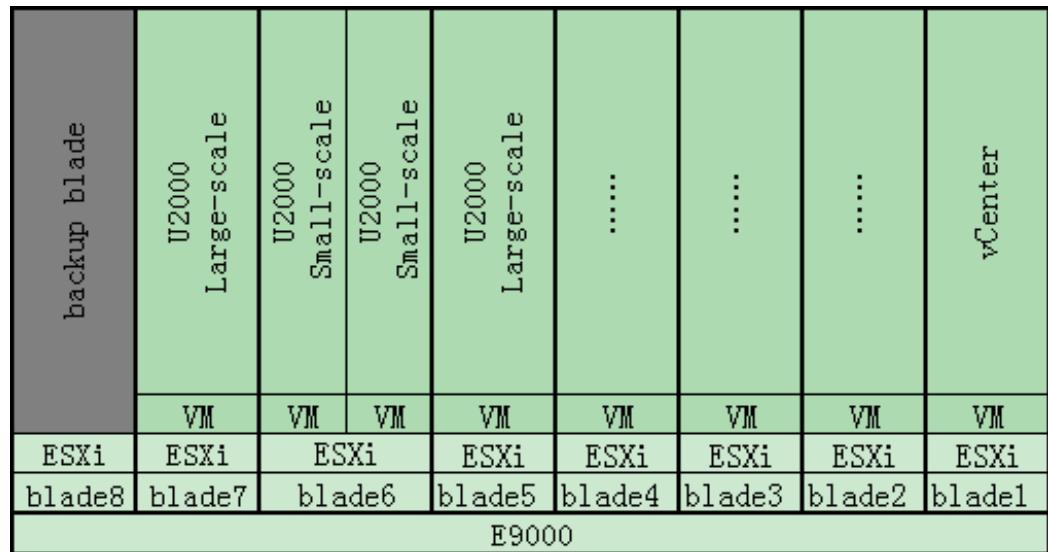


For the single-server system (VMware, blade server), two computing nodes need to be reserved for special usage: one serving as a backup blade and one having the VCSA installed. [Figure 6-8](#) shows the software structure of the single-server system (VMware, blade server).

The backup blade provides protection for blades in the U2000. If a fault occurs on a blade with the U2000 system installed, the U2000 system on the faulty blade will be automatically switched to the backup blade.

The blade that has the VCSA installed can manage multiple ESXi hosts simultaneously and combine all blades and VMs installed on the OS to form a cluster. As a result, if a blade in the cluster fails, VMs installed on this blade will be automatically migrated to the backup blade, implementing local hardware HA.

Figure 6-8 Software structure of the single-server system (VMware, blade server).



Software structure descriptions:

- ESXi is created on a blade's local disk, and all VMs and their data are created in the disk array.
- Blades provide CPU and memory computing resources, and the disk array provides storage resources for virtual machines.
- A blade can house two medium- or common-sized U2000 VMs or one large-sized U2000 VM at most.

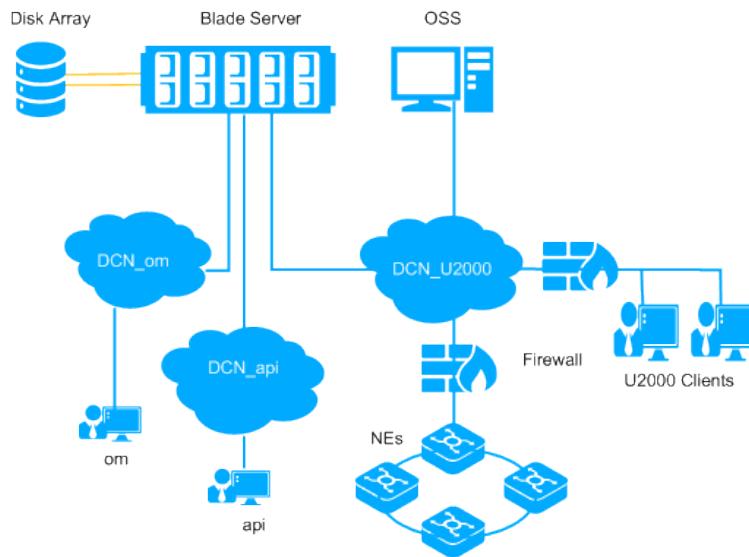
Concepts:

- blade: computing node.
- ESXi: a VMware-tailored Linux OS and an entrusted virtualization platform for VM delegation. Each blade must have a set of VMware vSphere ESXi installed.
- vCenter Server Appliance (VCSA): VCSA indicates the VMware virtualization management software installed in the VCSA VM.

Single-server System (FusionSphere, blade Server)

Figure 6-9 shows the U2000 networking based on the FusionSphere virtualization platform.

Figure 6-9 U2000 networking based on the FusionSphere virtualization platform



Definitions

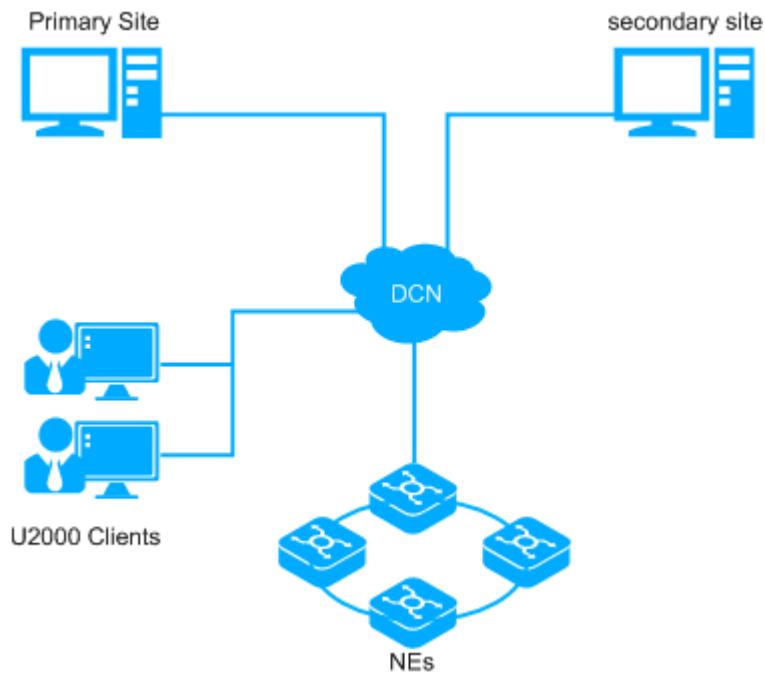
- **Blade server:** A blade server has multiple blades (computing nodes) that serve as computers. Each blade is installed with the FusionSphere OS and basic services, providing basic installation, deployment, and OS capabilities for the FusionSphere OpenStack.
- **API:** FusionSphere OpenStack external management network plane, which connects to external networks, allowing external network users to access internal VMs.
- **OM:** Internal operation and maintenance (O&M) network plane, which connects to external networks and allows users to access internal networks from an external network.

6.1.2.2 Deployment Mode of the U2000 Virtual Machine Cold Backup System

In the virtual machine cold backup solution, two single server U2000 systems with the same version, deployment domain, language, OS type, server time, and time zone are deployed. One system is run on the primary site and the other is run on the secondary site.

[Figure 6-10](#) show the deployment Mode.

Figure 6-10 Cold Backup Deployment Mode



- In normal conditions, the primary site provides the network management functions. The network management process and maintenance tool on the secondary site are standby while the database is running. The primary site backs up the network management data periodically, and the secondary site obtains the backup file from the primary site at regular intervals.
- If the U2000 on the primary site fails, the U2000 on the secondary site starts immediately to provide network management functions.

NOTE

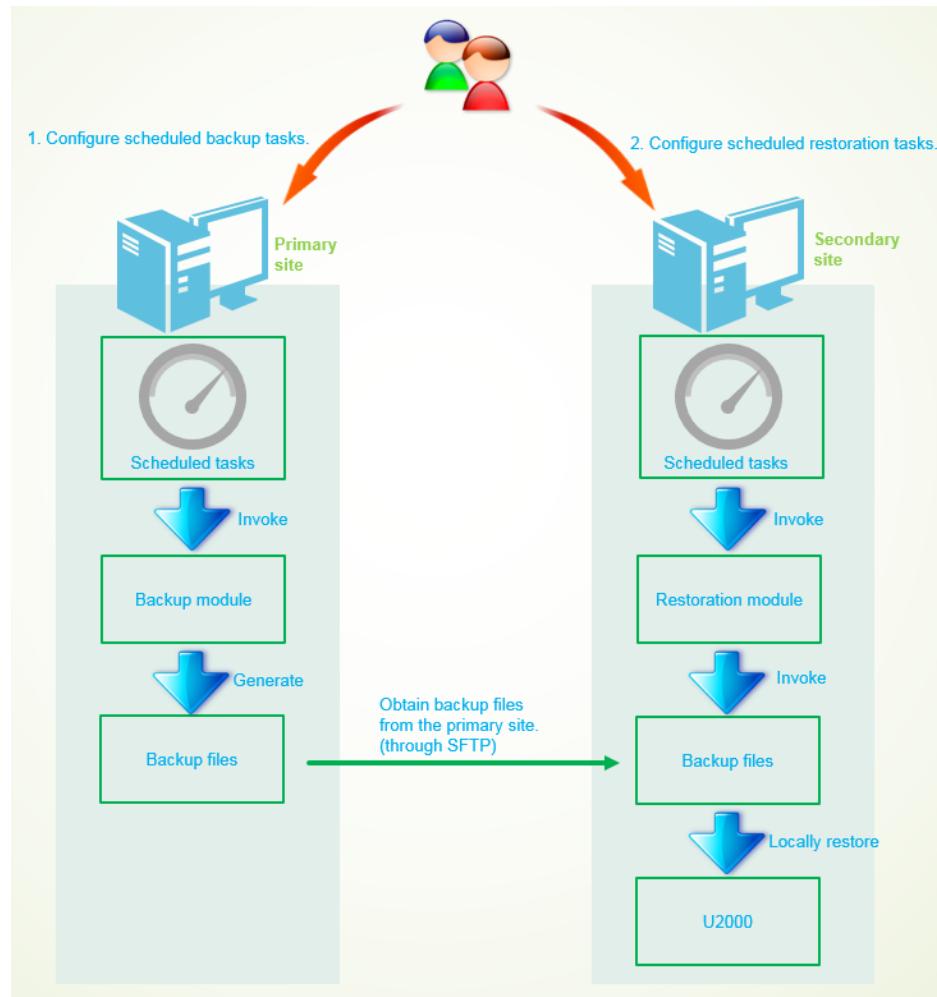
- The backup object is the entire database, including the custom data at the U2000 side (excluding the custom options of the system), network layer trail data, NE-side configuration data, alarm data and performance data. In addition, a backup is created for the structure of the entire database, all database tables (including the system tables and the user tables), table structure, and stored procedures. The personal information (including personal name, phone numbers and addresses) on the U2000 and all user names and passwords are also backed up. Therefore, you are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the personal data of users is fully protected.
- The following data is not backed up when you back up the U2000 database:
 - The data that is not saved at the NE side, that is, the data that cannot be uploaded.
 - The custom options of the system. For example, font, color setting, and audio setting.

The fast restoration scheme for the U2000 cold backup system supports manual and automatic backup and restoration. If you use manual backup and restoration, you need to manually start the backup or restoration task each time. If you use automatic backup and restoration is used, you only need to configure a scheduled backup and a scheduled restoration task. The automatic backup and restoration is recommended.

- Automatic backup and restoration scheme: To automatically back up and restore data, you need to configure scheduled backup tasks on the primary site and automatic restoration tasks on the secondary site. The process is as follows:

- a. On the secondary site, install a single server U2000 whose version, deployment domain, language and database username are the same as those on the primary site.
- b. Configure scheduled backup tasks on the primary site. The backup files are generated through backup modules and stored on the primary site.
- c. Configure scheduled restoration tasks on the secondary site. Obtain the backup files through SFTP from the primary site and restore the files on the secondary site.
- d. When the primary site malfunctions, start the U2000 on the secondary site to fast restore the U2000.

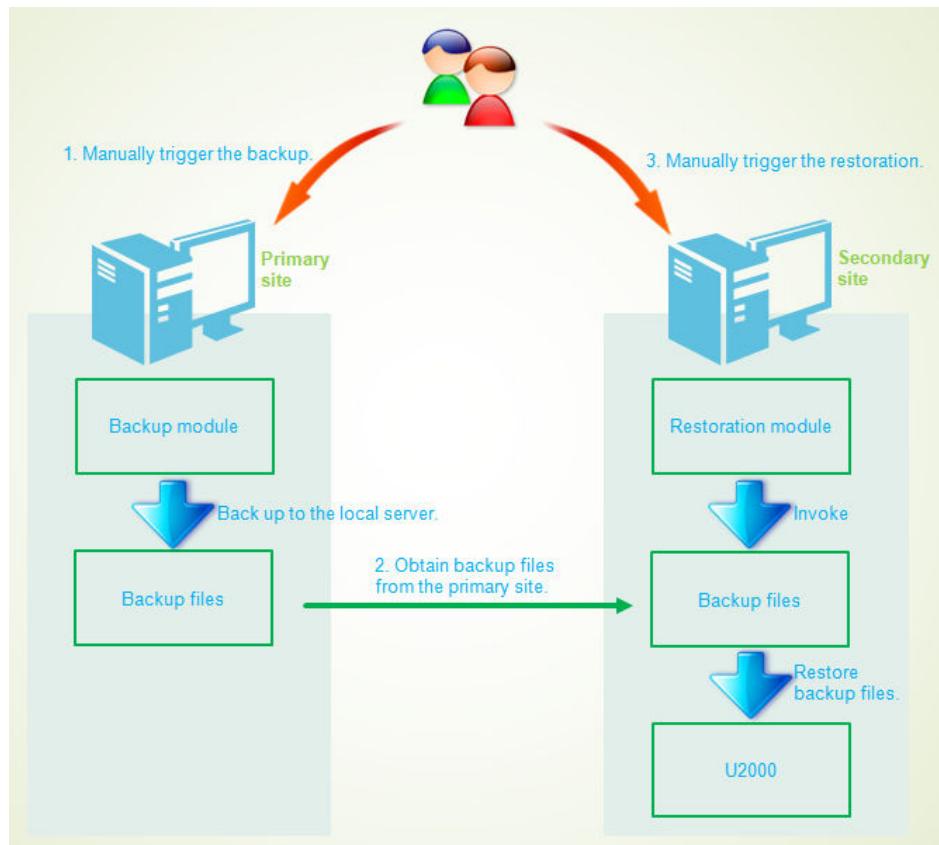
Figure 6-11 Automatic backup and restoration scheme



- Manual backup and restoration scheme: The manual backup and restoration scheme requires a cold backup tool to back up and restore data. The process is as follows:
 - a. On the secondary site, install a single server U2000 whose version, deployment domain, language and database username are the same as those on the primary site.
 - b. Use a cold backup tool to back up the U2000 data on the primary site as backup files and store the files on the primary site.
 - c. Copy the backup files from the primary site to the secondary site, and use the cold backup tool to restore the files on the secondary site.

- d. Start the U2000 on the secondary site.

Figure 6-12 Manual backup and restoration scheme



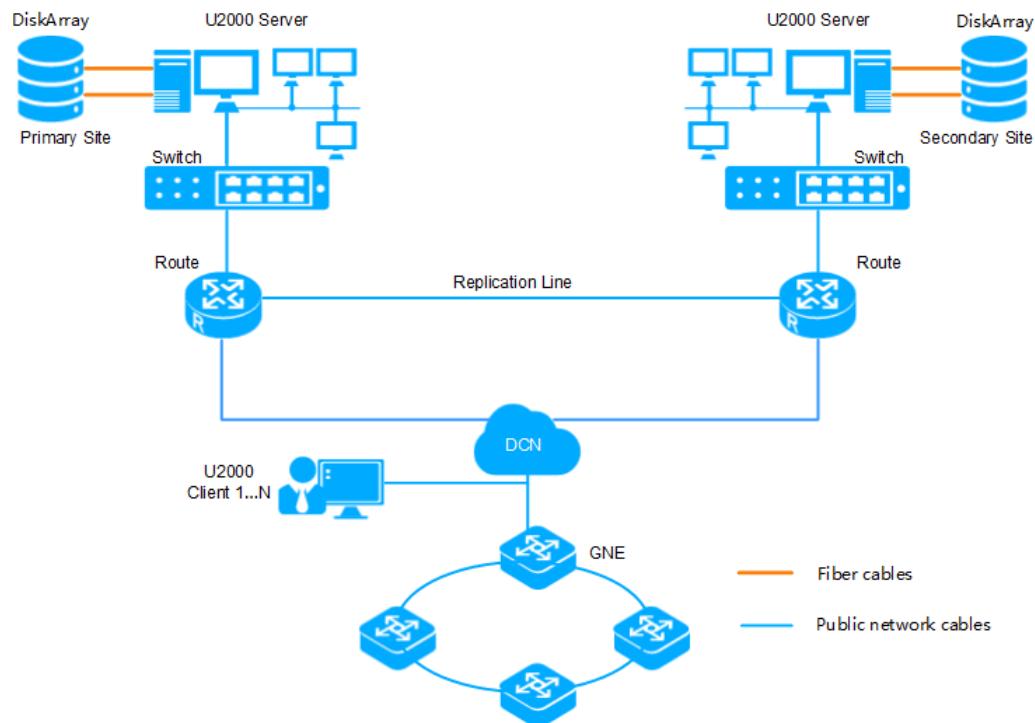
6.1.2.3 Deployment Mode of the U2000 Virtual Machine Remote High Availability System

The U2000 can be installed and runs on VMware or FusionSphere virtual machines (VMs). This topic describes the networking and principles of the U2000 Virtual Machine Remote High Availability System deployment solution.

Remote High Availability System (VMware, blade Server)

The hardware configurations and software structure figures are the same for the remote high availability system (VMware, blade server) and single-server system (VMware, blade server). You can install a U2000 HA system on the virtual machine environment at the primary and secondary sites and connect the two sites to form a remote high availability system (VMware, blade server). **Figure 6-13** lists the remote high availability system (VMware, blade server) networking.

Figure 6-13 Remote High Availability System (VMware, blade Server) networking

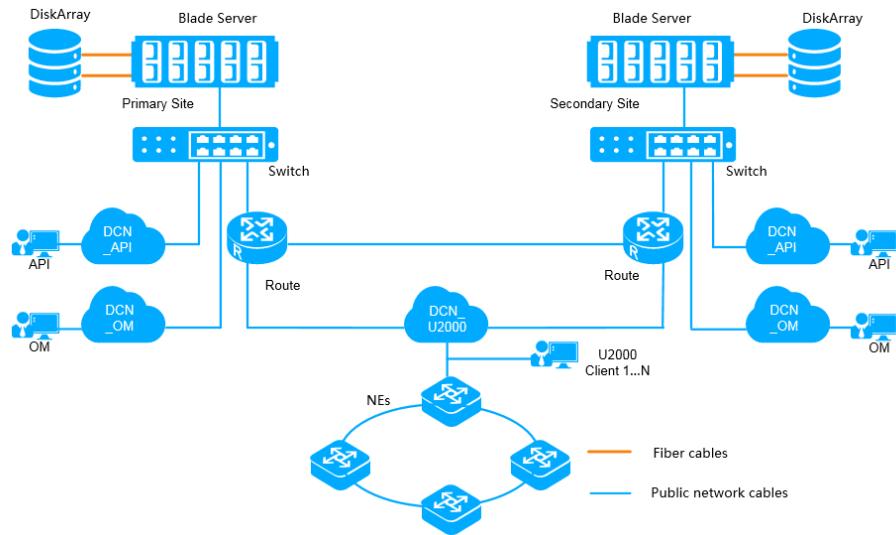


Remote High Availability System (FusionSphere, blade Server)

The hardware configurations and software structure figures are the same for the remote high availability system (FusionSphere, blade server) and single-server system (FusionSphere, blade server). You can install a U2000 HA system on the virtual machine environment at the primary and secondary sites and connect the two sites to form a remote high availability system (FusionSphere, blade server).

Figure 6-14 shows the U2000 networking based on the FusionSphere virtualization platform.

Figure 6-14 U2000 networking based on the FusionSphere virtualization platform



Definitions

- Blade server: A blade server has multiple blades (computing nodes) that serve as computers. Each blade is installed with the FusionSphere OS and basic services, providing basic installation, deployment, and OS capabilities for the FusionSphere OpenStack.
- API: FusionSphere OpenStack external management network plane, which connects to external networks, allowing external network users to access internal VMs.
- OM: Internal operation and maintenance (O&M) network plane, which connects to external networks and allows users to access internal networks from an external network.

6.2 Networking Mode Between the U2000 and NEs

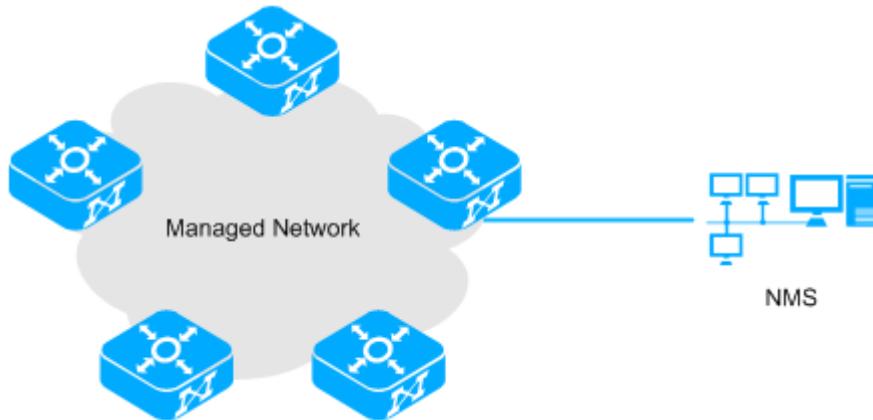
The U2000 adopts the widely used C/S (client/server) architecture. In such architecture, the client and the server communicate by means of a LAN or WAN. The U2000 server communicates with managed NEs in inband or outband networking mode. Faults on the U2000 have no impact on networks between managed NEs and services on these NEs.

6.2.1 Inband Networking Mode

In inband networking mode, the U2000 uses the service channels that are provided by the managed equipment to transmit network management information. The information is transmitted between the U2000 and the equipment through the service channels of the managed equipment.

Figure 6-15 shows an example network in inband networking mode.

Figure 6-15 Example network in inband networking mode



Networking Description

All the equipment managed by the U2000 is connected to the managed network. The U2000 is connected to only the nearby equipment on the managed network. After configuring the related routes, you can manage all the equipment on the network.

The method used for connecting the U2000 with the managed network depends on the distance between the U2000 and its nearby equipment. If the U2000 and its nearby devices are in the same telecommunications room, you can connect them by means of LAN. If the U2000 and its nearby devices are far from each other, you can connect them by means of private lines. The private line mode is similar to the outband networking mode.

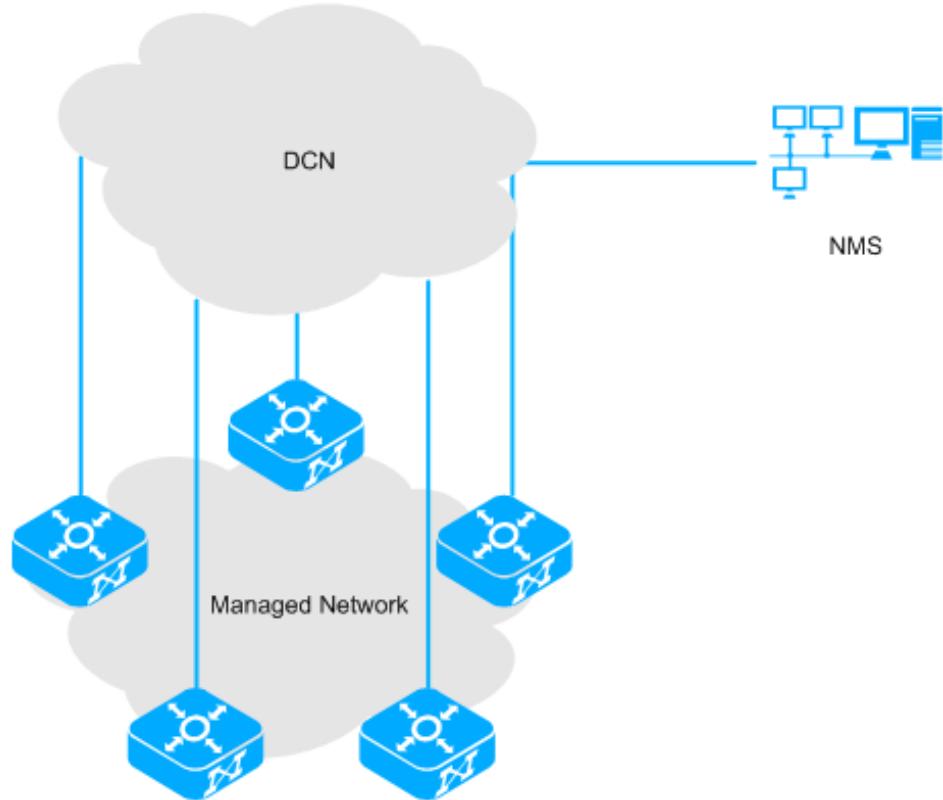
- Networking advantages: The inband networking mode is flexible and cost-effective. It does not need extra equipment.
- Networking disadvantages: When a fault occurs in the network, the communication channel between the U2000 and its managed network is interrupted, and you cannot maintain the managed network on the U2000.

6.2.2 Outband Networking Mode

In outband networking mode, the U2000 uses the communication channels that are provided by non-managed equipment to transmit network management information. Generally, the ETH port (outband management interface) on the control board of the managed equipment functions as the access interface.

In outband networking mode, the U2000 can be connected to the managed equipment in several ways. For example, the U2000 can be connected to the managed equipment through the data communication network (DCN), E1 lines, or routers. This topic uses the DCN as an example to describe how the U2000 manages equipment. [Figure 6-16](#) shows an example network in outband networking mode.

Figure 6-16 Example network in outband networking mode



Networking description

All the equipment managed by the U2000 is connected to the managed network. The U2000 connects to the equipment on the managed network by means of the DCN that is comprised of other equipment, and then manages the network and equipment.

- Networking advantages: In outband networking mode, the U2000 is not directly connected to its managed equipment. This mode provides equipment management channels that are more reliable than those in inband mode. The U2000 can quickly locate faulty equipment and implement real-time monitoring.
- Networking disadvantages: In outband networking mode, the U2000 manages equipment through a maintenance channel that is independent from the service channel. This management means that the network is comprised of extra equipment, which translates to higher costs in network construction.

6.3 Application Scenarios of U2000 Management

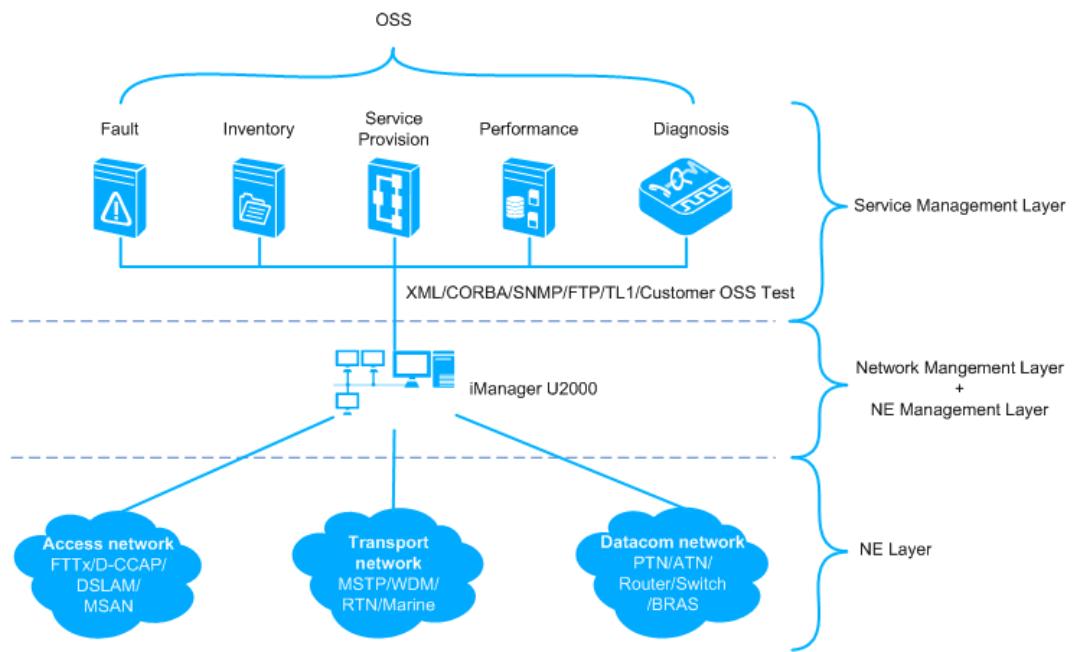
This topic describes typical application scenarios of U2000 management.

6.3.1 Unified Management of Network Products

This topic describes the application of the U2000 for unified management of network products. This is a typical solution provided by the U2000.

- The U2000 is a unified platform for managing access, transport, and IP NEs. It revolutionizes the vertical management mode to achieve unified management at the element and network management layers. In addition, the U2000 supports right- and domain-based management. This feature enables the U2000 to manage NEs in each domain separately without interference from various networks and departments.
- The U2000 follows the network convergence trend and provides management solutions for a variety of networking scenarios. The U2000 has a uniform GUI style that makes service provisioning easy. Highly effective service monitoring and service assurance ensures a good user experience and reduces the network O&M costs.
- The U2000 provides NBIs to reduce the workload for OSS integration.

Figure 6-17 Unified management of network products



Network Deployment

- Centralized deployment and right- and domain-based management
The U2000 is used to assign each NMS user a management level and to specify the objects that the users are given access to, which helps ensure system security.
- High availability solution
The U2000 can be installed in an HA system. The HA system monitors the U2000 and automatically protects data in real time.

Service Provisioning

The U2000 automatically creates a service after you select the source and sink. This function allows for quick provisioning of new services. The time required for provisioning services decreases from minutes to seconds and the configuration efficiency is improved in comparison to configurations performed on a per-NE basis.

- Provisioning of end-to-end services across domains.
 - Supports E2E TDM service provisioning and management across traditional microwave and MSTP networks, which shortens the time needed for large-scale network deployment and service provisioning.
 - Supports E2E packet service provisioning and management across IP microwave and PTN/Hybrid MSTP networks, which accelerates service provisioning in IP networks.
 - Supports E2E management of Ethernet service, CES service, ATM service, MPLS tunnels, and PWs for PTN, MSTP, RTN, switch, and NE series devices, to meet the development in the fixed market as it gets driven towards fixed-mobile convergence (FMC).
 - Supports E2E service (Ethernet, CES, and ATM) provisioning across PTN and CX networks; and supports E2E management of MPLS tunnels and PWs, to meet the development in the mobile market as it gets driven towards FMC.
 - Supports E2E service (Ethernet, CES, and ATM) provisioning across RTN and CX networks; and supports E2E management of MPLS tunnels and PWs, to meet the development in the mobile market as it gets driven towards FMC.
 - Supports E2E service (Ethernet, CES, and ATM) provisioning across ATN and CX networks; and supports E2E management of MPLS tunnels and PWs, to meet the development in the mobile market as it gets driven towards IPRAN.

Service Assurance

The U2000 supports cross-domain fault locating, which greatly improves the efficiency of rectifying faults and ensures proper operation of services.

- All NEs in the network are uniformly monitored and the number of alarms decreases.
- Multiple network management systems and teams are combined into one NMS and one team, thereby improving the efficiency of rectifying faults.
- Alarm correlation and intelligent analysis help to accurately locate faults.
- Alarm management on a per-service basis helps to directly locate the base station that is affected by an alarm, which improves the efficiency of rectifying faults by 50%.
- Unified fiber management enables the U2000 to clearly display the fiber connections between NEs network-wide. You can directly locate the NE that a fiber is connected to based on the alarm generated on the fiber.

6.3.2 Single Metro Solution

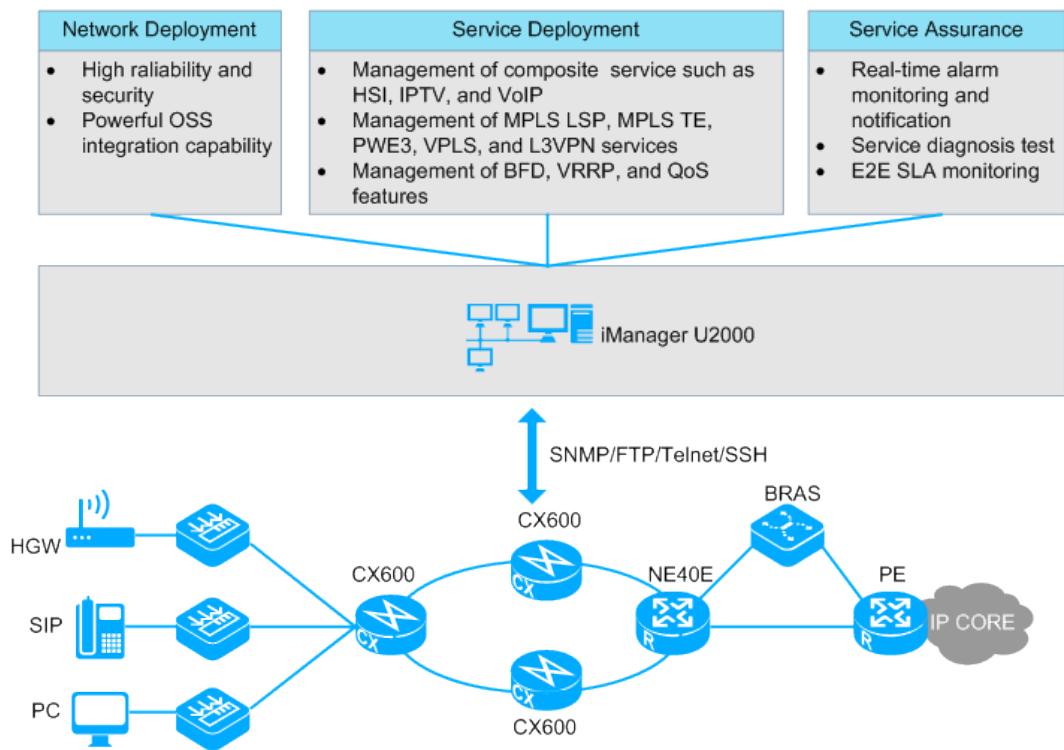
The U2000 is used in the complete solution for broadband metro networks in terms of network deployment, service deployment, and service assurance.

Networking Diagram

With the advent of the all-service and super-broadband era, carriers are integrating mobile and fixed broadband in order to offer a fuller range of services. An integrated super-broadband bearer network helps to quickly and flexibly deploy all services and greatly reduces the total cost of ownership (TCO) of the network. Constructing these types of bearer networks is a challenge for carriers.

Carrying multiple services is one of the most distinctive features of the Metro Ethernet. Services such as the high-speed Internet (HSI), IPTV, and voice over IP (VoIP) services must be established on logical channels, as shown in [Figure 6-18](#).

Figure 6-18 Network management solution for a single metro network



Network Deployment

The U2000 has the following features to make network deployment more efficient:

- Automatic discovery of network-wide equipment
 - The U2000 can automatically discover network topologies and links.
- Automatic discovery of existing services
 - The U2000 can automatically discover services, which means existing services on the network side can be restored to the U2000 in just two steps.
- Visualized service deployment
 - One-stop configuration: The U2000 provides the tunnel template, L3VPN/VPLS/PWE3 service template, and QoS policy template for one-stop service configuration. These templates predefine 80% of the parameters, which reduces the configuration workload.
 - Automatic computation: The U2000 automatically computes static routes for static CR tunnels, implementing automatic label allocating.

Service Deployment

The Metro Ethernet often carries heavy service traffic. To adapt to this feature, the U2000 deploys services in batches and quickly creates end-to-end services.

- End-to-end service management and deployment

The U2000 allows you to quickly establish specific logical channels on physical networks through GUIs. You can verify the validity of services before deployment and modify services after the logical channels are established.

- Creation of an end-to-end tunnel: After you select the ingress, egress, and transit nodes, an end-to-end tunnel can be automatically created. After tunnel configuration, parameter settings can be instantly deployed and both the primary and bypass hop-by-hop tunnels will be displayed in the topology view. The U2000 can create forward and backward tunnels at the same time, which facilitates tunnel management. In addition, the U2000 supports automatic assignment of LSP labels to avoid manually assigning labels.
- Creation of an end-to-end service: Select the service node to be configured and set some parameters to complete E2E service creation. The U2000 can automatically check service configurations and service connectivity, ensuring that services are successfully deployed at a time.
- Batch management of multicast parameters
The U2000 can set, adjust, and verify multicast parameters in batches, which helps carriers improve IPTV service deployment and helps users ascertain the running status of multicast services in real time.

Service Assurance

The U2000 uses several methods to monitor the network 24 hours a day, 7 days a week. It can detect network faults or degradation in a timely manner and report end-to-end SLA data of the network.

The U2000 provides the following service assurance measures for broadband bearer networks:

- **Reduction of IP alarms**

On the U2000, the following four technologies are used to reduce the number of IP alarms by 85% in most scenarios.

- Engineering alarm marking: At the engineering implementation stage, engineering alarms are marked for you to focus on valid alarms.
- Analysis of intermittent alarms: When multiple intermittent alarms of the same type are generated during a specified period, only one alarm is displayed.
- Alarm correlation analysis: The root alarm can be quickly located from lots of alarm records.
- Alarm consolidation: If an NE generates duplicate alarms, the U2000 displays only one alarm record and records the alarm generation time as well as the alarm quantity.

- **Fault location**

The U2000 displays network-wide routes and allows you to accurately diagnose service faults layer by layer and hop by hop. Service faults can be located down to the specific NE and protocol in as short as several minutes as opposed to hours.

- **Visualized service monitoring**

- Supports service-oriented visualized service monitoring so that you can directly query services affected by a specific alarm.
- Uses a full complement of service-based tests and diagnostic methods to quickly check service connectivity and rectify faults.

- Provides service-based functions for displaying performance through GUIs, generates alerts when performance thresholds are exceeded, and analyzes performance trends.
 - Supports layer-based management so that you can query the network bearer relationships in real time.
- **Relationships between visualized objects**
 - On the U2000, services are associated with tunnels and tunnels are associated with routes so that the network bearing relationship can be easily identified.
 - When a fault occurs, you can quickly locate and rectify the fault according to the bearing relationship.
 - **Quick check of network-wide links**
 - The network scanning tool can automatically compute IP links between equipment, which improves the efficiency of network checks.
 - The status of all links on the network can be monitored with just two clicks.
 - Network quality is displayed in different colors (red, yellow, and green) help easily locate and rectify network problems.
 - **Independent Web-based performance report system (iWeb)**
 - You can use Internet Explorer to log in to the iWeb report system without having to upgrading the client.
 - The iWeb report system provides a variety of reports, including alarm and Syslog reports, resource reports, performance statistics reports, PTN reports, and service reports.
 - **Real-time alarm monitoring and notification**

The U2000 can monitor network faults and the status of equipment and interfaces in real time. The system notifies the related personnel of network faults through SMSs or emails to ensure proper network performance.
 - **Performance monitoring 24 hours a day, 7 days a week**

The U2000 periodically collects the traffic data of all the links or some key links on the entire network to provide effective support for network monitoring.
 - **End-to-end SLA monitoring on network nodes**

The U2000 periodically collects the SLA data between PEs, the SLA data between the local CE and PE, and the SLA data between the PE and remote CE. With this data, you can detect network degradation, predict network performance, and optimize the network.
-  **NOTE**
- SLA: service level agreement
 - PE: provider edge
 - CE: customer edge

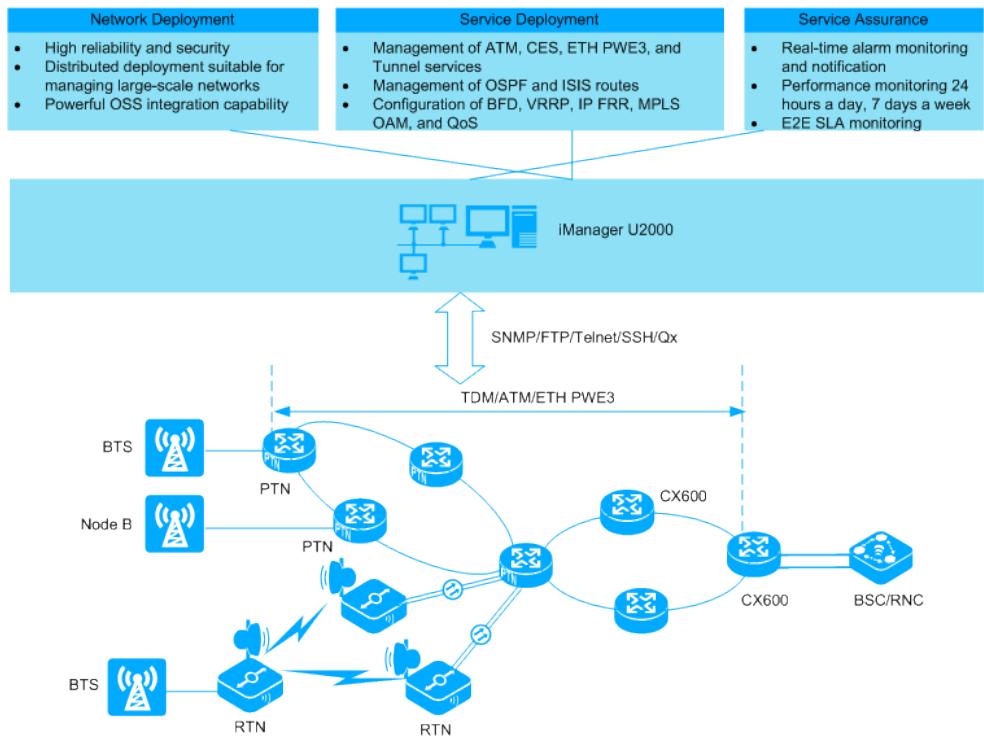
6.3.3 Single Backhaul Solution

All-IP networks are becoming the new trend as a variety of mobile data services are sprouting up everywhere while networks are becoming complex to maintain because of huge number of device types that are deployed. Therefore, operation, administration, and maintenance (OAM) systems must be improved while staying within the proper OPEX to support more complex and flexible configuration for multiple services and to provide a variety of fault monitoring methods.

Challenges for the OAM in the IP transformation of mobile bearer networks include

- Unified management of many types of devices: Fibers, microwaves, copper cables, and Ethernet may function as media to carry services of mobile bearer networks. The maintenance and management of various types of media present challenges to carriers.
- End-to-end (E2E) service provisioning and QoS assurance: The OAM experience of traditional SDH and MSTP networks must be inherited for the OAM of all-IP networks. In addition, all-IP networks need to be merged with microwave networks. Therefore, carriers need to improve their capabilities in E2E service management and QoS monitoring.
- As shown in **Figure 6-19**, in mobile bearer networks, 2G and 3G services on the base station (BS) side are transmitted through TDM-E1, IMA-E1, or FE ports and then carried over E2E PWs. In addition, fixed networks and mobile networks are merged. Specifically, the CX series equipment carries broadband services and the PTN equipment functions as the mobile access service gateways at the two ends.

Figure 6-19 Single backhaul solution



The U2000 provides solutions to the **Network Deployment**, **Service Provisioning**, and **Service Assurance** of mobile bearer networks.

Network Deployment

Software commissioning without visiting the site

- The data communication network (DCN) becomes available automatically and the U2000 searches for devices remotely. Software commissioning engineers do not need to

physically visit the sites; that is, the devices do not require field software commissioning. Only hardware installation engineers need to visit the sites to install the devices.

- Software commissioning is implemented entirely in the network management center (NMC). Customer engineers do not need to perform operations on site.

Auto-discovery of NEs and links

- The U2000 automatically searches for all NEs in a specified range and adds them in the Main Topology.
- NEs that are searched out are displayed in a list, which helps you modify and maintain NE properties in a unified manner.
- The U2000 automatically searches for fibers in a specified range and adds them in the Main Topology.

Quick fiber searches and creation. Automatic fiber search can add physical fibers to the U2000 quickly and therefore facilitates fiber creation.

Automatic network-side IP address assignment

- Automatic IP address assignment on the NE network side: Network-side IP addresses of NEs can be automatically assigned when fibers are created, which simplifies network deployment.
- Centralized management of IP addresses of NEs: A report is provided to collect the IP addresses of all NEs on the entire network.

Plug-and-play (PnP) function. After a device is connected to a microwave network, all devices on the network are searched out and are displayed in a list. The U2000 supports one-touch device creation.

PnP function of boards. A physical board is automatically displayed when the NE Panel is displayed. The U2000 supports one-touch board creation.

Packet service cutover of PTN equipment. The cutover of packet services only requires six steps. In the daytime, cutover tasks are created in batches and service data to be cut over are verified. At night, services are automatically cut over. Automatic cutover reduces the workload and enhances the cutover efficiency.

- With an increase in services, packet service cutover can quickly balance the service traffic load between the RNC and base station controllers (BSCs).
- To meet the requirements of frequent network adjustment, packet service cutover can efficiently and correctly adjust services to reduce errors and service interruptions.

Automatic WDM optical power commissioning. The automatic WDM optical power commissioning feature shortens the learning curve for deployment engineers and increases the deployment efficiency.

- Multiple types of fibers are supported, such as G.652, G.653, G.655, and the combination of G.652 and G.655.
- Mainstream WDM equipment from Huawei and multiple networking schemes are supported. For example, the chains, rings, intersecting rings, and mesh networks are supported.

Wizard-based network adjustment. Wizard-based network adjustment makes the process easy.

- Nodes can be added to a ring or link and the link capacity can be expanded.
- Wizard-based and step-by-step operations increase the efficiency in network adjustment and shortens the learning curve for OAM engineers.

- The entire process of network expansion can be ensured. Specifically, network resources are checked before network expansion, an automatic service rollback is triggered upon an expansion failure, and a comparison report is generated after a successful network expansion. This feature ensures high reliability of network expansion and facilitates management.

Service Provisioning

Quick, accurate, and automatic service restoration. The U2000 provides an easy-to-use function for automatically restoring services. In addition, only two steps are required to restore network-side services to the E2E service configuration on the U2000. In this manner, services are quickly restored.

- Services are automatically created after you specify the source and sink and select a routing policy. Service provisioning is efficient and errors are reduced.
- A large number of services can be rapidly provisioned because services can be created in batches.
- The creation and management of E2E services that traverse both microwave and MSTP equipment is supported, which is unique in the telecommunications industry.

E2E management and service provisioning

- The E2E packet service provisioning and management of the IP microwave and PTN/MSTP devices shortens the service provisioning time on IP networks.
- The E2E TDM service provisioning and management of the traditional microwave and MSTP devices enhances the efficiency in the network deployment and service provisioning for a large number of microwave devices.
- E2E service provisioning on the network of the PTN equipment and CX equipment is supported.
- E2E packet service provisioning on the network of the PTN equipment and MSTP equipment is supported.
- The network of the OptiX RTN 910/950 and PTN equipment is supported and E2E CES service provisioning can be performed on the mixed network.
- The network of the PTN equipment and CX equipment is supported.
- E2E VLAN service provisioning is supported.
- E2E Ethernet service provisioning on WDM trails is supported.

Visualized E2E service provisioning

- Visualized tunnels.
- Visualized protection relationships between tunnels.
- Visualized service topologies that can be previewed.

Bulk deployment: The U2000 supports bulk deployment of Metro Ethernet services. This function improves large service deployment. Bulk deployment shortens service deployment time.

Quick service provisioning: Configurations are quickly applied to NEs after you specify the source, sink, and TE constraints. In addition, hops of working and protection trails are displayed in the topology view.

Service Assurance

Service-based E2E OAM

- All OAM data are configured based on E2E services and you do not need to separately configure OAM data for each node on an E2E trail.
- Default parameters are provided and one-touch tunnel configuration is supported. Wizard-based Ethernet OAM is supported and a remote maintenance end point (MEP) is automatically generated.

Service-based fault diagnosis and rapid fault locating

- E2E service diagnosis is supported without having to check to each node. This feature helps to locate a fault quickly.
- Fault information is collected during diagnosis. The fault information helps analyze fault causes quickly.

Visualized network-wide clock

- Clocks such as IEEE 1588v2 clocks, synchronous Ethernet clocks, and SDH clocks can be auto-discovered in the topology view. In addition, network-wide clocks are displayed in the same topology view. In the topology view, the clock tracing status and clock synchronization status are refreshed in real time when a network fault occurs.
- The clock status is monitored in real time and the clock alarm, clock tracing status, and clock protection are displayed in real time.
- Synchronize with Physical View.
- Display Master Clock ID.
- Query Clock Attributes.
- Display Clock Lock State.

Server-centered alarm monitoring

- Relevant alarms are displayed in the E2E service management window when a faulty network affects service provisioning.
- Services affected by alarms can be located with a one-touch operation in the alarm management window.
- You can view network-wide alarms on the U2000 client or Web browser after alarms are generated.

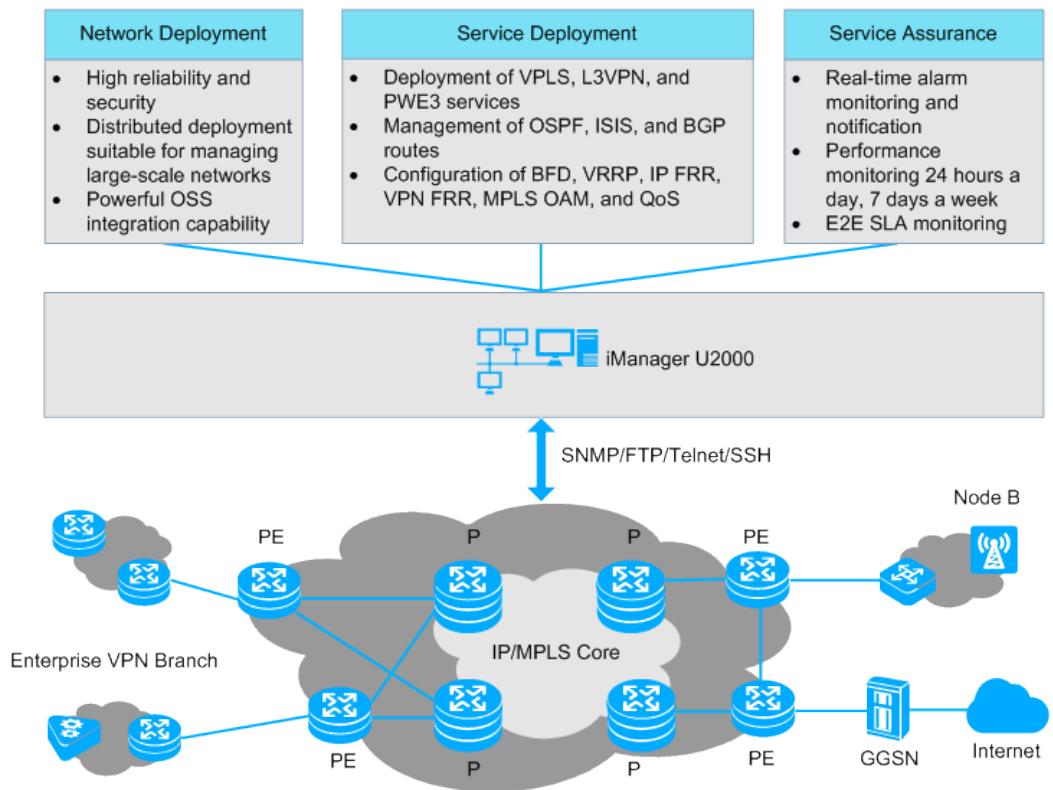
6.3.4 Single Backbone Solution

The U2000 is used in the complete solution for backbone networks in terms of network deployment, service deployment, and service assurance.

With the development of carrier-class IP technologies such as MPLS, VPN, and OAM technologies, carrier-class network technologies based on the IP backbone network are becoming increasingly more mature. The single backbone solution is provided for multi-service core bear networks, Internet backbone networks, and international gateways. Carrier-class maintenance must be stringently performed on the IP core network because of its core position on a telecommunications network. As shown in [Figure 6-20](#), the single backbone network has the following networking features:

- The core layer uses the dual-plane structure and fully meshed connections are set up between provider core routers (Ps).
- Dual-homing connections are set up between provider edge routers (PEs) and Ps.
- Two sets of equipment are deployed on important nodes for backup.
- The MPLS VPN is planned in a unified manner to achieve isolation between users or services.

Figure 6-20 Network management solution for a single backbone network



Network Deployment

The U2000 has the following features to make network deployment more efficient:

- Automatic discovery of topologies and services
The U2000 can automatically discover network topologies, links, and IP services.
- End-to-end reliability
The U2000 can manage mainstream routing protocols such as OSPF, IS-IS, and BGP; configure IGP (OSPF and IS-IS) fast convergence; and configure BFD, VRRP, IP FRR, VPN FRR, and MPLS OAM to ensure service reliability.
- End-to-end QoS deployment
The U2000 supports QoS deployment in common Diff-Serv mode so that traffic can be classified according to the service priorities of users. On a PE, complex traffic classification is performed according to the source IP address, destination IP address, interface, and VLAN; on a P, only simple traffic classification is performed. In addition, the U2000 supports VPN HQoS deployment in scheduling multiple services on a VPN and different VPN traffic on public TE tunnels.

Service Deployment

The U2000 provides the following functions for effectively and accurately deploying services:

- Supports creation of MPLS tunnels.

- Supports deployment of mainstream services (for example, L2VPN, L3VPN, and PWE3 services) that are carried over tunnels; provides multiple service configuration templates and batch configuration templates, and supports automatic verification of parameter settings.
- Provides simple and user-friendly GUIs for improving the service deployment efficiency. After a service is created in the topology view, the U2000 immediately displays the service and deployment results. All parameters can be set in only one GUI, which quadruples the configuration efficiency.

Service Assurance

The U2000 provides the following service assurance measures for single backbone networks:

- Protection switchover in less than 50 ms in the event of a local fault
You can configure MPLS TE FRR to implement fast route convergence. This ensures that traffic can be switched in 50 ms after a fault occurs on a node or link on the network. On an MPLS TE network, after the FRR is configured for the primary LSP, traffic is quickly switched to the bypass LSP if a link or a set of equipment becomes faulty. MPLS TE FRR is a temporary local protection mechanism. With this mechanism, when the primary LSP recovers, traffic is switched back to the primary LSP or a new LSP.
- Protection switchover in less than 200 ms in the event of an end-to-end fault
With VPN FRR deployed, when a fault occurs on a remote PE, the local PE can quickly switch traffic to the remote backup PE in 200 ms. The switching duration is irrelevant to the number of routes on the private network.
- Real-time alarm monitoring and notification
The U2000 can monitor network faults and the status of equipment and interfaces in real time. On the U2000, the status and severity of equipment alarms are identified by the colors of the nodes in the topology view. Maintenance engineers can quickly locate alarm-affected services from specific equipment alarms. The U2000 notifies personnel of network faults through SMSs or emails to help ensure timely rectification of network faults.
- Performance monitoring 24 hours a day, 7 days a week
The U2000 periodically collects the key performance indicators of network-wide links or specified links, and dynamically displays network status. This function provides important references for network fault locating. The U2000 periodically collects the traffic data of all the links or some key links on the entire network to provide effective support for network monitoring.
- E2E SLA monitoring on network nodes
The U2000 periodically collects the SLA data between PEs, the SLA data between the local CE and PE, and the SLA data between the PE and remote CE. With this data, you can detect network degradation, predict network performance, and optimize the network.
- Layered fault diagnosis and location
After a fault occurs, the U2000 analyzes the tunnel associated with the specific service and the route associated with the tunnel. The system then diagnoses the service according to different network layers to accurately locate the faulty point (equipment, port, or service) and to determine the causes of the fault for quick troubleshooting.

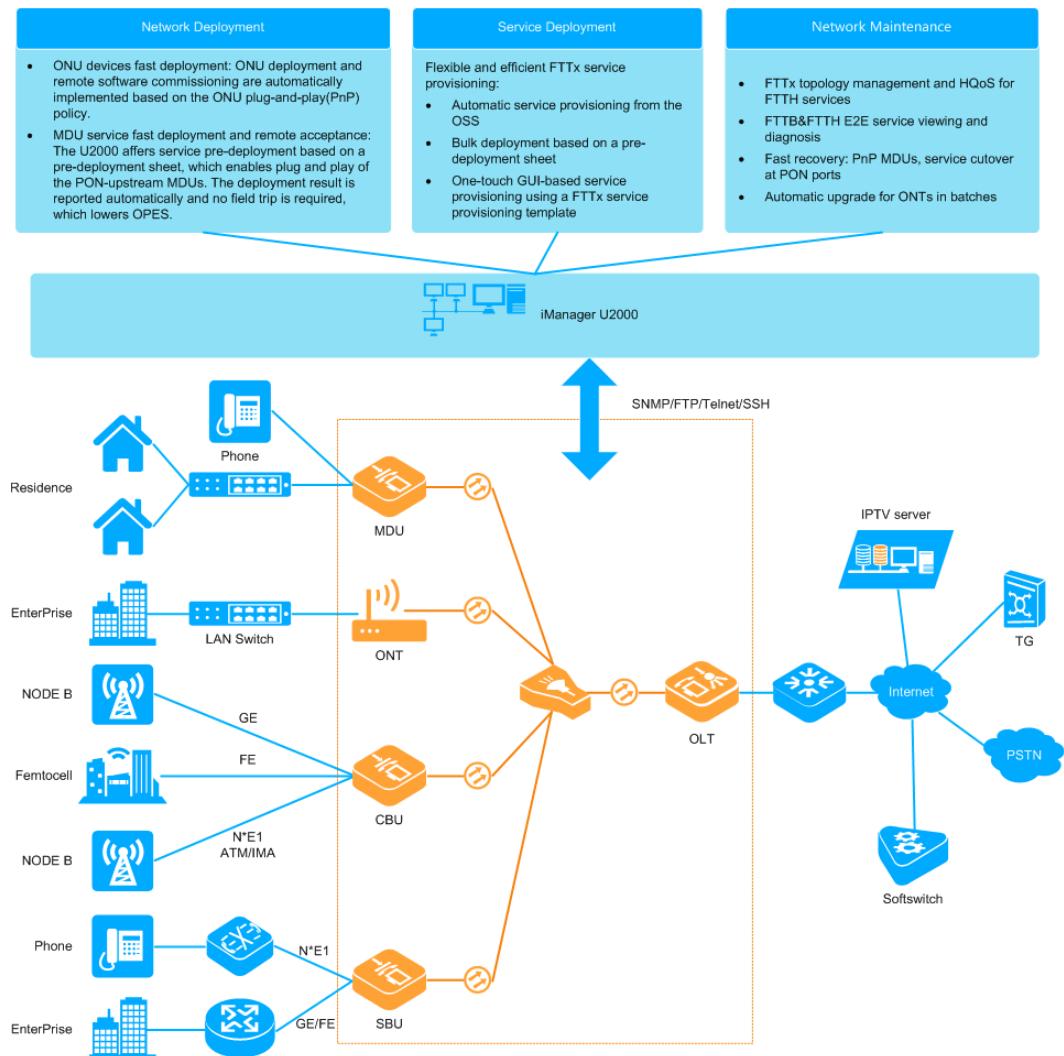
6.3.5 Single FTTx Solution

The FTTx solution is the optical access solution that supports a large capacity of subscribers and long-distance transmission and provides high bandwidth. The U2000 provides a

comprehensive solution for FTTx access devices to manage and maintain the OLT, ONU, SBU, and CBU in a centralized manner.

In the FTTx access solution, a single fiber is used to provide voice, data, and video services. The FTTx access solution meets the networking requirements for fiber to the curb (FTTC), fiber to the building (FTTB), fiber to the home (FTTH), fiber to the office (FTTO), FTTM(Fiber To The Mobile Base Station), FTTD(Fiber To The Door), FTTS (Fiber To The Service Area), IP private line interconnection, and wholesale services. **Figure 6-21** shows the networking application for FTTx access network management.

Figure 6-21 Networking application for FTTx access network management



Network Deployment

- **Fast ONU deployment:**

ONU deployment and remote software commissioning are automatically implemented based on the ONU plug-and-play (PnP) policy, which greatly improves the deployment efficiency and reduces the network construction costs.

- Complete scenarios: ONU PnP deployment is supported in preconfiguration and non-preconfiguration scenarios.
 - Unified configuration: The user interface (UI) of configuring the ONU PnP policy, including assigning IP addresses, adding ONUs and management service ports, upgrading software, and configuring scripts, in each FTTx scenario is unified, which allows users to upgrade, add, and implement software commissioning for ONUs in a simplified manner.
 - Simple process: You can configure a PnP policy and bind it to related OLTs on the U2000. After ONUs go online the first time and report messages to the U2000, the U2000 automatically invokes the ONU PnP policy and performs operations defined in the policy to complete ONU deployment.
- **Fast deployment and remote acceptance test of MDU services:**
- In an FTTB network, the U2000 provides the PON-upstream MDU predeployment and remote acceptance functions. By using the functions, you can improve the PON-upstream MDU deployment efficiency and reduce the operational expenditure (OPEX).
- The U2000 provides the ONU predeployment function. Before powering on an ONU, create a corresponding virtual NE and configure service data on the U2000. After you power on the ONU, the U2000 automatically applies the preset configuration to the ONU to complete the service deployment. Therefore, the network predeployment and device installation can be started at the same time. In this way, the time required for network construction is reduced by half.
 - The U2000 offers sheet-based predeployment of NEs. By using this function, you can import NE data to the U2000 in batches. The devices do not need field software commissioning and acceptance tests can be performed remotely. Only hardware installation engineers need to visit the sites to install the devices. In this way, the ONU becomes a plug and play (PnP) device that improves deployment efficiency and reduces construction costs.
 - The U2000 provides flexible authentication that works together with the preconfiguration function to implement the PnP of the ONU. In this way, the installation cost is greatly reduced. You only need to enter the authentication information when you replace a faulty ONU. The U2000 automatically applies the configuration data of the faulty ONU to the new ONU. You do not need to re-configure the new ONU.
 - The U2000 provides the remote acceptance function for the ONU. Specifically, the U2000 automatically applies the preconfiguration data after the ONU goes online and implements the remote service acceptance if you create an acceptance task for the ONU when it is offline.
 - The U2000 supports import of optical topology sheets to fast create topology views, including creating optical splitters under ports and removing ONUs to other optical splitters. This function improves O&M efficiency.

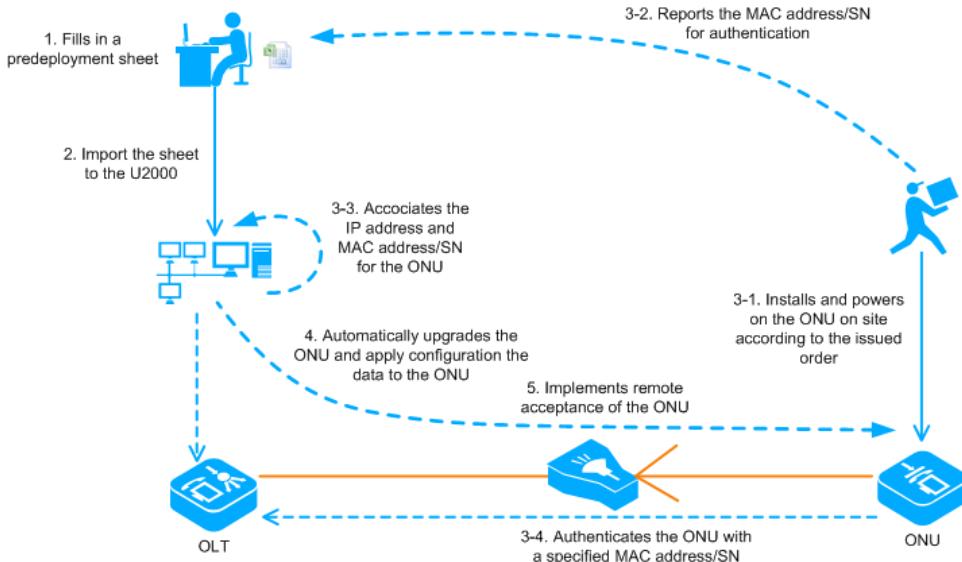
The U2000 provides a solution for quick ONU deployment. With the solution, engineers visit a site only once (for installing the devices) and complete the ONU deployment in the following five steps:

- a. Plan data: With the Excel-based plan tool, you can easily copy and paste data when configuring a large amount of data.
- b. Perform offline deployment: Import Excel sheets that contain planned data to the U2000 and complete pre-provisioning of services offline.
- c. Install ONUs on site: Only the hardware installation engineers need to visit the sites to install ONUs. There is no need for on-site software commissioning.

- d. Activate services: Power on ONUs. The PnP features of the ONUs take effect.
- e. Perform remote acceptance: Engineers do not need to visit the sites. Instead, NEs automatically report acceptance results without manual intervention.

Figure 6-22 shows the FTTx predeployment flowchart.

Figure 6-22 FTTx predeployment flowchart



Service Provisioning

The U2000 provides the following three convenient and fast service provisioning methods. With these methods, you can quickly provision the configuration data of FTTx NEs regardless of whether the OSS is interconnected with the EMS.

- **Automatic provisioning upon interconnection with the OSS:**

The U2000 provides standard and open northbound interfaces (NBIs) that quickly connect to the OSS for the FTTx solution.

- **Sheet-based service provisioning:**

The U2000 provides convenient and fast predeployment for ONUs and preconfiguration for services in the FTTx solution. With this function, the U2000 automatically provisions services, which simplifies the operation for engineers.

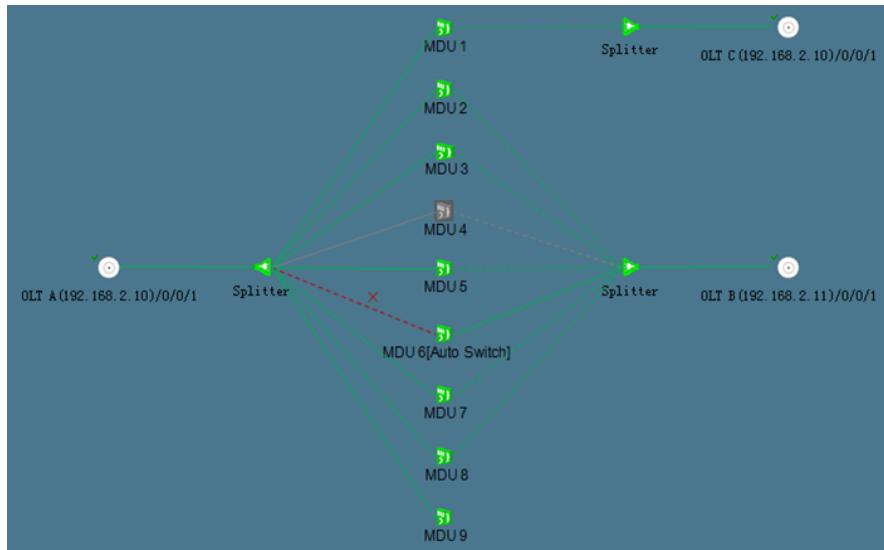
- **FTTx service provisioning template:**

The U2000 provides templates for provisioning FTTx services. You can customize service provisioning templates for specific subscribers and provision services with a single touch. In this way, the efficiency and correctness of service provisioning are greatly improved.

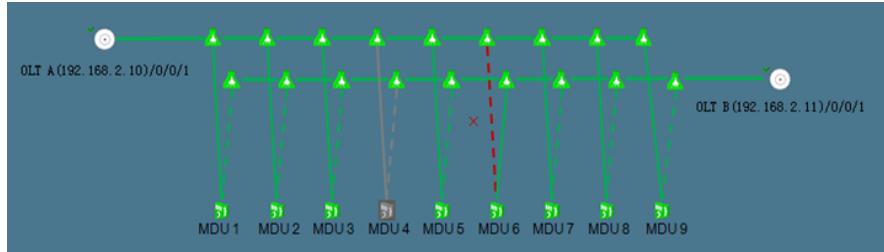
Network Maintenance

- **FTTx topology management:**

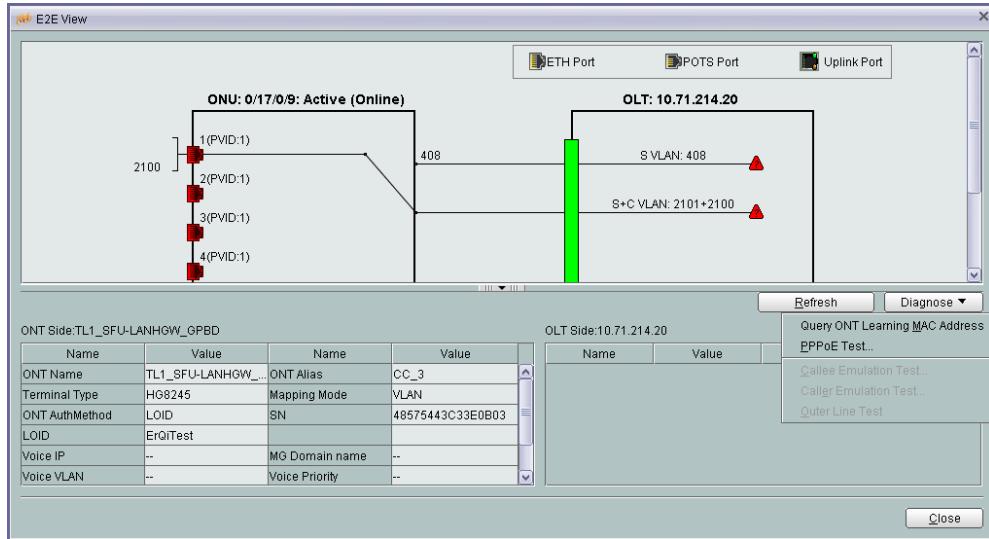
- ODN view: displays PON ports, optical splitters, fibers, and ONUs on OLTs as well as a complete network topology of type C protection (see the topology view).



- Hand-in-hand view: displays a complete hand-in-hand topology (see the topology view).



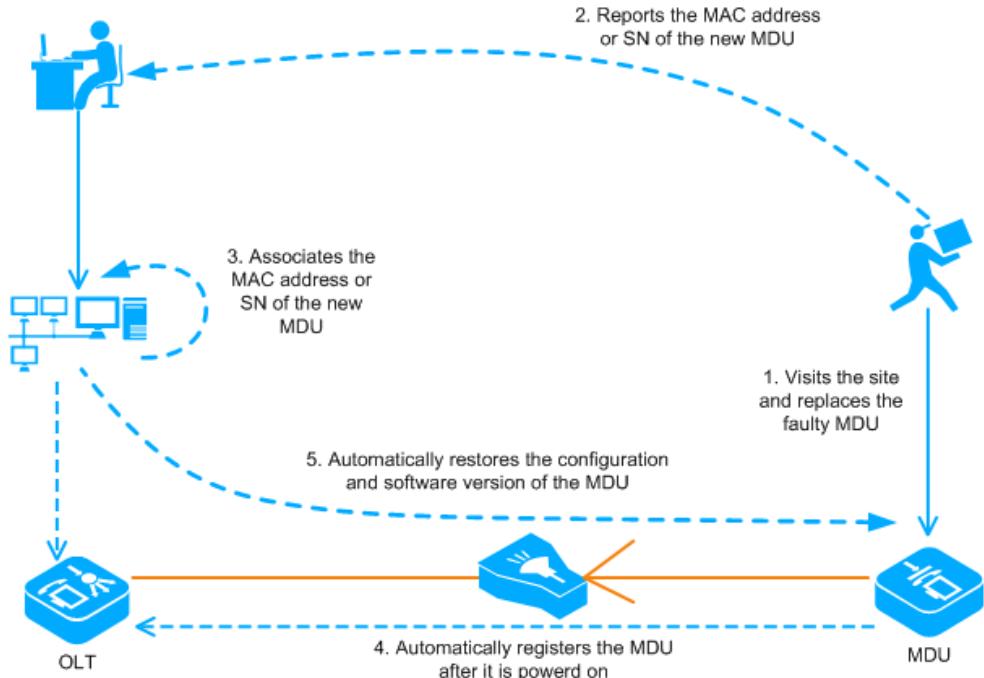
- **HQoS for FTTH services:** The U2000 provides private-line users and key users with dedicated management terminals to implement hierarchical monitoring on ONTs and improve service guarantee capabilities.
 - Hierarchical management on ONTs by user-defined level
 - Hierarchical monitoring on ONTs' performance KPI by user-defined level
 - Topology display for ONTs by user-defined view
 - Bulk alarm suppression by ONT level to reduce user-undesired alarms
- **FTTB&FTTH E2E service viewing and diagnosis:** The U2000 provides the function of viewing services from OLTs to MDUs or OLTs to ONTs in the E2E service view and provides multiple testing and diagnosis functions to locate faults. These functions facilitate maintenance and troubleshooting. The following shows the FTTH E2E service viewing and diagnosis functions:



- PnP of the MDU after replacement:**

When an MDU is faulty, you need to locate the fault and recover services quickly. However, it is time-consuming to rectify a hardware fault of the MDU. Therefore, it is recommended that you directly replace faulty MDUs and send them to a maintenance center for repair later on. The U2000 provides PnP MDUs. With this function, you only need to rebind the MAC address or SN of the MDU on the U2000 and then the U2000 automatically applies the configuration and NE software version to the MDU, which means that you do not need to configure the MDU on site or on the OSS. **Figure 6-23** shows how the PnP function is implemented after the MDU is replaced.

Figure 6-23 PnP function of the MDU after replacement



- Automatic upgrade for ONTs in batches:**

- The U2000 upgrades newly installed ONTs automatically before provisioning services on these ONTs.
- The U2000 upgrades live-network ONTs automatically based on the ONT types and versions and specified upgrade policies.

6.3.6 OptiCable D-CCAP Solution

The OptiCable D-CCAP solution applies to the cable television subscribers who need bidirectional transformation and new cells where cable television and broadband access are required on coaxial networks.

D-CCAP Standalone NE Management

Networking Applications

The D-CCAP supports GPON independent networking mode and GE independent networking mode as shown in [Figure 6-24](#) and [Figure 6-25](#). OLTs are located in branch equipment rooms, CMCs are located on optical nodes, and CMs are located in users' homes (In GE independent networking mode, CMCs can be directly connected to the switch). On the U2000, OLTs and CMCs are independent NEs. CMCs require an independent management IP address. In the built-in EQAM solution scenario, EQAM devices are moved down from the hub to the FN and are integrated in CMC devices.

Figure 6-24 D-CCAP networking using PON upstream transmission

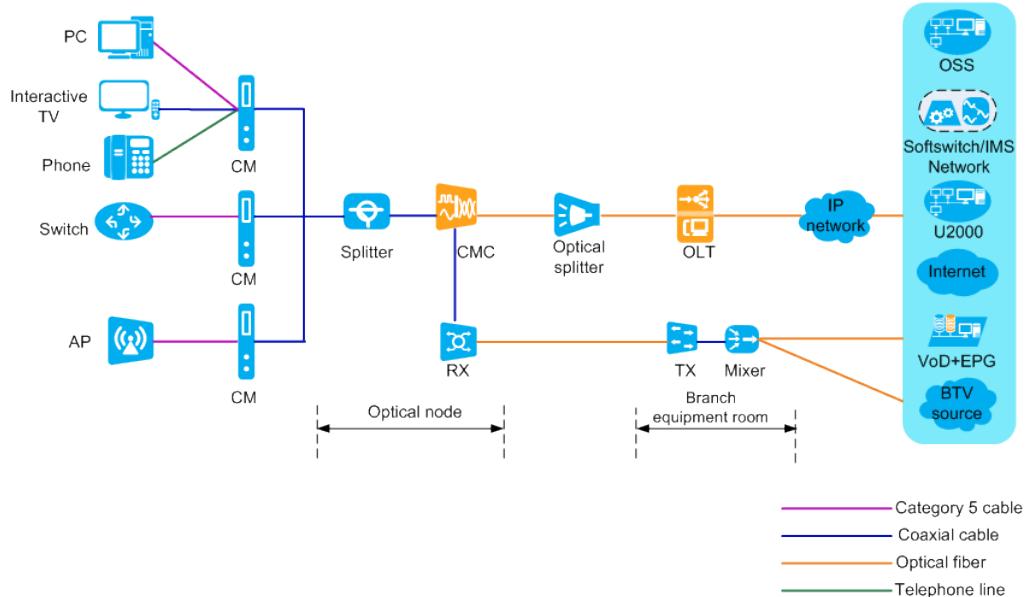
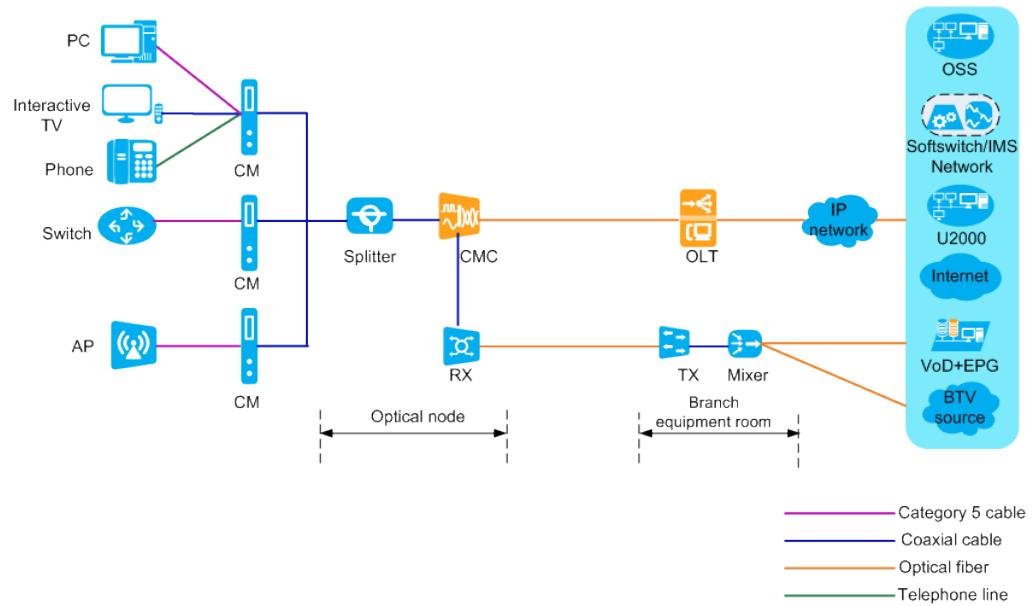


Figure 6-25 D-CCAP networking using GE upstream transmission



Network Pre-deployment

CMCs are installed in numerous installation offices that are distributed deployed. Therefore, CMC deployment is difficult and features high costs. U2000 supports offline batch deployment through a network planning sheet and remote MDU configuration issuing. The management channel and the service channel are set up immediately after the CMC is powered on and registers with an optical line terminal (OLT), and field manual configuration is not required. That is, the CMC is plug-and-play and supports remote and automatic configuration.

D-CCAP Centralized Management

Networking Applications

D-CCAP centralized management is categorized into GPON extended subrack management ([Figure 6-26](#)) and GE extended subrack management ([Figure 6-27](#)).

The OLT (MA5800 included) deployed in a hub equipment room functions as a main frame. It connects to CMCs (extended frames) located on optical nodes through GPON cascading boards or GE cascading boards. An optical line terminal (OLT) deployed in a branch equipment room functions as a main frame and connects to CMCs (CMCs, extended frames) located on optical nodes by using cascading boards. In this manner, remote extended frames are no longer standalone NEs (no longer allocated independent management IP addresses), but are managed by the main frame. These remote extended frames are regarded as remote service boards of the main frame and have the same functions and features as those of the main frame. The OLT and the CMC can be used as a traditional CMTS.

In the built-in EQAM solution scenario, EQAM devices are moved down from the hub to the FN and are integrated in CMC devices.

Figure 6-26 Networking diagram of centralized management for GPON extended subracks

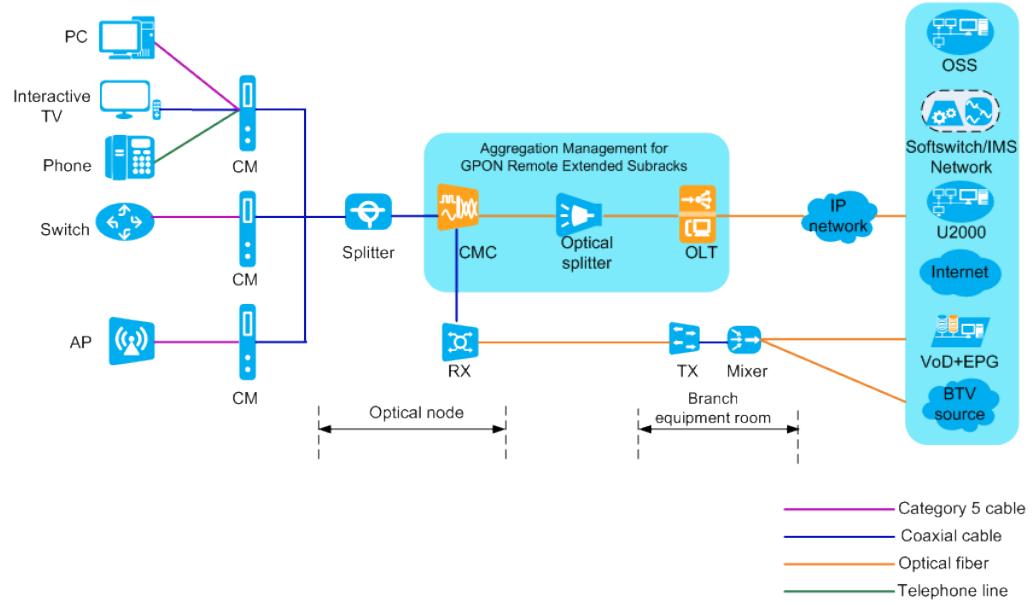
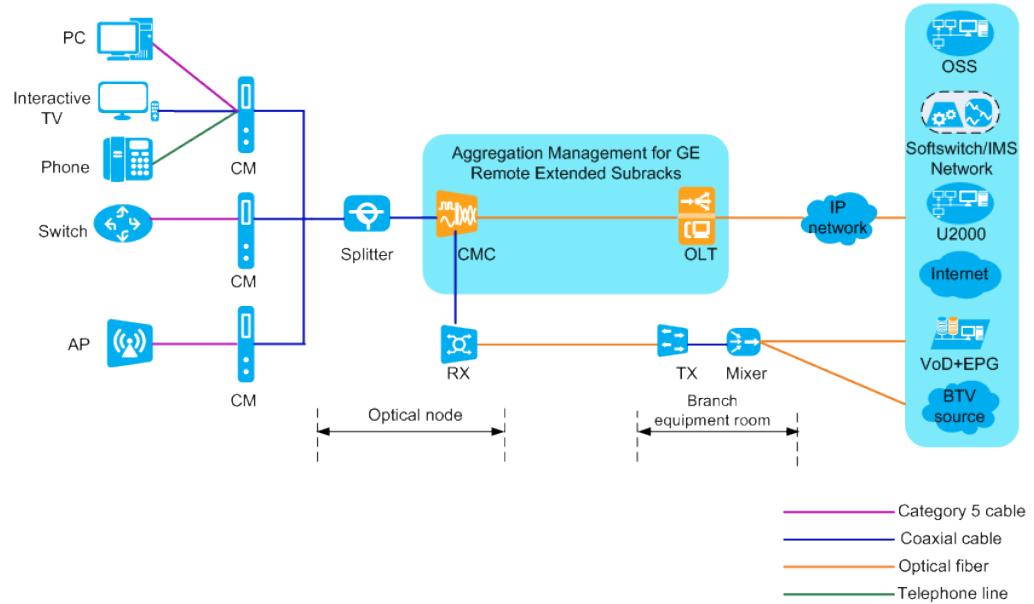


Figure 6-27 Networking diagram of centralized management for GE extended subracks



- This feature is compatible with the existing network.

A D-CCAP network consists of a coaxial cable network on the user side, a hybrid fiber coaxial (HFC) transmission network, and a metro aggregation network. In CMC centralized management, the OLT and the CMCs are compatible with the existing D-CCAP network and can replace traditional CMTSs. The coaxial cable network on the user side and the metro aggregation network remain unchanged. The CMC connects to a CM through a radio frequency (RF) port.

- This feature supports more users without increasing the number of management objects.
- Software commissioning is not required for remote extended frames and one onsite operation suffices.
- Service provisioning interfaces on remote extended frames remain unchanged. The user interface for extended frames is the same as that for a service board of the main frame, enabling consistent user experience.

Each CMC deployed at the remote end can be regarded as a new service board deployed on the main frame. The CMC does not need to interconnect with the upper-layer OSS or NMS system, reducing operating expense (OPEX) and total cost of operation (TCO) for carriers.

- PON ports and Layer 2 forwarding operations are transparent between the OLT and the CMCs, simplifying configurations for carriers.
- A new CMC after replacement does not require manual configurations because the OLT automatically issues configurations for it.

CMC Migration

In the D-CCAP centralized management scenario, CMCs can be migrated on a GE or GPON network to recover services automatically.

- GE migration scenario
 - CMC parts replacement: No operation needs to be performed on the U2000.
 - CMC migration: CMCs are migrated from one port to another. You need to open the **Migrate Frame** dialog box on the U2000 and select a cascade port.
- GPON migration scenario
 - CMC parts replacement: You need to open the **Migrate Frame** dialog box on the U2000, select the original cascade port, and enter the SN of the new hardware.
 - CMC migration: If no parts are replaced during CMC migration, you do not need to change SNs on the U2000. If parts are replaced, you need to change SNs and port IDs on the U2000.

Enhanced Cable O&M capability

Includes the enhanced networking capability, O&M capability, and security features.

- Enhanced networking capability: The EQAM solution is built in, which is mainly used in new network deployment or suburban bidirectional coverage. Suburban equipment rooms have poor conditions, and fewer data service bandwidths are occupied. The idle channels can be used for EQAM services, which lowers costs.
 - EQAM devices are moved down from the hub to the FN and are integrated in CMC devices.
 - Independent management, centralized management, and GPON and GE upstream transmission are supported.
- Enhanced O&M capability:
 - Cable traffic report: The cable traffic report collects cable traffic on network-wide CMC devices. This report supports two granularities, OLT and CMC, and provides guidance for network expansion.
 - Upstream spectrum monitoring: The upstream spectrum can be scanned when RF is disabled. You can disable an RF branch and check the noise of enabled branches to determine which branch the noise comes from. This reduces upstream noise and improves data, voice, and other service quality for cable users.

- EQAM service monitoring: The U2000 provides a monitoring GUI that presents a program list and brief information about programs carried by each RF port and channel of an EQAM device. You can intuitively view the VoD and device load condition.
- CMC migration: In the aggregate D-CCAP management scenario, CMCs can be migrated on a GE or GPON network to recover services automatically.
- Various maintenance methods are supported, such as reverse query of CMs based on CPE MAC addresses, service VLAN query based on CMs, upstream channel configuration maintenance, remote CM ping tests, DHCP emulation tests, and NGOD edge device management.
- Enhanced security features:
 - Anti-theft authentication failure alarms and key configuration are supported.
 - The TFTP proxy can be configured in aggregate management mode.
 - CMCs support Type B protection.

7 Basic Functions

About This Chapter

The U2000 provides comprehensive management functions at the element management layer and network management layer.

7.1 Overview of Functions and Features

This topic presents an overview of functions and features of the U2000.

7.2 Security Management

This topic describes how to implement security management, such as user management, login management, rights- and domain-based management, and security policy management, to ensure the security of the U2000. Security management also includes log management, which manages logs about the login, user operations, and running of the U2000. In addition, the high availability (HA) scheme and data backup are supported to provide a comprehensive security solution.

7.3 Topology Management

In topology management, the managed NEs and their connections are displayed in a topology view. You can learn the network structure and monitor the operating status of the entire network in real time by browsing the topology view.

7.4 Alarm Management

When an exception occurs on a network, the U2000 needs to notify maintenance engineers in a timely manner so that they can recover the network quickly.

7.5 Fault Diagnosis

The fault diagnosis tool is used to detect network connectivity and perform troubleshooting for the carrier network.

7.6 Performance Management

The performance of a network may deteriorate because of internal or external factors and faults may occur. To achieve good network performance for live networks and future networks while controlling costs, network planning and monitoring are necessary. In addition, network efficiency needs to be measured in terms of the throughput rate, resource usage, and error rate. The performance management function enables you to detect the deteriorating tendency in advance and solve the potential threats so that faults can be prevented. In addition, high-precision (10^{-6}) performance measurement based on service packets is implemented to collect performance indicators, including the packet loss rate, delay, and jitter.

7.7 Inventory Management

The U2000 supports unified inventory management of physical and service resources on the entire network. The U2000 provides clear and easily-accessible information to users so that they can acquire an accurate and complete understanding of the network-wide resources. The inventory information serves as a reference for service and expansion planning.

7.8 Log Management

Logs are used to record the information about operations that were performed and important events that occurred on the U2000. The U2000 allows administrators to query and save logs and collect statistics on logs periodically. This action facilitates fault analysis and detection of unauthorized logins and operations. Specifically, by browsing and collecting statistics on logs, you can query the client from which a user logged in to the U2000 server and query the operations performed by the user after login. You can also dump and print logs. Logs also can record operations that the OSS performed on NEs through NBIs.

7.9 Database Management

Database management includes managing NE databases and U2000 databases, and maintaining data consistency between the U2000 and NEs.

7.10 NE Communication Parameter Management

The U2000 communicates with managed NEs successfully only after the connection parameters are correctly set.

7.11 DCN Management

The U2000 communicates with NEs and manages and maintains network nodes through a DCN network.

7.12 NE Software Management

NE Software Management, also called DC, is an independent subsystem of the U2000. The DC is used to manage NE software and upgrading or downgrading NE software. Managing NE software includes saving, backup and policy management. Upgrading or downgrading NE software includes loading, restoration, task management and managing Software etc. For security, recommend to use SFTP as the transfer protocol between U2000 and NE.

7.13 Report Management

The U2000 provides reports on alarms, logs, and resources. You can print the data or save the data as a file. The reports in tabular format can be filtered by equipment type and saved in XLS, TXT, HTML, or CSV files.

7.14 System Monitoring

The U2000 provides a GUI-based system monitoring tool, which is used to manage the U2000 and query the system information.

7.15 Network Management System Maintenance Suite

The network management system maintenance suite (MSuite) is a tool offered by the U2000 for commissioning, deployment, maintenance of HA systems and distributed systems, and database management.

7.1 Overview of Functions and Features

This topic presents an overview of functions and features of the U2000.

Table 7-1 Overview of functions and features of the U2000

Function or Feature	Description
Unified network management	<p>The U2000 provides unified GUI-based management for Huawei NEs in the transport, IP, access domains (GUI is short for graphical user interface). It is a unified network management system (NMS) that offers comprehensive functions in managing NE and network alarms, security, performance, topology, logs, inventories, reports, and databases. In addition, it can obtain third-party equipment information using the SNMP protocol to manage third-party equipment. This function meets the requirements of network convergence and rapid development of customer services.</p>
Local craft terminal (LCT)	<p>The U2000 provides an LCT to manage and maintain the plug-and-play function of IP NEs and some transport NEs.</p> <ul style="list-style-type: none"> ● The U2000 LCT is an NE layer management system for the optical transport network. The U2000 LCT uniformly manages OptiX series optical transmission equipment from Huawei, such as MSTP, Metro WDM, LH WDM, LH WDM (NA), PTN and submarine equipment. ● U2000 Web LCT is an NE layer management system for the transport network. The Web LCT uniformly manages OptiX series optical transmission equipment from Huawei, such as the OSN 9560, NG WDM, NG WDM (NA), RTN and submarine equipment. ● U2000 IP LCT can generate scripts by using configuration templates and planning tables, and deploy the scripts to NEs in batches. This improves efficiency of making scripts. <p>For more information, see the corresponding <i>iManager U2000 LCT Product Documentation</i> at http://support.huawei.com/carrier for carrier or http://support.huawei.com/enterprise for enterprise.</p>
Centralized task management	<p>Centralized task management is an NMS task management mechanism that manages and coordinates all scheduled tasks in a unified management GUI. Two types of tasks are managed in the centralized task management mode: system scheduled tasks (periodic) and custom scheduled tasks (one-off). The two types of tasks can run automatically at a scheduled time. Users can set parameters and browse the task status, progress, and results.</p>
NE template management	<p>NE template management allows users to bulk configure NEs by using configuration templates. This makes NE configuration faster and easier. A large amount of repetitive and labor-intensive data entry for NE configurations can be avoided by using templates that automatically fill in the parameter values of the NEs.</p>
NE data configuration and management	<p>During NE data configuration, the U2000 supports bulk configuration of NE services by using configuration templates, importing data sheets, and loading configuration files. During data management, the U2000 supports the backup, restoration, and synchronization of NMS data and NE data. With this function, services can be provisioned quickly in the GUI.</p>

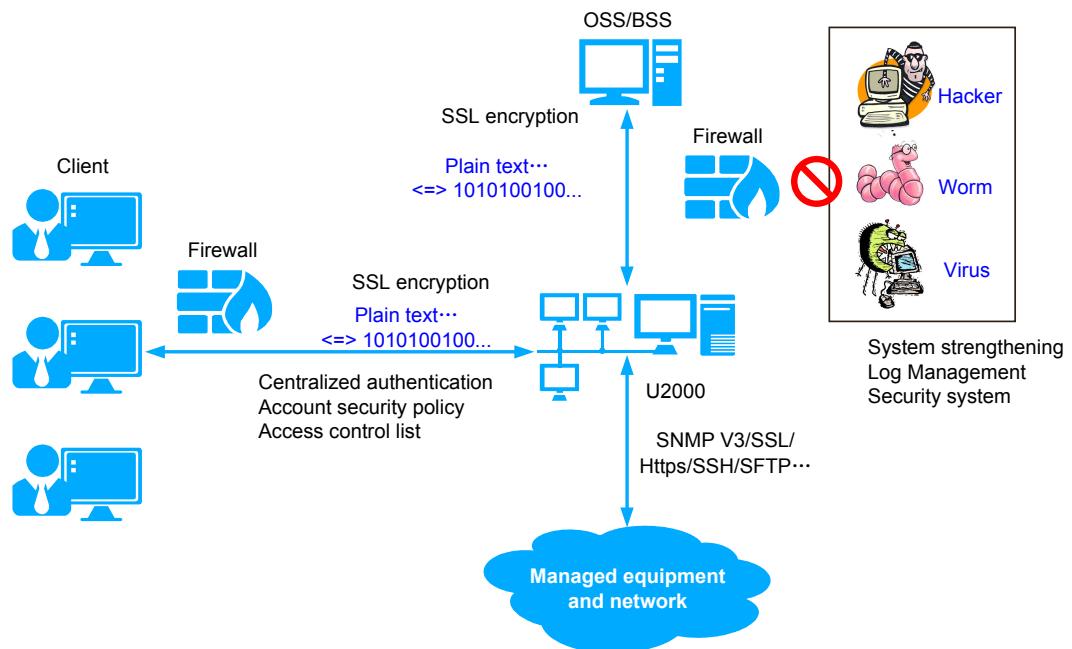
Function or Feature	Description
License management	<p>The U2000 provides an intuitive and easy-to-use NE license management window.</p> <p>License management allows users to query, apply for, and adjust licenses (in the event of a change in capacity or servers). By setting licenses, users can perform the operations required by the service scenario.</p>
Client auto install and update (CAU)	<p>The CAU function enables the U2000 client to install and upgrade automatically through the Internet provided that the U2000 server functions properly and communicates successfully with the U2000 client.</p>
Smooth upgrade	<p>The U2000 can be upgraded smoothly without service interruption, including version patch installation, rollbacks, and cross-version upgrades. After the upgrade, the NE status, basic services, and routing relationships are checked and a check report is generated. This helps to ensure the proper operation of major services immediately after the upgrade and achieve timely detection of issues such as data loss.</p>
Online Help	<p>The Online Help is displayed if users press F1 when using the U2000. It provides comprehensive help information and supports quick information searches. The help information is also available in offline mode.</p>

7.2 Security Management

This topic describes how to implement security management, such as user management, login management, rights- and domain-based management, and security policy management, to ensure the security of the U2000. Security management also includes log management, which manages logs about the login, user operations, and running of the U2000. In addition, the high availability (HA) scheme and data backup are supported to provide a comprehensive security solution.

Figure 7-1 shows the overview of security management.

Figure 7-1 Security management overview



This section mainly describes the network management system (NMS) user security.

- For the security solution to log management, see [Log Management](#).
- For the U2000 HA scheme, see [Deployment Mode](#).
- For the backup and restoration of the database, see [Database Management](#).
- For details about the firewall security policy, system enhancement policy, operating system (OS) and database security policy, and data transmission security policy, see chapter "Security and Reliability Planning" in the *iManager U2000 Planning Guide*.

User Management

When NMS users are planned, the required management and operation rights are assigned to specific users and only the authorized users can perform these maintenance tasks or use management functions.

- User management: The U2000 uniquely identifies the login, operation, and management rights of NMS users according to user names and passwords. Passwords for the U2000 users are encrypted using MD5+Salt or SHA256 encryption mechanism and saved in the database. Only one default user, **admin**, is provided after the U2000 is installed. User **admin** has all operation and management rights. Other users are directly or indirectly created by user **admin**.
 - The U2000 supports creation, modification, and deletion of users.
 - The creation of a user involves filling in the detailed information about the user and setting the user's group, management domains, operation rights, and access control lists (ACLs).
- User group management: The U2000 creates, modifies, and deletes user groups. The U2000 can create a user group to manage users that have the same rights and to bulk manage rights of NMS users. User group management reduces management costs. After

the management attributes of a user group are set and a user is added to the user group, the user has the same rights assigned to all the users in that group. A user can be added to multiple user groups. In this scenario, the user has all rights of its user groups as well as other rights that are uniquely assigned to the user.

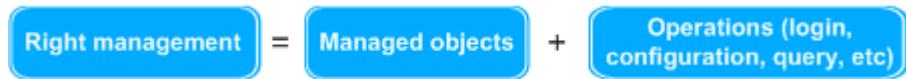
The U2000 has seven default user groups: **Administrators** group, **SMMangers** group, **NBI User Group**, **Maintenance Group**, **Guests** group, **Operator Group** and **uTraffic User Group**.

- The **Administrators** group has the rights to manage all network objects and has all operation rights except the security management rights. However, the management scope and operation rights cannot be modified. For example, if one U2000 user is locked, each member in the **Administrators** user group can unlock the user.
 - The **SMMangers** group has the rights to manage all network objects and has the related rights to perform security management, such as managing users, user groups, user names and passwords, user login, operation sets, device sets, and security logs, and setting user security policies.
 - **NBI User Group**: The user group that is created on the U2000 for the upper-layer OSS to interconnect with the U2000 through NBIs. Each member in this user group manages the access permissions for managing the OSS.
 - By default, users in the maintenance engineer, operator, or Guests are assigned a specific set of operations that they are allowed to perform. The sequence of these groups with an authority level from the highest to the lowest is the maintenance engineer group, operator group, and Guests.
 - The **Guests** group: Users can perform browsing and querying operations only.
 - Operator group: Users have basic rights of the Guests and can perform creation, modification, and deletion operations on the NMS, for example, create NEs, modify alarm severity, and configure an SDH trail.
 - Maintenance group: Except for having rights of the Guests and operator group, users can perform configuration operations that greatly affect NMS and NE running, for example, search SDH protection subnets and trails and delete a composite service.
 - uTraffic User Group: When uTraffic interconnects with the U2000, uTraffic accounts will be created on the U2000 to manage operation uTraffic rights on the U2000.
- A user account will be locked if you enter incorrect passwords for a consecutive of 3 times (The default value is 3. You can set the incorrect times.) to log in to the U2000. The user account can be unlocked in the following scenarios:
 - User **admin** is unlocked automatically after the automatic unlocking interval for user **admin**.
 - Non-admin users can be unlocked either automatically after the automatic unlocking interval or manually by user **admin** or members of the security management group.

Rights Management

Rights define operations that can be performed on managed objects. Each user has a specific set of rights to perform certain types of operations on certain elements. That is, for rights management, two aspects are involved: managed objects and operation rights, as shown in [Figure 7-2](#).

Figure 7-2 Rights



After NMS users are planned, these users can perform operations on network elements (NEs) only after required rights are assigned to them.

- Managed objects define objects that can be managed by users or user groups, and ranges of configuration data. For example, if user A is not authorized to manage NE C and object set D, the topology view will not display NE C and object set D to user A. An object set is a collection of managed NEs. The U2000 can create, modify, and delete an object set.
- Operation rights define operations that a user can perform. Different operation rights to the same NE or object set can be assigned to different users. An operation set is a collection of operation rights. Operation right management is implemented by managing the operation sets or specific operation rights. If operation sets are assigned to users or user groups, these users and user groups have rights to perform operations defined in the operation sets. The U2000 can create, modify, and delete an operation set.
- The U2000 also supports rights- and domain-based management. Only domain users with the required operation rights can perform operations on NEs in specific domains. Only members of the **SMMangers** user group can assign rights and domains to other users.
 - Domain-based management divides a network into different domains by allocating network objects such as NEs, services, or data to different domains. Users or user groups with domain rights can manage objects in those domains. Meanwhile, specific NEs can be assigned directly to a user or user group. In domain-based management, network objects in these domains are managed by different O&M divisions separately.
 - Right-based management authenticates on a per-domain basis. Users and user groups of a domain can be assigned different operation rights. In this manner, users with different responsibilities (in different positions or belonging to different O&M divisions) in the same domain have different operation rights to managed objects in the domain.

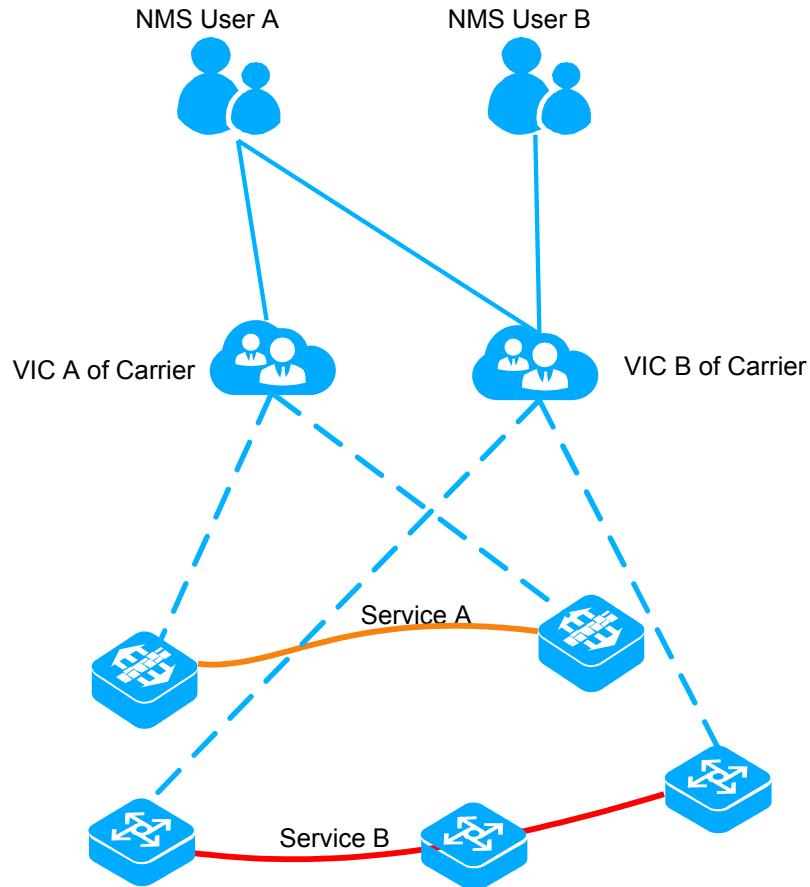
The U2000 manages NEs and functions in rights- and domain-based mode in a unified manner. Domain-based management is NE-specific and right-based management is NE-function-specific.

- The rights- and domain-based management provided by the U2000 has the following features:
 - For access NEs: supports menu-item-specific operation rights and board-specific management.
 - For transport NEs: supports menu-item-specific operation rights and end to end (E2E) service authentication for SDH or WDM trails.
 - For IP NEs: supports menu-item-specific operation rights and authentication for E2E services, including Layer 3 virtual private network (L3VPN), virtual private LAN segment (VPLS), pseudo wire emulation edge-to-edge (PWE3) and convergence services.
- The U2000 also supports flexible rights- and domain-based management for VIP services. Specific maintenance engineers are assigned to manage and maintain the

networks of specific customers. For example, some maintenance engineers are assigned for the services of a VIP customer, and these engineers are responsible for the network O&M for this customer. Rights- and domain-based management focuses on network monitoring for VIP customers. It improves O&M efficiency and achieves active O&M. Rights- and domain-based management supports the following authorization modes:

- Direct authorization: Administrators authorize services or service groups to NMS users.
- Indirect authorization: Administrators authorize customers to NMS users. Then, the NMS users can manage the services in the management domains of the customers. For details, see [Figure 7-3](#).

Figure 7-3 Indirect authorization



On the U2000, the trails that can be managed by a user are the trails that are covered by both authorization modes.

Only user **admin** can authorize or unauthorize a specific user by default. Other users are rights- and domain-based users. A new user cannot manage any services by default. Operation rights to services can be obtained only after service authorization.

Relationships between rights- and domain-based service management and NE management authentication can be explained as follows: Rights- and domain-based service management is complementary to NE management authentication. To obtain management rights to services, a user must meet the requirements for first NE management authentication and then service authentication.

NMS User Authentication Management

The U2000 provides three types of user authentication management: local authentication, remote authentication dial-in user service (RADIUS) authentication, and lightweight directory access protocol (LDAP) authentication.

- Local authentication: NMS user management, login authentication, and security strategies are implemented by the U2000 server. Local authentication is the default authentication mode for user login. For details, see [Local Authentication](#).
- RADIUS authentication: When a user logs in to the U2000, the RADIUS server verifies and authenticates the login request, and the U2000 assigns the logged-in users the rights of their user group. For details, see [RADIUS Authentication](#).
- LDAP authentication: When a user logs in to the U2000, the LDAP server verifies and authenticates the login request, and the U2000 assigns the logged-in users the rights of their user group. LDAP authentication is similar to RADIUS authentication, but the authentication protocols are different. For details, see [LDAP Authentication](#).

Local Authentication

In the local authentication mode, user security management ensures the security of the U2000 on multiple levels, including local user management, rights management, password policy, account policy, and login control.

- Password policy sets the following items:
 - Minimum password length (8 characters by default) and maximum password length (16 characters by default)
 - Correlation policy between the current password and historical passwords, including the minimum number of different characters between old and new passwords, and whether the password can be similar to historical passwords
 - Password validity, including the term (180 days by default), minimum use days (10 days by default), and number of days in advance that a warning is issued to users that their passwords will expire (10 days by default)
 - Rules for password complexity (for example, must contain at least one letter and at least one digit)
- Account policy sets the following items:
 - Minimum length of a user name (6 characters by default)
 - Time before unlocking a user (30 minutes by default)
 - Maximum number of login attempts (3 attempts by default)
 - Timeout period when a login or unlocking failure occurs (3 seconds by default)
 - Use policy for users that have never logged in (accounts are suspended by default if left unused for 60 days)
 - Time before locking out a user (by default, logged-in accounts will be automatically locked out if no operation is performed within 10 minutes)
- Login control sets the following items:
 - Login mode. It specifies whether multiple users are allowed to log in to the U2000 at the same time. Usually, the U2000 works in multiuser mode. If exclusive access to the U2000 server is required to perform a particular operation, set the login mode to single-user mode to avoid interferences from other users.
 - Login period. It specifies periods during which users can log in. Users can log in to the U2000 only during the specified login period.

- Login IP address. The ACL specifies the login IP addresses of clients. Users can log in to the U2000 server only from the specified IP addresses. This measure prevents unauthorized logins for someone who uses the stolen user account and password. The U2000 provides hierarchical ACLs:
 - System-level ACL: It specifies the IP address range for system clients. Specifically, only the clients in the specified IP address range can log in to the U2000.
 - User-level ACL: It specifies the users who can log in to the U2000 from the clients in the specified IP address range. User-level ACLs are included in system-level ACLs and take effect for specified users.

RADIUS Authentication

When RADIUS authentication is adopted, the administrator does not need to create a user account on the NMS in advance. The user account for logging in to the U2000 is an existing account that can pass the authentication of the RADIUS server.

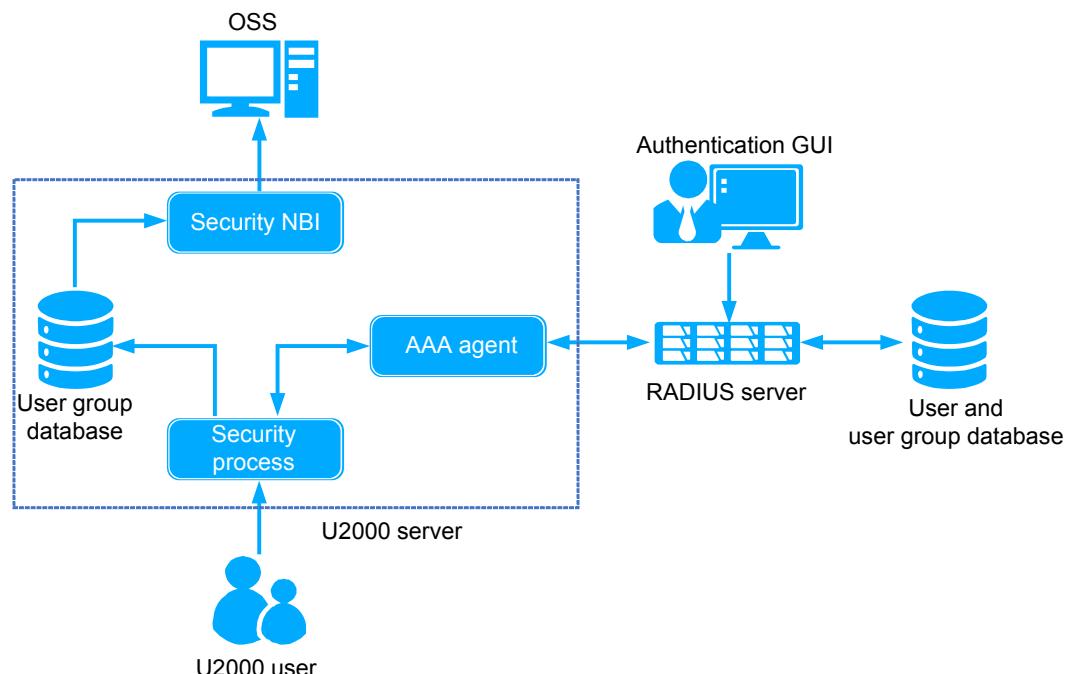
When a user enters the user name and password, the security process of the U2000 server sends the user name and password to the RADIUS server. If the user passes RADIUS authentication, the security process learns the user group to which this user belongs, and then the security process assigns rights to the user according to the operation set policy of the user group.

NOTE

Before using the RADIUS authentication mode, ensure that the name of the user group defined on the U2000 is the same as that defined in the account database of the RADIUS server. In addition, ensure that the account to be authorized is added to a user group.

For the RADIUS authentication process, see [Figure 7-4](#).

Figure 7-4 RADIUS authentication



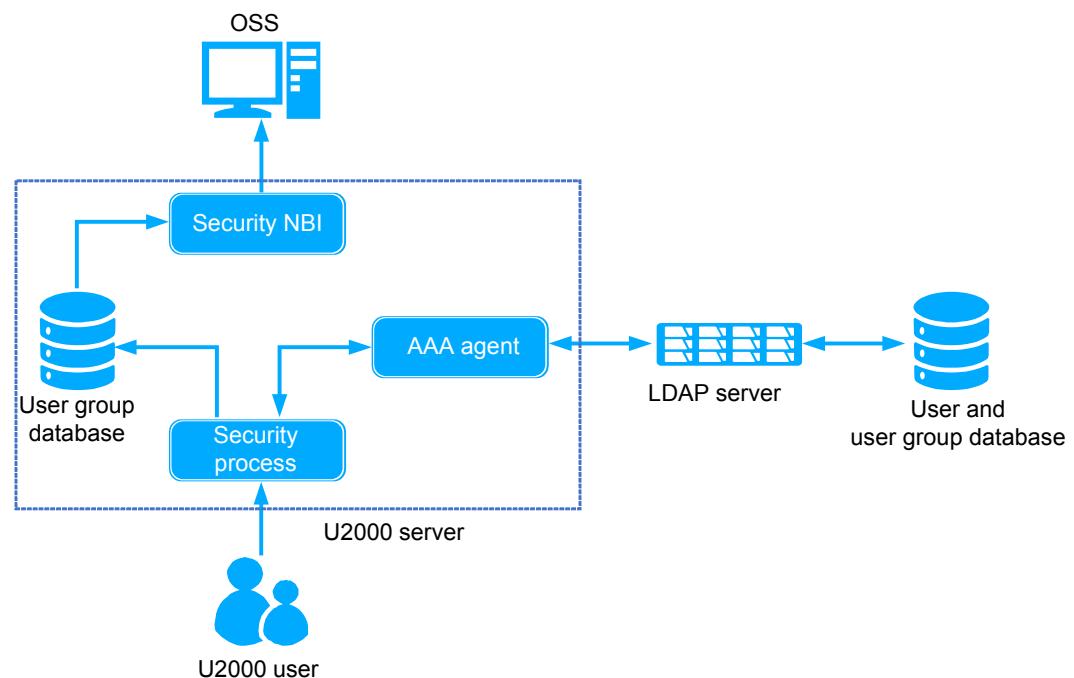
LDAP Authentication

As a distributed client/server system protocol, LDAP is used in the VPN and WAN to control user access to the network and prevent unauthorized users from accessing the networks. The LDAP authentication mode is similar to the RADIUS authentication mode, but they have different authentication protocols. The LDAP authentication mode supports the following features that are not supported by RADIUS authentication:

- Common mode (encryption-free), secure sockets layer (SSL) mode, and transport layer security (TLS) mode for communication between the U2000 and LDAP servers.
- Multiple LDAP authentication servers that are compatible with the HA scheme of the U2000.

For the LDAP authentication process, see [Figure 7-5](#).

Figure 7-5 LDAP authentication



Session Management

- The members of the SMMangers group can monitor sessions and operations of common U2000 users, forcibly log out U2000 users.
- The U2000 can automatically detect and terminate invalid sessions.
- Client lockout and unlocking:
 - Clients can be locked to prevent login of unauthorized users.
 - Automatic lockout: If you enable automatic lockout for a client, the client is locked automatically after a specified period of inactivity.
 - Manual lockout: A user can lock a client manually at any time to prevent unauthorized operations of other users.

Client unlocking for different users:

- If the current user is user **admin**, enter its password to unlock the client.
- If the current user is a non-admin user, enter its password to unlock the client. If the non-admin user forgets the password, an administrator can reset the password to unlock the client.

OS Security Hardening

The U2000 runs on common OSs: Windows, Solaris, or SUSE Linux. The default OS configurations usually do not meet the security needs of a telecommunications management system. Redundant services are running and unnecessary communication ports are opened by default, and the default TCP/IP parameters are vulnerable to attack. The OS can easily become a weak point of U2000 operations and management. To ensure that operations are secure and stable, the U2000 ships with OS security hardening software (SetSolaris/SetSuse/ SetWin) and default security hardening policies.

- SetWin is contained in the U2000 Windows software package and installed along with the U2000.
- SetSolaris is contained in the U2000 Solaris software package and installed along with the U2000.
- SetSuse is contained in the U2000 SUSE Linux software package and installed along with the U2000.

OS Security Patch

Because the U2000 runs on a commonly used OS, keeping the OS secure is a must for keeping the U2000 secure. U2000 version releases include the latest OS security patches and the U2000 prompts you periodically to install updated security patches. All security patches have passed U2000 compatibility tests.

For details about OS security patches, see the U2000 release notes.

Database Security Hardening

The U2000 uses common third-party database software, such as SQL Server and Sybase. Because the database software manages key U2000 data, database software security is crucial for U2000 data security.

Currently, the U2000 security solution ensures database security from the aspects of the database account password, sensitive file permissions, and patch. Only authorized users can access sensitive files. The database patch can be installed to address high-risk issues.

- Account/password management:
 - The default password for the database vendor is not used.
 - The database password meets the complexity requirements.
 - Unused accounts do not exist on the database.
- Authorization:
 - Strict permission control is performed on sensitive files of the Sybase database. The sensitive files can be read and written only by the database operating user and DBA user.
 - The minimum permission control is used for the backup of the database file and the data model file.

- Resource hardening:
 - Security hardening is performed on the system table to prevent unexpected modification. Only the **sa** user has the permission to modify the system table.
 - The risky storage extension process is removed from the Sybase database and the public permission for system storage extension is removed from the SQL Server 2008 database. This is to prevent malicious use of unwanted storage processes.
 - Unwanted functions, such as Java, system file access, are disabled on the Sybase database.
 - Neither the Sybase nor SQL server database uses the default system port provided by the database vendor. This is to prevent malicious attacks on the default system port.
 - The minimum permission control is performed on the Sybase database installation directory and home directory.
- Audit authentication: Login failure or success logs are recorded in the database log, which can be used to trace attacks on the database.
- Patch: U2000 version releases include the latest database security patches and the U2000 prompts you periodically to install updated security patches. All security patches have passed U2000 compatibility tests. For details about database security patches, see the U2000 release notes.

Antivirus

A virus scan using Symantec, OfficeScan, McAfee, Avira AntiVir and Kaspersky software is run before the U2000 is released. The U2000 has also passed the OfficeScan compatibility test.

The U2000 software package includes OfficeScan to protect the system against viruses.

Communication Security

Communications are subject to eavesdropping, tampering, and interception and redirection during the transmission process. The U2000 supports secure channels such as SNMPv3, SSL, and SSH to safeguard communication between U2000 components and between the U2000 and peripheral systems.

- Between the U2000 server and NEs: TCP/IP is used for communication between the U2000 server and gateway NEs. SNMPv3, SSL, SSHv2, SFTP, or STelnet can run between the U2000 server and non-gateway NEs.
- Between the U2000 server and clients: By default, Security(SSL) mode is used for communication between the U2000 server and clients. SSL or TLS can be used to implement communication encryption on data channels. HTTPS can be used for web installation of U2000 clients.
- Between the U2000 server and OSS: The U2000 server provides CORBA NBIs. SSL or TLS can be used to implement communication encryption on data channels. Secure communications that use SNMPv3, SFTP, XML (SSL), TL1 (SSL), and MML (SSL) or NBI are also available.

ACL

The U2000 provides an Access Control List (ACL) function to prevent unauthorized clients from accessing the U2000 server. IP addresses and network segments of clients allowed to access the U2000 server are configured in an ACL. Unauthorized clients are denied access..

The user management function can be used to configure ACLs for specific users. Specific entries can be selected from the system ACL entries. The selected entries form a subset of the system ACL and take effect only for specific users

Password Security

The U2000 uses a series of password protection mechanisms and solutions to prevent passwords from being compromised.

Password security policy management

- The U2000 checks by default that complexity requirements are met when a password is set.
- By default, passwords must meet complexity requirements.
- A maximum number of password entry attempts can be configured; failure to enter the correct password results in lock out.
- A lock out duration can be configured for users who reach the failed password entry attempt threshold.

Password use rules

- Passwords cannot be displayed in plaintext in the operation interface.
- Information in the password input box cannot be copied.
- Users can change their passwords. The current password must be verified before being changed.
- Passwords are not transmitted in plaintext.

Passwords transmitted between the U2000 server and clients are encrypted using RSA2048 and sent through SSL channels. In the server database and the configuration file, passwords are encrypted using AES128.

NE user passwords transmitted between the U2000 server and NEs can be sent through encrypted channels.

Passwords transmitted between the U2000 server and OSS can be sent through encrypted channels.

- Locally stored passwords must be encrypted. U2000 user passwords are encrypted using MD5+Salt or SHA256.

Software Integrity

Some bytes in software may be lost when software is released, during transmission, or when it is used. Software may also be tampered with by hackers or damaged by viruses or Trojan horses. Running software with such problems adversely affects the OS. A mechanism that protects software integrity and ensures that genuine software, which has not been tampered with is essential, is obtained.

The U2000 supports the PGPVerify to protect software integrity.

Privacy Protection

When the U2000 communicates with managed NEs, it may need to collect, process, and store personal data to prevent the data against malicious disclosure, loss, or damage. The U2000 provides a series of security protection mechanisms, including authentication, rights controls, and log records. Carriers also have a responsibility to formulate privacy policies that comply with the laws of the countries in which they operate and to take effective measures to ensure that personal data is fully protected.

Interface and Command Openness

- For details on the common commands of the U2000, see the *Administrator Guide*.
- For reference documents of the advanced commands, submit an application to Huawei. The advanced commands are used for internal commissioning and fault diagnosis only. Improper use may result in U2000 malfunction or service interruption.

7.3 Topology Management

In topology management, the managed NEs and their connections are displayed in a topology view. You can learn the network structure and monitor the operating status of the entire network in real time by browsing the topology view.

The U2000 has the **Physical Root**, **Clock View**, and **Custom View**. Important information can be easily learned in different views, which enables you to ascertain and monitor the operating status of the entire network conveniently.

The U2000 offers service topology management for various end-to-end services such as VPLS, PWE3, L3VPN, E-AGGR, and tunnel services. By means of the service topology, users can view and configure services easily.

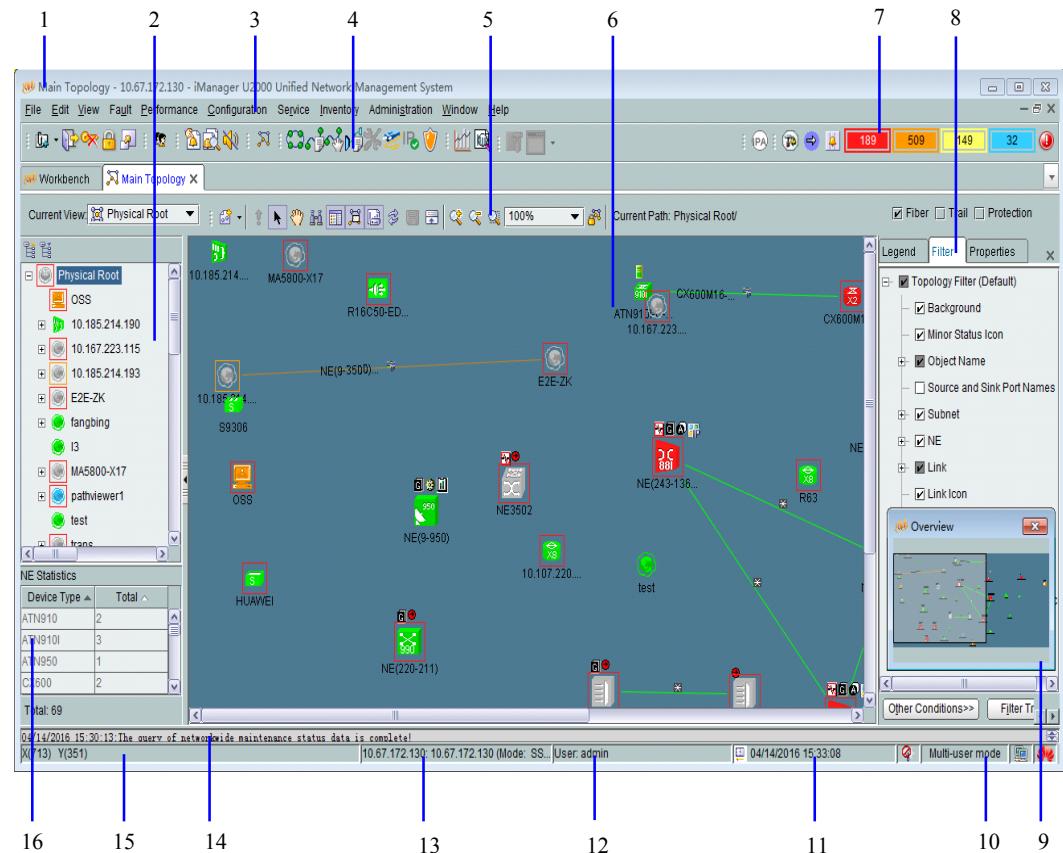
Topology View and Its Functions

The topology view of the U2000 consists of a navigation tree on the left side and a view on the right side. The navigation tree shows the network hierarchy. The view displays the objects at different coordinates on the background map, which helps to identify the locations of deployed objects.

You can set the background of the main topology view. U2000 supports the GIF and JPG pictures. U2000 offers a lot of geographical maps.

Figure 7-6 shows the topology view of the U2000 and its functions.

Figure 7-6 Topology view and its functions



1: NMS name

You can change the name of the network management system (NMS) as needed.

2: Topology navigation tree

In this area, all NEs managed by the U2000 are displayed. Using this tree, you can locate the required NE quickly.

3: Menu bar

You can perform operations on the NMS and the NE with the submenu bar, including configuring tasks and managing tasks.

<p>4 & 5: Shortcut icon</p> <p>By clicking a shortcut icon, you can:</p> <ul style="list-style-type: none"> ● Perform a simple task quickly. For example: exit NMS, lock terminals, log out, manage NMS users, stop the current alarm sound, NE Explorer, Browse Alarm, and Creating Connections. ● Perform a simple task quickly in the Main Topology. For example: zoom in or zoom out on the view, refresh or save the view, show or hide the navigators, search for objects, view object attributes, and lock or unlock the view. 	<p>6: Main Topology</p> <p>Views the managed NE.</p> <p>In the Main Topology, you can perform operations such as Creating NEs, Configuring the NE Data, Creating Connections, Browsing Fibers/Cables, Deleting Topology Objects, Browsing the Current Alarm, and Starting the NE Data Collection; enter the NE Explorer to configure the service for the NE and so on.</p> <p>To check the NE status and communication status, see Filter tree and Legends.</p>	<p>7: Alarm Panel/Alarm button bar/Event button</p> <p>The Alarm panel collects statistics on alarms of the managed objects by alarm severity and state according to the current alarm template. The alarm panel provides the fault status of the entire network. It can work as a monitoring panel.</p> <p>The Alarm buttons for alarms with different severities are in different colors. The number on the Alarm buttons indicates the number of the uncleared alarms generated on the current U2000. You can click the button to view current alarms.</p> <p>When the U2000 has abnormal events, the Abnormal event indicator turns red from green. You can click the indicator to view current abnormal events.</p>
<p>8: Legend, Filter and Attribute</p> <p>In this area, you can set the display modes of the objects in a view, view the descriptions of legends and NE attributes in the view. The filter tree and legends help you to locate an object quickly.</p>	<p>9: Overview</p> <p>You can locate the area displayed in the topology window easily.</p>	<p>10: Login mode</p> <p>Displays the login mode of the server. It can be single-user mode or multiuser mode.</p>
<p>11: Displays the client time in real time.</p>	<p>12: Views user name of the logged-in U2000 user currently.</p>	<p>13: Views the name which is set by the current U2000 client, and views the IP address of the current U2000 server.</p>

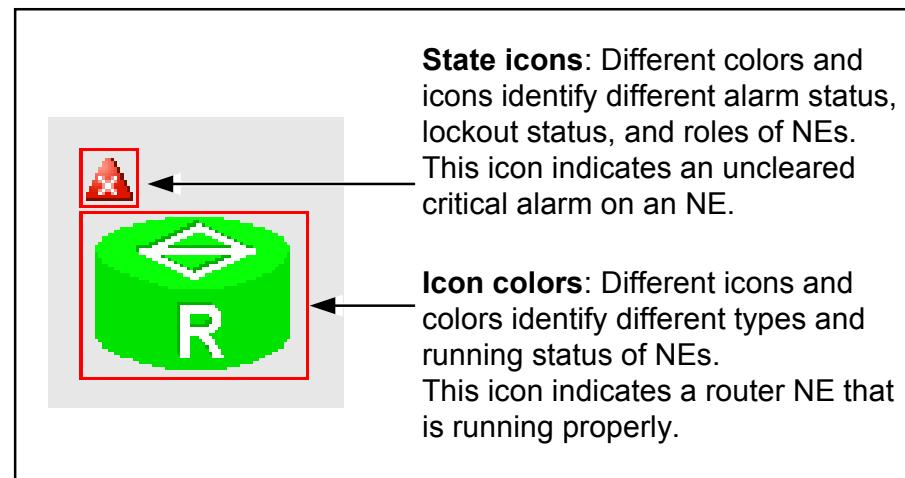
14: System information output window In this area, it mainly displays prompt information and operation echo information that affect the running of the U2000 server or client,	15: Display the mouse coordinate in the Main Topology currently.	16: Network-wide NE statistics In the NE Statistics , you can collect statistics on the types and quantities of the NEs on the entire network.
---	--	--

Alarm Display in the Topology View

In the topology view, alarms are displayed in different colors or icons to indicate different status of the subnets and NEs. The alarms are displayed with two methods: color-coded display and small icon display. The default method is the color-coded display, as shown in [Figure 7-7](#).

You can choose nodes of different levels from the **Physical Root** navigation tree such as a subnet, a node, or an NE to browse current alarms.

Figure 7-7 Alarm display in the topology view



The alarm display in the topology view has the following features:

- The color of a topological node indicates the operating status (such as normal, unknown, or offline) and alarm status of the monitored NE.
- When an NE generates multiple alarms of different severities, the color or icon that indicates the highest alarm severity of these alarms is displayed in the topology view.
- When multiple nodes in a subnet generate alarms, the subnet is displayed in the color or icon that indicates the highest alarm severity of these alarms.
- You can switch to the current alarm window of an NE using the shortcut menu of the NE node. In addition, you can query the details of current alarms in the NE Panel.

Automatic Topology Discovery

The U2000 provides an automatic topology-discovery function to automatically add NEs to the topology view; a feature that helps reduce the OPEX, as shown in [Figure 7-8](#).

For routers and switches, the U2000 supports some of the topology and link management functions defined in the IPv6 protocol.

- IPv6-based NEs and links are displayed with icons in the **Physical Root** view.
- When the relative configurations of the IPv6-based NEs and links are changed, the U2000 refreshes the IPv6-based NEs and links in the **Physical Root** view in real time. For examples, in scenarios wherein the NE-layer IPv6 function is enabled or the type of the IPv4 or IPv6 address of an interface is changed, the U2000 is triggered to refresh the **Physical Root** view.
- The **Protocol Type** parameter is used to filter NEs and links to display IPv6-based NEs and links in the topology view. The options are **IPv4**, **IPv6**, and **Dual-stack**.
- When IPv6-related alarms are reported to the U2000, the icons of IPv6-based NEs or links are color-coded based on the alarm severity to display the alarm status in the **Physical Root** view.

The U2000 supports the automatic topology-discovery function as follows:

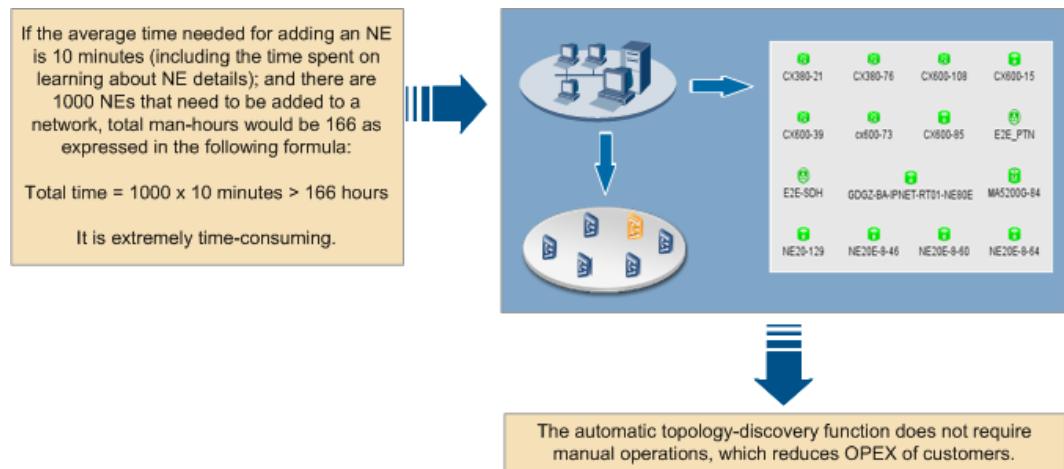
- Creates NEs in batches
 - Bulk creation of SNMP/ICMP-based NEs: SNMP/ICMP-based NEs involve the router, switch, security and access NEs. When the U2000 communicates with the preceding NEs successfully, it can search out the required NEs by IP address or by network segment and then bulk create these NEs.
 - Bulk creation of transport/PTN NEs: Based on the IP address, network segment, or network service access point (NSAP) address of a GNE, the U2000 automatically searches for all the NEs that communicate with the GNE and bulk creates the NEs.
 - Bulk import of NEs: Security GNEs, service monitoring GNEs, and security virtual network (SVN) series security NEs periodically sends proactive registry messages that contain the IP addresses of NEs to the U2000 server. With proactive registry management, the U2000 bulk creates the NEs after receiving the messages.
- Automatically discovers NEs: NEs can be automatically created on the U2000 and the associated data can be uploaded automatically to add the NEs to the U2000.

NOTE

The U2000 provides a secure channel for discovering NEs. The secure channel applies to the following NE versions:

- V600R009C00 and later versions of PTN 6900, NE, and CX series NEs
- V100R007C00 and later versions of PTN series NEs (excluding PTN 7900)
- V100R005C00 and later versions of RTN 300 series NEs, V100R008C00 and later versions of RTN 900 series NEs
- Schedules NE searches: The U2000 searches for specified NE types in specified network segments at scheduled intervals. The system automatically adds the new NEs to the topology view. The NE types include access, routers, switches, and security NEs.
- Automatically creates fibers/cables/Microwave Links or links: The U2000 can create fibers/cables/Microwave Links and links in batches. It can perform bulk searches for new fibers/cables/Microwave Links and links and automatically add them to the topology view after a search.

Figure 7-8 Illustration of the automatic topology-discovery function



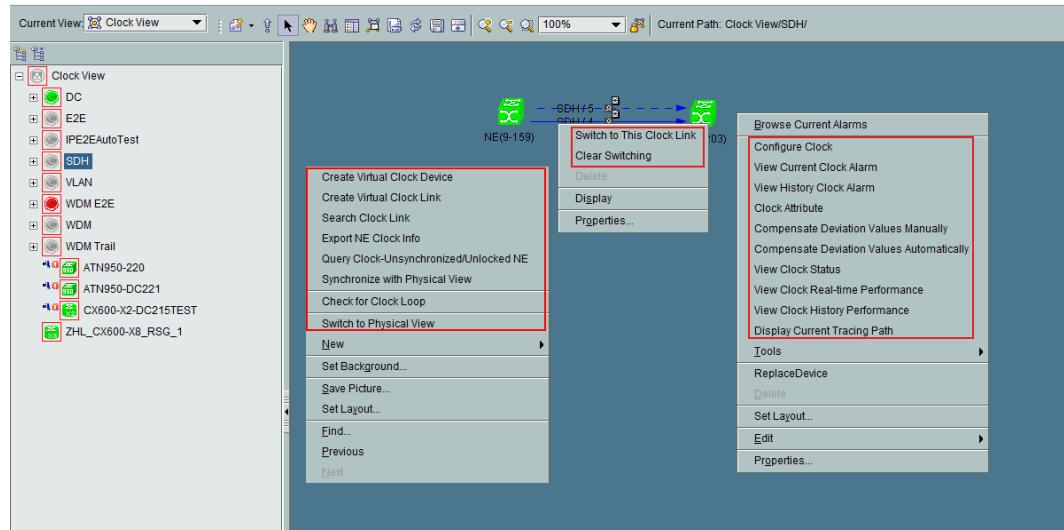
1. Automatic topology discovery is implemented step by step through a wizard. The wizard instructs you to set the parameters required for the automatic discovery, such as NE type, SNMP parameters, and the IP address range.
2. After you set the parameters, the U2000 searches for the required NEs in the specified network segments according to the preset conditions. All NEs from Huawei and other vendors that meet the conditions will be displayed in the topology view. Meanwhile, the basic configuration data of such NEs is uploaded, which simplifies configuration.
3. You can pause the automatic topology discovery at any time. If the discovery fails, you can view the cause after the discovery ends.

Clock View and Its Functions

In the clock view, you can perform the following operations: set NE clocks, query the network-wide clock synchronization status, search for clock tracing relationships, synchronize with the Physical View, view the master clock ID, query clock attributes, and view the clock lock state. The U2000 supports passive optical network (PON) clock, Physical clock, PTP clock, ACR clock and ATR clock. In the clock view, a variety of NEs can be displayed, such as MSTP series, NG WDM series, RTN series, OLT series NEs, ONU series NEs, MxU series NEs, PTN series, router NE40E, ATN series and CX600 NEs.

Figure 7-9 shows the clock view of the U2000 and its functions.

Figure 7-9 Clock view and its functions



<p>Discovering the clock topology automatically: The U2000 searches for clock links between all NEs in the entire network to obtain the clock tracing relationships of all NEs. You can search for clock links by NE or by clock link type. When the NE traced clock source has changed, you need to re-search for the clock trace relationship.</p>	<p>Viewing the clock topology: After the U2000 automatically discovers the clock topology, you can view the clock tracing relationships in the entire network. To adjust the clock topology, you can manually create and delete topological nodes and links.</p>	<p>Configuring clocks: In the clock configuration window of the NE Explorer, you can configure the clocks of the NE. You can configure the following clocks: PON clock, Physical clock, PTP clock, ACR clock and ATR clock. The clock configuration function varies with NE types.</p>
<p>Monitoring the change of clocks: When an NE or a link fails or a switching of clock sources occurs in a network, the U2000 automatically updates the clock tracing relationships and the clock synchronization status in the topology view. According to the clock alarms generated on the NE where a clock was changed, you can identify the fault.</p>	<p>Switching clocks manually: You can select a clock link and set its clock tracing relationship as the current clock tracing relationships of the NE.</p>	<p>Synchronizing with Physical View: You can synchronize the coordinate positions of NEs and subnets in the Clock View with the corresponding coordinate positions in the Physical View. In addition, after the synchronization, the subnets that have clock NEs are synchronized from the Physical View to the Clock View. The empty subnets in the Clock View are deleted.</p>

<p>Querying the clock attributes:</p> <p>You can query the type, hop count, and port name for clocks traced by the current NE, and view the compensation value for clocks traced by the port.</p>	<p>Querying the clock Status:</p> <p>You can query specific configurations of the NE. If the NE is in the abnormal state, this operation helps you diagnose and troubleshoot the fault.</p>	<p>Query Clock Loop:</p> <p>You can query clock loops for network-wide NE clock tracing relationships. In the query results, you can view loop information. If there are clock loops, double-click a record in the query result list to locate it on NEs in the clock view. Then, you can modify incorrect configurations on the NEs.</p>
<p>Switch to Physical View:</p> <p>The GUI switches to the corresponding subnet in the physical view. If the subnet does not exist in the physical view, the GUI will switch to the root of physical view.</p>	<p>Switch to Clock View:</p> <p>The GUI switches to the corresponding subnet in the clock view. If the subnet does not exist in the clock view, the GUI will switch to the root of the clock view.</p>	<p>Viewing master clock ID:</p> <p>When you move the pointer over a clock NE where clock tracing relationships exist, a tooltip pops up, displaying the NE's clock mode, master clock ID, port status, and other information.</p>
<p>Viewing Cable Transmitting Warp Report:</p> <p>The U2000 allows users to query cable transmission warp values for PTP clock links between NEs. Users can easily find the sites with large warp values and perform measurement only for these sites.</p>	<p>Querying Clock-Unsynchronized/Unlocked NE:</p> <p>You can search for the clock NEs in the unsynchronized or unlocked state. Such NEs are listed in the lower pane. In this list, you can select desired NEs and export their data.</p>	<p>Browsing real-time or historical clock performance:</p> <p>You can query clock performance status in the performance monitoring window displayed.</p>
<p>The clock view can display NEs copied in the physical root view and their clock tracing relationships. NEs copied from an NE own the same clock tracing relationships as the NE.</p>	<p>Querying the clock tracing trail:</p> <p>The U2000 highlights the current clock tracing paths of clock NEs. When a fault occurs, users do not need to draw the clock tracing path between NEs manually. This improves fault diagnosis efficiency.</p>	<p>Export NE Clock Info:</p> <p>Exports the clock information about one or all NEs to a specified path.</p>

7.4 Alarm Management

When an exception occurs on a network, the U2000 needs to notify maintenance engineers in a timely manner so that they can recover the network quickly.

Alarm management consists of the following functions:

- Network-wide alarm monitoring and remote alarm notification enable the U2000 to notify maintenance engineers of network exceptions in a timely manner so that the engineers can rectify faults quickly.
- Alarm correlation analysis, alarm association (with NEs, ports, or services), alarm masking, alarm suppression, alarm reversion, maintenance experience base, and configuration of alarm or event northbound filtering rules improve the accuracy and efficiency of alarm processing.
- Alarm synchronization ensures the reliability of alarms.
- Custom functions, such as alarm filtering, alarm redefinition, and time localization that can meet the requirements of different scenarios.

Alarm Severity

Table 7-2 shows different alarm severities and the handling methods.

Table 7-2 Alarm severity

Alarm Severity	Definition	Handling Method
Critical	A critical alarm indicates a fault or an event that may seriously affect an NE or the entire network, such as a board failure or a clock board failure.	Handle a critical alarm immediately to avoid a system breakdown.
Major	A major alarm indicates a fault or an event that may affect part of a network, such as a board failure or line failure.	Handle a major alarm in a timely manner to avoid failure of important functions.
Minor	A minor alarm indicates a general fault or an event affecting board or line functions.	Such alarms are used to remind the maintenance engineer to efficiently locate the alarm causes and eliminate the possible faults.
Warning	A warning alarm indicates a fault or an event that does not affect system performance or services but may potentially affect the service quality of the NE or resources. Some refers to the prompt information about the system when equipment restores to normal, for example, the switching alarm.	Handle a warning alarm based on the operating status of the network and NEs.

- You can specify alarm sounds for different severities of alarms. If an alarm is generated, the sound box on the computer where the client is installed produces corresponding sound.
- Different handling policies are provided for different severities of alarms. You can redefine severities of specified alarms on the U2000 based on needs by following [redefine alarm severities](#).

 **NOTE**

Alarm severities need to be adjusted to suit the impact that the alarm has on services.

Alarm Status

- Alarm acknowledgment and alarm clear
 - Alarm acknowledgment: An acknowledged alarm indicates that the alarm has been handled by a user. Alarm acknowledgment includes manual acknowledgment and automatic acknowledgment.
- Alarm status classification

Based on the status of alarm acknowledgment and alarm clear, alarm status can be classified into the following types:

- Unacknowledged and uncleared
- Acknowledged and uncleared
- Unacknowledged and cleared
- Acknowledged and cleared

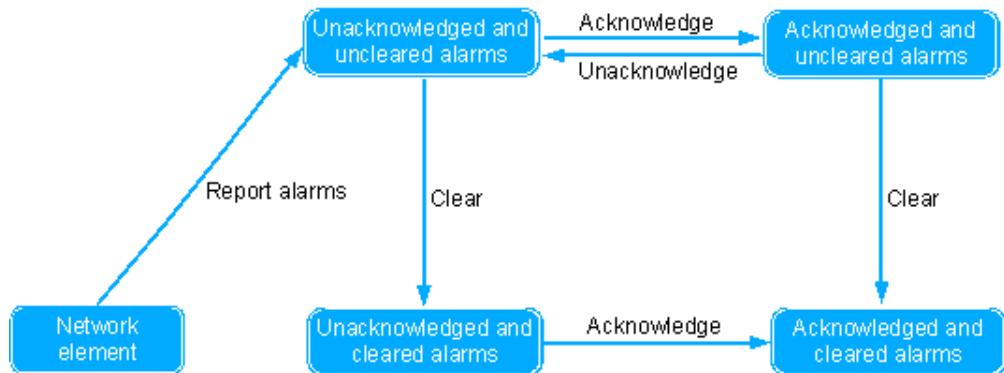
 **NOTE**

Acknowledged and cleared alarms become historical alarms after the user-preset period elapses.
All non-historical alarms are current alarms.

- Changing alarm status
 - Changing the clear status
When the condition triggering an alarm disappears, the NE or the U2000 server recovers. In this case, the NE or the U2000 server reports a clear alarm. The alarm status changes from uncleared to cleared. You can also manually clear an alarm.
 - Changing the acknowledgment status
If an alarm is acknowledged, it indicates that the alarm will be handled or has been handled. After the alarm is acknowledged, the alarm status changes from unacknowledged to acknowledged.
You can unacknowledge an acknowledged alarm if necessary; doing so will switch the alarm status back to unacknowledged.
- Relationships between alarm states

Figure 7-10 shows the relationships between alarm states and how an alarm changes from one state to another.

Figure 7-10 Relationships between alarm states



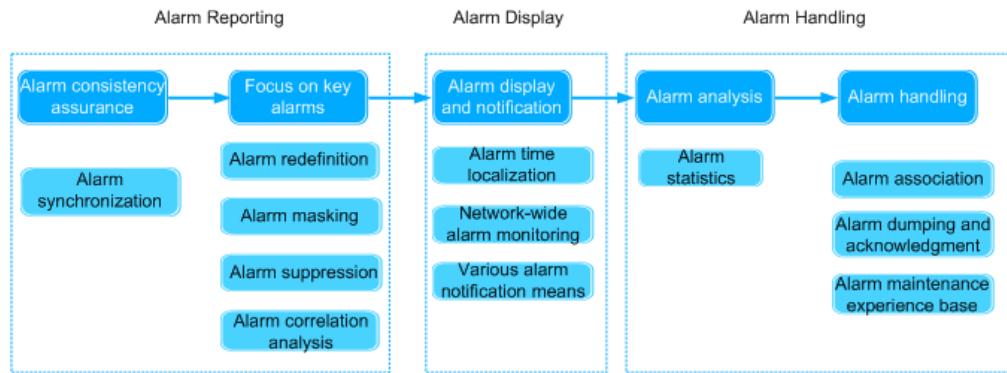
Alarm Category

- Communication alarms: refer to the alarms related to NE communication, ECC communication, and optical signal communication. For example, the interruption of NE communication and the loss of optical signals.
- Process alarms: refer to the alarms related to the software processing and exception. For example, equipment bus collision and the standby path check failure.
- Equipment alarms: refer to the alarms related to equipment hardware. For example, the laser failure and the optical port loopback.
- Service alarms: refer to the alarms related to the service status and network QoS. For example, the multiplex section performance threshold-crossings and the excessive B2 bit errors.
- Environment alarms: refer to the alarms related to the power supply system and the environment, such as temperature, humidity, and access control. For example, the temperature of the power module exceeds the threshold.
- Security alarms: refer to the alarms related to the security of the U2000 and NEs. For example, an NE user is not logged in.

Alarm Reporting and Handling Flowchart

Figure 7-11 shows the alarm reporting and handling flowchart of the U2000.

Figure 7-11 Alarm reporting and handling flowchart



Network-Wide Alarm Monitoring

Traditionally, network maintenance was domain-based. Faults across domains needed to be located manually, which lowered the efficiency. The U2000 provides unified alarm monitoring such as the network-wide alarm panel and alarm browsing, which helps users to ascertain the operating status of the network in real time. It also provides alarm query templates that are a collection of common query criteria. Users can create different alarm query templates according to the region, type, and network layer of the device on which an alarm is generated. The alarm query templates facilitate the query and monitoring of alarms.

There are three distinct alarm displays: alarm panel display, alarm bar chart, and alarm query and browsing.

Table 7-3 Alarm display functions

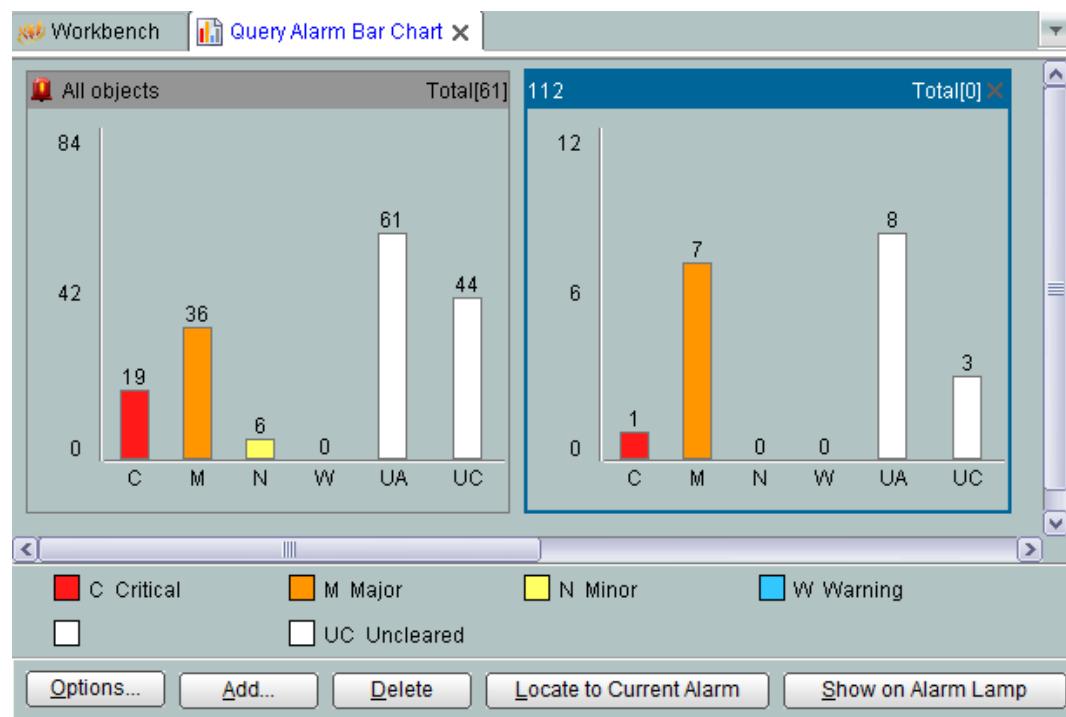
Function	Description
Alarm panel	<p>Figure 7-12 shows the alarm panel.</p> <p>The alarm panel collects and displays statistics such as alarm severity and quantity of managed objects. The alarm panel provides a summary of system faults and can be used as a monitoring panel.</p>
Alarm bar chart	<p>Figure 7-13 shows the alarm bar chart.</p> <p>The alarm bar chart shows alarm statistics in real time. The alarm bar chart displays the alarm statistics collected by the alarm panel.</p>

Function	Description
Querying and viewing alarms	<p>Browsing alarms includes browsing current alarms, browsing historical alarms, browsing alarm logs, and browsing event logs. In addition, alarm browsing provides multiple customized functions, as shown in Figure 7-14 and Table 7-4.</p> <ul style="list-style-type: none"> Viewing current alarms: Query the fault alarms that have not been handled; that is, unacknowledged or uncleared alarms. Viewing historical alarms: Query the fault alarms that have been handled; that is, acknowledged and cleared alarms. Viewing alarm logs: Query all fault alarms that are reported. Viewing event logs: Query all abnormal events that are reported. Configuring an alarm query template: Save common filter criteria as an alarm query template. Users can then use the template to search for alarms based on the criteria set forth in the template. This function helps users view and monitor important alarms. <p>In the alarm browsing window, you can browse the following information about an alarm: the severity, name, alarm source, location information, frequency, first time of occurrence, last time of occurrence, clear time, acknowledgment time, Fiber/Cable Name, clear user, acknowledgment user, clear status, acknowledgment status, location, direction, trail domain, alarm reversion, protection subnet name, alarm plane, trail name, ASON object name, and operation impact flag.</p>

Figure 7-12 Alarm panel



Figure 7-13 Alarm bar chart



Alarm browsing consists of viewing current alarms, historical alarms, alarm logs, and event logs; and has several customizable functions, as shown in [Figure 7-14](#) and [Table 7-4](#).

Figure 7-14 Viewing alarms

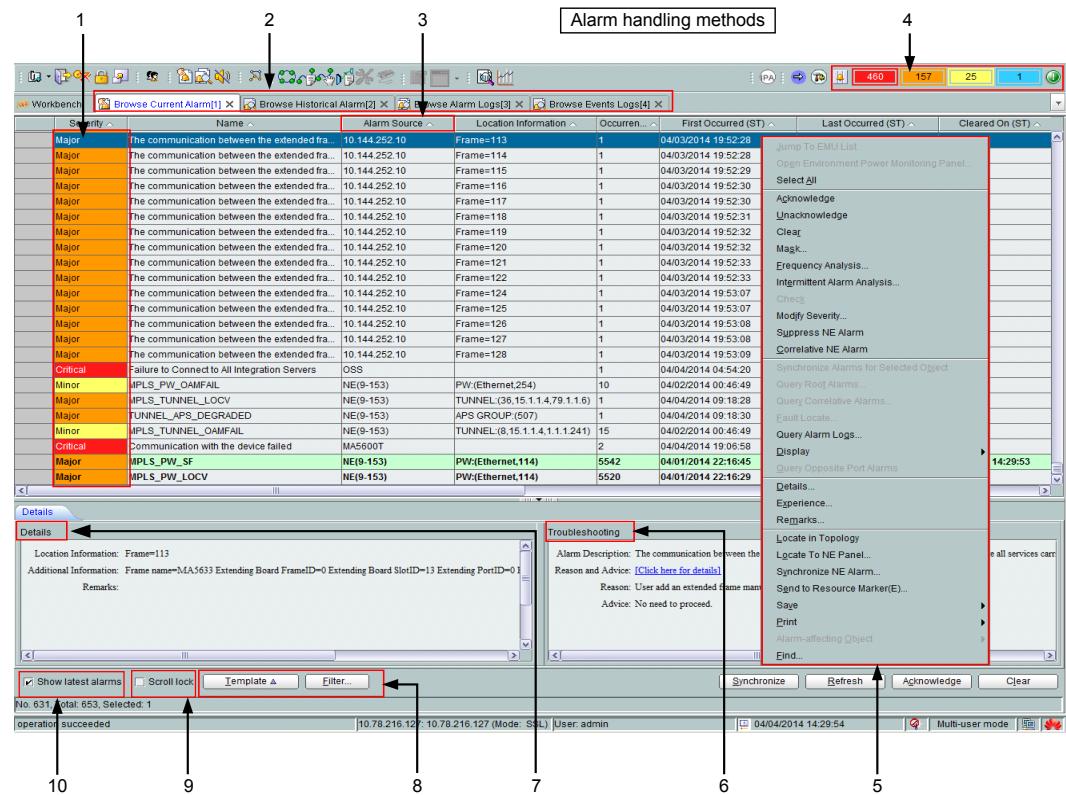


Table 7-4 Alarm function

No.	Function	Description
1	Alarm display in color	Alarms of different severities are displayed in different colors in the alarm list. The colors can be customized.

No.	Function	Description
2	Alarm viewing	<p>On the U2000, you can view NE alarms and service alarms to ascertain the operating status of the NEs and networks, and view the hierarchical alarms of NEs, boards, interfaces, protocols and services. Specifically, multiple windows for browsing alarms can be opened on one client.</p> <ul style="list-style-type: none"> ● Viewing current alarms: View current alarms of all severities on the entire network. ● Viewing current alarms that are severity-specific: You can quickly ascertain the critical, major, or minor alarms of the entire network from the alarm icons on the toolbar. ● Viewing the alarms of a specified NE or U2000: You can select an NE or a U2000 in the Main Topology and quickly ascertain the current alarms of the selected object. ● Viewing the current alarms of a trail: In the trail management window, you can quickly ascertain the alarms and events of the managed trails. This function facilitates trail maintenance. ● Viewing historical alarms: By viewing all historical alarms of the U2000, you can ascertain the faults that occurred on the U2000 and NEs. The historical alarm data can be used for long-term performance analysis.
3	Alarm sort Customized display	You can sort alarms by field and customize the columns displayed in the alarm list. Alarm data can be saved to a file (.txt, .html, .xls, pdf, or .csv) and can be printed.

No.	Function	Description
4	Dynamic alarm panel	On the U2000 client, the alarm panel sorts alarms by severity and quantity. Current alarms are indicated with a pop-up alarm panel or flashing indicators. Double click the alarm panel to display the window for browsing alarms.
5	Alarm handling method	<p>Alarm masking: A large number of alarms may be generated during NE maintenance, testing, or deployment. You can set alarm masking rules on the U2000 to discard unneeded alarms and events, which are neither saved to the alarm database nor displayed on the U2000 or upper-layer OSS. This mechanism allows you to quickly locate desired ones.</p> <p>Alarm locating: You can select a desired alarm, right-click, and choose Locate in Topology from the shortcut menu to locate the alarm object in a topology (choose Locate to NE Panel from the shortcut menu for a physical alarm).</p> <p>Alarm Acknowledgment Alarm acknowledgment enables you to check whether alarms were processed properly and that timely follow-ups will be performed on alarms that remain unprocessed. Alarms can be acknowledged manually or automatically.</p> <p>Remote alarm notification: You can select a desired alarm, right-click, and choose Remote Alarm Notification from the shortcut menu to allow the U2000 to send alarm information to maintenance personnel through an email or text message. This function enables remote maintenance personnel to know alarm and event information in a timely manner and then take appropriate measures.</p>

No.	Function	Description
		Alarm saving/printing: Query results can be saved and printed.
6	Handling suggestion	The handling suggestions provide information, such as the alarm cause, recovery suggestion, alarm description, maintenance experience, and cause type. In the Handling Suggestion area, a link to the corresponding alarm reference topic in Online Help is provided. You can click Click here to show detail information to display the corresponding alarm reference topic in Online Help.
7	Details	You can obtain the details of an alarm, such as the alarm name and identification information.
8	Alarm filtering	Alarm filtering When a large number of alarms exist, you can filter alarms by alarm name, alarm severity, status, type, last occurrence time segment and clear time segment. The alarm filtering function improves the efficiency of viewing alarms. You can also customize filter templates based on the attributes of alarm sources, such as the objects of NEs, object groups, and maintenance areas. In this manner, you can select the required alarm filter template to filter alarms.
		Alarm template The alarm template can be customized. Therefore, you can sort and locate alarms quickly.
9	Scroll lock	After this check box is selected, alarms displayed in the alarm browsing window remain unchanged.

No.	Function	Description
10	Show latest alarms	After this check box is selected, the most recently reported alarms are automatically displayed in the current alarm browsing window, which helps obtain the latest alarm information.

Alarm Statistics

You can quickly acquire alarm information by collecting and analyzing alarm statistics.

The U2000 can sort alarms by the preset criteria. The criteria include the name, severity, function type, generation time, alarm status, alarm source, or a combination of the preceding items.

Alarm Masking

- By using the alarm masking function, you can set conditions to mask irrelevant alarms/events to avoid redundant information.
- While an NE is being repaired, tested, or deployed, the NE may report a large number of alarms which can be ignored. In this case, you need to mask these alarms so that the U2000 neither displays nor saves them.

Correlation Analysis

The U2000 provides the following methods for correlation analysis: alarm/event correlation analysis, transient alarm analysis, repeated event analysis, alarm/event frequency analysis, and analysis on duration of acknowledged but uncleared alarms.

● **Alarm/event correlation analysis**

Alarm/event correlation analysis U2000 is used for analyzing alarms reported by NEs within a period and identifying root and correlative alarms based on some rules. These identified alarms are then displayed to O&M personnel. If a root alarm is cleared, its correlative alarms will be automatically cleared.

This function enables O&M personnel to recognize root and correlative alarms. When locating a fault, they can ignore correlative alarms and focus on root alarms so as to improve fault handling efficiency.

Alarm correlation analysis is used for three types of alarm: NE, NMS, and custom alarms.

- Alarm correlation rules on NEs: inherent alarm performance monitoring mechanism of a logical function block of an NE. These rules cannot be modified. Understanding the monitoring mechanism helps you to correctly analyze and identify faults.
- Alarm correlation on the U2000: After you set alarm correlation analysis rules on the U2000 and enable the alarm correlation analysis, correlative alarms are masked.

IP alarm correlation analysis is applicable to the following routers and switches.

Alarm correlation analysis is applicable to all transport devices for the following alarms:

- Alarms generated on the same NE.
- Alarms generated between upstream and downstream services.
- Alarms generated at the peer end of a service.

Alarm correlation analysis is mainly applicable to FTTx network services, including GPON and EPON services.

Viewing root and correlative alarms: In the alarm list, root alarms are displayed while correlative alarms are hidden. The bell icon indicates that the alarm next to it is a root alarm with correlative alarms, as shown in [Figure 7-15](#).

Figure 7-15 Viewing root and correlative alarms

Severity	Name	Alarm Source	Location
Major	The communication between the service board and the control board fails	MA5606T	Frame=0, Slot=2, Board Name=H802SHLB Board de...
Major	The communication between the service board and the control board fails	10.71.62.8	Frame=0, Slot=4, Board Name=H801EPBA
Major	The communication between the service board and the control board fails	10.71.62.8	Frame=0, Slot=7, Board Name=H801AIUG
Major	The communication between the service board and the control board fails	10.71.62.8	Frame=0, Slot=16, Board Name=H801CTB
Major	The communication between the service board and the control board fails	10.71.62.8	Frame=0, Slot=15, Subslot=65535, Port=2,
Major	The feed fiber is broken or OLT can not receive any expected optical signals(LOS)	10.71.62.8	Frame=0, Slot=15, Subslot=65535, Port=2,
Major	The communication between the service board and the control board fails	MA5606T	Frame=0, Slot=3, Board Name=VDM Board descrip...
Major	The communication between the service board and the control board fails	MA5606T	Frame=0, Slot=3, Board Name=H802SHLB Board de...
Major	The communication between the service board and the control board fails	MA5606T	Frame=0, Slot=3, Board Name=ADL Board descrip...

● **Transient alarm analysis/Repeated event analysis**

- Transient alarms are the alarms that are cleared twice within the preset period. Repeated events are the events that are reported repeatedly within the preset interval.
- If transient alarms are reported continuously within a short period, the NE or services may be repeatedly switched between the normal state and the abnormal state. To resolve the problem in time, enable the transient alarm analysis and raise the alarm severity so that maintenance engineers assign the proper priority to handling the alarms. For example, if an alarm is reported and cleared five times within ten seconds, the U2000 changes the severity of the alarm to major.
- Alarms or events that are reported repeatedly within a short period due to certain faults may be redundant to maintenance engineers, lower the alarm severity, sort the repeated alarms, or directly mask these alarms.
- For these alarms or events, you can set analysis rules for transient alarms and repeated events on the U2000. Then, the U2000 will display only the first repeated event or cleared transient alarm and will discard the rest.

● **Alarm/Event frequency analysis**

- Alarms of the same type that are generated within a period may be related to each other. After you enable the alarm/event frequency analysis, if the number of the same alarms generated within a period reaches a certain number, it can be concluded that those alarms are related to each other.
- After you set rules for the event/alarm frequency analysis, if the number of specified alarms generated within a specified period exceeds the preset threshold, it can be concluded that these alarms are related to each other. The U2000 will handle these alarms according to the preset method.

● **Analysis on the duration of acknowledged but uncleared alarms**

- Major alarms are normally cleared within 30 minutes after they are handled. If a major alarm is not cleared within 30 minutes after it is processed, further actions are

required. To ensure that major alarms are handled in time, enable the analysis on the duration of acknowledged but uncleared alarms. If a major alarm is not cleared in 30 minutes after it is handled, the U2000 changes the severity of the alarm to critical.

- Enable this function for acknowledged alarms that remain uncleared for a long time. The U2000 changes severities of the alarms to a higher level to remind maintenance engineers to handle the alarms in a timely manner.

Alarm/Event Dumping

U2000 supports the following 3 methods of alarm/event dumping:

- **Manual Dump:** you can manually dump alarms or events. Dumped alarms or events are deleted from the database, avoiding insufficient database space.
- **Overflow Dump:** the U2000 periodically checks whether the number of alarms or events in the database reaches the specified threshold. If the overflow dump condition is met, the U2000 automatically dumps alarm/event logs. The dumped alarm/event logs are deleted from the database, avoiding insufficient database space.
- **Scheduled Alarm Log Dump:** you can periodically or immediately export alarm or event logs that meet the conditions. The exported logs are saved in files and these logs cannot be deleted from the database.

NOTE

- You can only modify task parameters, instead of deleting the three system tasks or establishing a new dumping task.
- The dumped alarm data can be saved as files in csv, xml, txt, or html format, and these files can be decompressed.

Alarm Dump	Default Path	Dump File Naming Rule
Manual dump	<ul style="list-style-type: none">● The dump path of alarm data is \$IMAP_ROOT/var/AlarmManualDump/F M on Solaris and SUSE Linux and %IMAP_ROOT\var\AlarmManualDump\FM on Windows.● The dump path of event data is \$IMAP_ROOT/var/EventManualDump/F M in Solaris and SUSE Linux and %IMAP_ROOT\var\EventManualDump\FM on Windows.	<ul style="list-style-type: none">● Alarm log file: YYYYMMDDHHMMS-S-alarm-log-manual_(UTF-8)-<number>.zip● Event log file: YYYYMMDDHHMMS-S-event-log-manual_(UTF-8)-<number>.zip

Alarm Dump	Default Path	Dump File Naming Rule
Overflow dump	<ul style="list-style-type: none"> ● The dump path of alarm data is \$IMAP_ROOT/var/ FaultOverFlowDump/F M on Solaris and SUSE Linux and %IMAP_ROOT\var \FaultOverFlowDump \FM on Windows. ● The dump path of event data is \$IMAP_ROOT/var/ EventOverFlowDump/ FM in Solaris and SUSE Linux and %IMAP_ROOT\var \EventOverFlowDump \FM on Windows. 	<p>The following files are generated in the <Export to>/<YYYYMMDD> directory.</p> <ul style="list-style-type: none"> ● If you select no compression when setting extension parameters, the following files are generated: <ul style="list-style-type: none"> - Alarm log file: YYYYMMDDHHM MSS-alarm-log-auto_(UTF-8)-<number>.xml - Event log file: YYYYMMDDHHM MSS-event-log-auto_(UTF-8)-<number>.xml ● If you select compression when setting extension parameters, the following files are generated: <ul style="list-style-type: none"> - Alarm log file: YYYYMMDDHHM MSS-alarm-log-auto_(UTF-8)-<number>.zip - Event log file: YYYYMMDDHHM MSS-event-log-auto_(UTF-8)-<number>.zip

Alarm Dump	Default Path	Dump File Naming Rule
Scheduled alarm log dump	<ul style="list-style-type: none"> ● (Solaris/Linux) \$IMAP_ROOT/var/ThresholdExport/FM ● (Windows) %IMAP_ROOT%\var\ThresholdExport\FM 	<p>Dump file naming rule: The following files are generated in the <Export to>/<YYYYMMDD> directory.</p> <ul style="list-style-type: none"> ● If you select no compression when setting extension parameters, the following files are generated: <ul style="list-style-type: none"> - Alarm log file: YYYYMMDDHHM MSS-alarm-log-auto_(UTF-8)-<number>.xml - Event log file: YYYYMMDDHHM MSS-event-log-auto_(UTF-8)-<number>.xml ● If you select compression when setting extension parameters, the following files are generated: <ul style="list-style-type: none"> - Alarm log file: YYYYMMDDHHM MSS-alarm-log-auto_(UTF-8)-<number>.zip - Event log file: YYYYMMDDHHM MSS-event-log-auto_(UTF-8)-<number>.zip

NOTE

- After the logs are exported, they are not deleted from the database.
- **\$IMAP_ROOT** is the installing path of U2000 for Solaris or SUSE Linux operating system, such as **/opt/oss/server**. **%IMAP_ROOT%** is the installing path of U2000 for Windows operating system, such as **D:\oss\server**.
- Each dump file saves a maximum of 5000 records. If more than 5000 records are dumped, they are dumped to two or more files. The number in the file name continuously increases. Example: **20141125153143-alarm-log-auto_(UTF-8)-1.xml** and **20141125153143-alarm-log-auto_(UTF-8)-2.xml**.

Alarm Synchronization

After communication between the U2000 and an NE recovers from an interruption, or the U2000 is restarted, some alarms on the NE are not reported to the U2000. The NE alarms on the U2000 are different from the actual alarms on the NE. In the case, you need to synchronize alarms. Manual synchronization of alarms ensures that the U2000 displays the current operating status of the NE correctly.

In normal situations, after a device generates an alarm, the alarm is reported to the U2000 within a short period (generally no longer than 10s) and displayed in the alarm list.

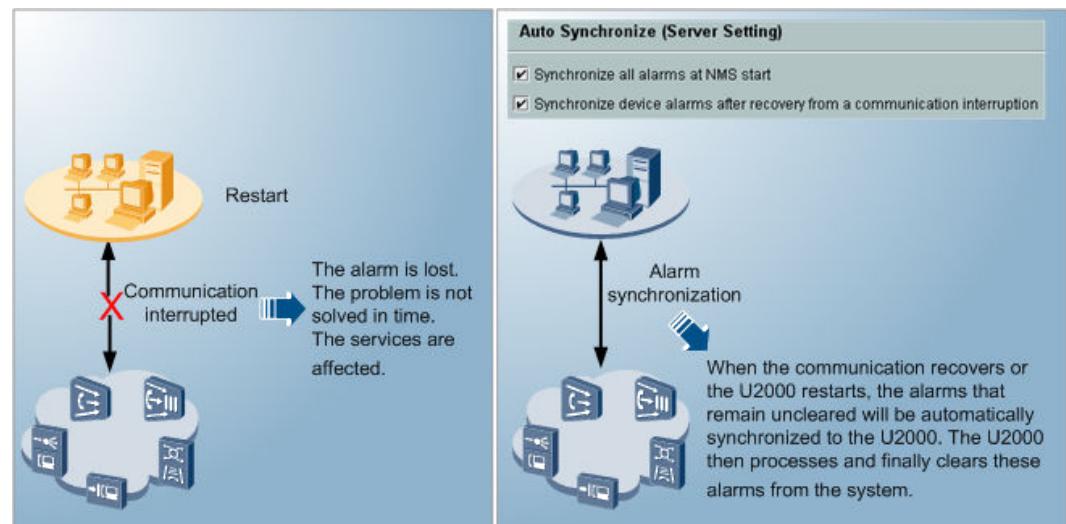
The U2000 can synchronize NE alarms manually or automatically. You can set the policy for automatic alarm synchronization. After you enable automatic alarm synchronization, the U2000 automatically synchronizes alarms to ensure alarm consistency between the U2000 and NEs after communication between the U2000 and NEs recovers or the U2000 is restarted.

Figure 7-16 illustrates the basic concept for alarm synchronization.

Alarms are synchronized according to the following rules:

- If an alarm is cleared from an NE but remains uncleared on the U2000, the alarm will be cleared from the U2000.
- If an alarm is present on an NE but absent from the U2000, the alarm will be added to the U2000.

Figure 7-16 Alarm synchronization



Alarm Redefinition

The U2000 allows you to redefine the alarm severity according to user requirements.

NOTE

Only users in the **Administrators** group can redefine alarm or event names.

This function changes the alarm severity displayed on the U2000 and highlights only the important alarms as defined by user settings.

Alarm/Event Template Management

The U2000 provides the customized alarm/event browsing template and alarm/event attributes template. You can quickly set the alarm/event browsing filter criteria and the alarm/event attributes, by using the preset customized alarm/event template.

Table 7-5 Template type

Type	Description
Alarm/event browsing templates	An alarm/event browsing template is a combination of filter criteria that are used to browse alarm/event information or alarm/event statistics.
Alarm/event attribute template	<ul style="list-style-type: none">● An alarm/event attribute template specifies the alarm severity, automatic alarm/event report, and alarm/event masking of NE alarms or events.● You can use the default alarm/event attribute template or create an alarm/event attribute template according to a particular alarm/event monitoring policy. <p>NOTE</p> <ul style="list-style-type: none">● You are an NMS user with Operator Group authority or higher.● An alarm/event template applies to the MSTP series, WDM series, WDM (NA) series, RTN series, PTN series (except PTN 6900 series) and marine series NEs and CX NEs.

When you create a template, you can set it to be shared. The shared template is visible to all users.

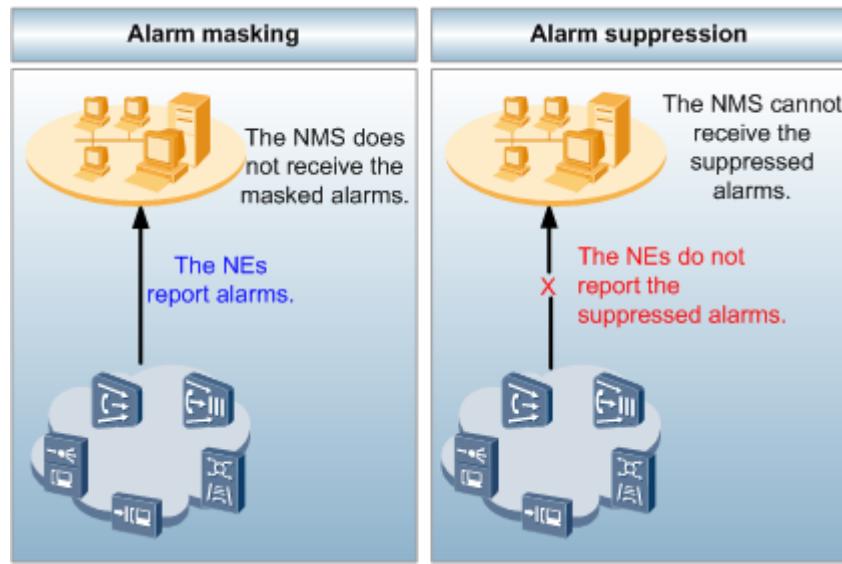
- The users other than Administrators can open only templates created by users themselves and shared by other users. Administrators can open all templates.
- The users other than Administrators can set only the templates created by users themselves to be shared. Administrators can set the templates created by any user to be shared.

Alarm Suppression

The U2000 supports the function of suppressing NE alarms. If you set the status of an alarm to **Suppressed**, the NE does not report the alarm.

The difference between alarm suppression and alarm masking is as follows: If you enable alarm masking, an NE still reports the masked alarm but the U2000 does not receive the alarm. If you enable alarm suppression, the NE does not report the suppressed alarm. For details, see [Figure 7-17](#).

Figure 7-17 Difference between alarm masking and alarm suppression



Alarm Reversion

During a new deployment, certain alarms that are reasonable but useless occur. For example, when you configure a tributary board, line board, or Ethernet board for a service but they are not connected with cables, a LOS alarm is generated. After the alarm reversion is set, the alarm is not displayed. This does not affect the network monitoring task.

The alarm reversion has three modes: non-revertive, manual reversion and automatic reversion. **Table 7-6** shows how alarms are handled in the three modes.

Table 7-6 Alarm reversion handling mode

Reversion Mode	Processing Conditions	Processing Results
Non-revertive	This default mode indicates the normal alarm monitoring status.	None
	When Reversion Mode is set to Non-Revertive for the alarms of an NE.	The U2000 prompts a failure message when you attempt to enable the alarm reversion for a port. This is because the alarm reversion of a port cannot be enabled in the Non-Revertive mode.

Reversion Mode	Processing Conditions	Processing Results
Manual reversion	When Reversion Status of a port is set to Enabled :	The status of the alarms reported from the port immediately changes to the opposite of the actual alarms regardless of the actual alarm status at the port. That is, when there is an alarm at the port, the alarm is not reported. When there is no alarm at the port, the alarm is reported.
	When Reversion Status of a port is set to Disabled :	The status of the alarms reported from the port is consistent with the actual alarm status regardless of the actual alarm status at the port.
Automatic reversion	When Reversion Status of a port is set to Enabled :	<ul style="list-style-type: none"> ● If there is no actual alarm at the port, the setting fails. ● If an actual alarm exists at the port, the setting successfully takes effect as the port becomes in the revertive mode. <p>NOTE When the alarm is cleared, the alarm reversion at the port is automatically stopped. In the automatic reversion mode, the alarm reversion status of a port automatically changes. This may be different from the alarm reversion status displayed on the U2000.</p>
	When Reversion Status of a port is set to Disabled :	The status of the alarms reported from the port is consistent with the actual alarm status regardless of the actual alarm status at the port.

Various Alarm Notification Methods

The U2000 uses a couple of methods to provide alarm notifications. It can notify maintenance engineers of alarms at any time and from anywhere so that they can locate and rectify faults quickly.

The U2000 also supports two remote notification methods: email and short message service (SMS). When a fault occurs on a network, the U2000 notifies non-onsite maintenance engineers of the fault through either of the two configuration methods to help them locate and rectify the fault promptly.

- Different filter criteria can be set to enable the U2000 to notify maintenance engineers of only those important alarms.
- For the alarms that are cleared within a certain period (customizable by the user), the U2000 does not notify maintenance engineers of these alarms because they no longer affect services.

Figure 7-18 shows the alarm notification methods.

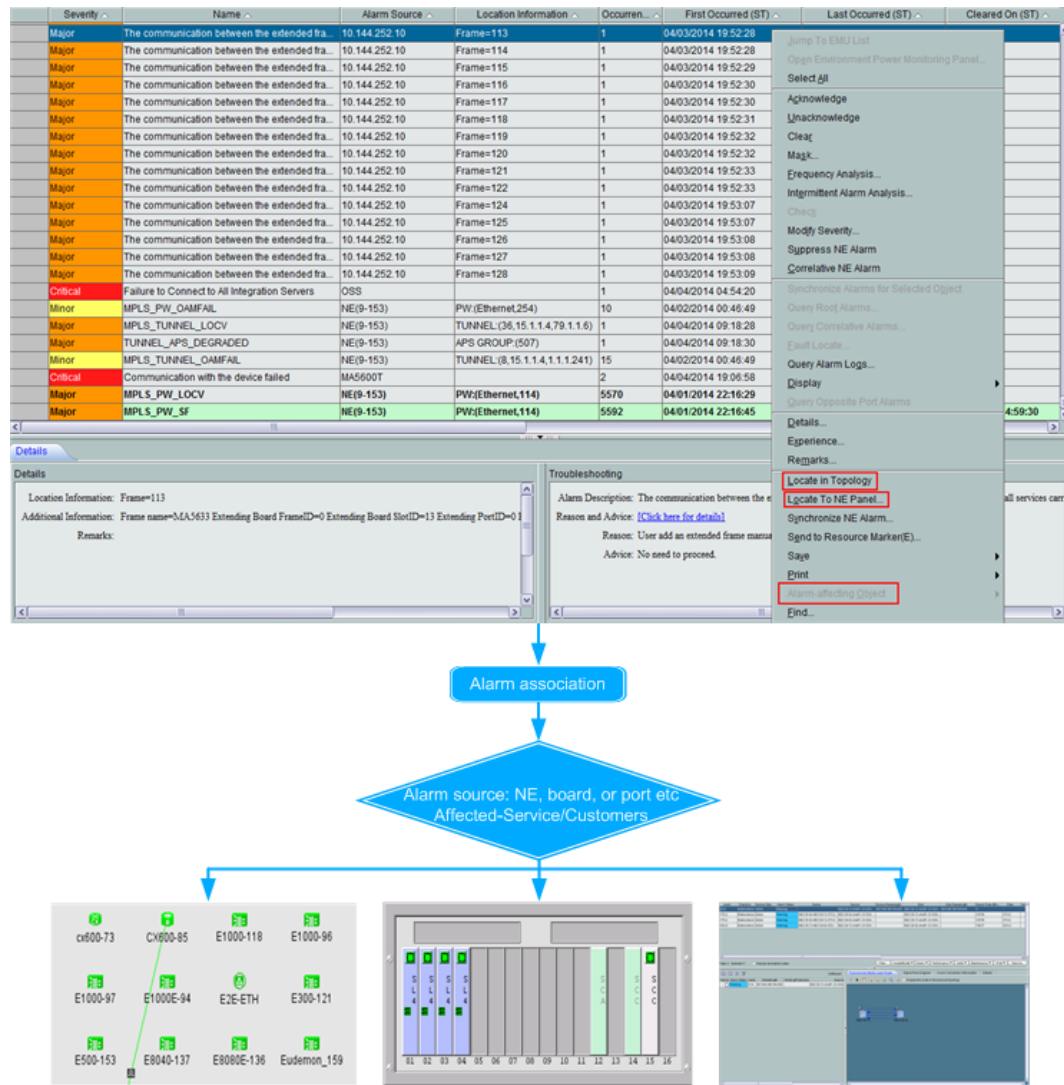
Figure 7-18 Various alarm notification methods



Alarm Association

The U2000 can locate alarms; that is, it can associate alarms with the topological object (NE or NE panel) where the alarms are generated. This function improves fault locating efficiency. Maintenance engineers can quickly locate alarm-affected services from specific equipment alarms. **Figure 7-19** shows the alarm association function.

Figure 7-19 Alarm association



Alarm Maintenance Experience Base

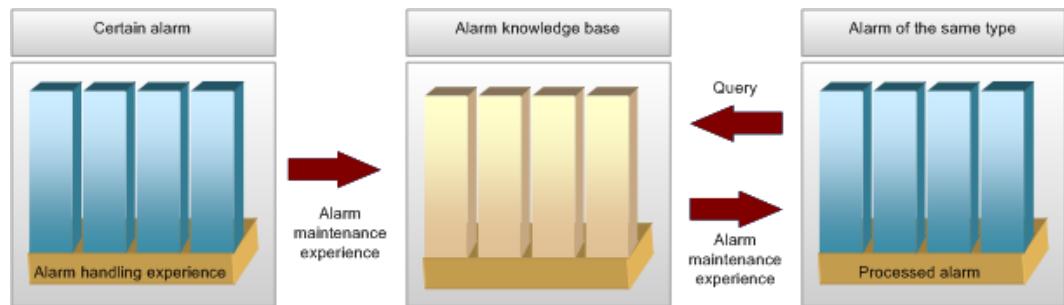
You can obtain information about how alarms were handled from the alarm maintenance experience base. This base is a database that stores alarm details. For details, see [Figure 7-20](#).

Alarm maintenance experience is summarized and recorded on the U2000 by users during maintenance. If a similar fault occurs, relevant alarm handling information is available in the base for reference to achieve efficient alarm handling.

By using the function of importing alarm/event maintenance experience, you can import the methods in which alarms were previously handled to the U2000.

By using the function of exporting alarm/event maintenance experience, you can export the methods in which alarms were previously handled from the U2000 to a file. These practices make it easier to view alarm/event maintenance experience and the information can be shared on other devices.

Figure 7-20 Alarm maintenance experience base



Alarm Time Localization

The NE that reports an alarm and the U2000 may be in different time zones. For the correct alarm generation time, the U2000 automatically converts the alarm generation time (expressed in the NE time) into the U2000 local time.

The U2000 displays the U2000 local time when an alarm is generated, acknowledged, or cleared. The U2000 local time supports two modes: server time and client time.

Alarm Maintenance State

During NE installation, commissioning and tests, alarms may be generated and reported to the U2000. There is no need to process these alarms before the operations are complete. Setting maintenance status to Maintenance helps you identify and filter out alarms in the Maintenance state to locate and fix important alarms more efficiently.

On the U2000, you can set maintenance status for managed objects by adding them to the default construction task or created construction tasks. The Managed objects include NEs, boards, ports and so on. You can also set maintenance status for selected NEs directly in the Main Topology by choosing the shortcut menu, which facilitates operations. After you set the maintenance status of an NE to **Maintenance**,  is displayed on the NE in the Main Topology. Alarms in the maintenance state do not affect the color of involved NEs.

Efficient Offline NE Alarm

The U2000 can detect an NE abnormality (offline or communication fault) within three minutes, display the NE status in the Main Topology, and generate an offline NE alarm.

Alarm or Event Northbound Filtering Rule

The U2000 reports all alarms or events to the upper-layer OSS through the northbound interface. The OSS receives a large number of alarms or events. This causes overload on the upper-layer OSS, resulting in network congestion and breakdown. In addition, users cannot locate their concerned alarms or events rapidly. After an alarm or event northbound filtering rule is set, the U2000 reports only alarms or events that comply with the filtering rule to the upper-layer OSS through the northbound interface. Therefore, load of the upper-layer OSS is reduced, the reported alarms or events are more accurate, and users can focus on concerned alarms or events.

Alarm or event northbound filtering rules are applicable only to alarms or events that are generated after the rules are set. Alarms or events generated before the rules are set cannot be filtered based on the rules. Alarm or event northbound filtering rules take effect for multiple upper-layer OSS.

7.5 Fault Diagnosis

The fault diagnosis tool is used to detect network connectivity and perform troubleshooting for the carrier network.

In addition to hardware faults, the U2000 can diagnose and locate IP network faults, and IP service faults.

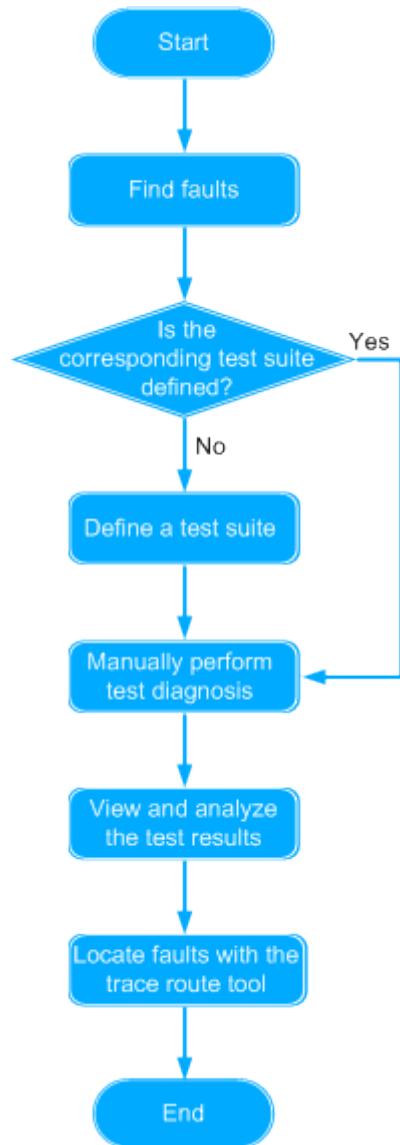
The remote fault diagnosis function of the U2000 reduces costs of on-site maintenance and troubleshooting, and improves troubleshooting efficiency (including effectively identifying the cause and location of the fault).

IP Network Fault Diagnosis

The U2000 provides a test diagnosis tool for diagnosing IP network faults. It can be used to detect the connectivity of multiple services and each network protocol layer, locate faults, and periodically perform tests according to the settings specified in the diagnosis policy. The test diagnosis tool can also test the connectivity of the entire network.

You can use the test diagnosis tool to locate faults during operation and maintenance. [Figure 7-21](#) shows the process of locating faults with the test diagnosis tool.

Figure 7-21 Flowchart of locating IP Network Faults



NOTE

A test suite is a collection of test cases. To define a test suite, create a test suite and add test cases to it. You can define different test suites based on the O scenarios at your site.

The test diagnosis function has the following functions:

- Abundant test methods
 - To accommodate different network layers and service types, the test diagnosis tool provides various test cases, including all applications at various protocol layers that may encounter network faults during O&M. You can create a test suite that contains the desired test cases for a specific scenario. The Trace Route tool can locate faults layer by layer and segment by segment based on the test result.
- Flexible diagnosis policies

These policies allow the U2000 to automatically execute one or more test suites at the interval specified based on the actual O&M scenario, for example, a network-wide connectivity test is performed at 2 a.m. every Sunday.

- Agile network-wide scanning

The scanning checks the network-wide virtual connections, IP links, and Layer 2 links, helping find the faulty links. The faults can be located using the Trace Route tool.

- Intelligent analysis

You can customize a result analysis template based on the service application level. You can specify thresholds for indicators such as the delay, jitter, and packet loss rate and policies for result analysis, helping quickly obtain the network health.

- Detailed historical data

The execution results of all test suites are saved to the **Historical Data** window, facilitating result viewing.

For details about the test diagnosis tool, see [Diagnosis Management](#).

IP Network Troubleshooting

The flexible networking scheme and service paths of a mobile bearer (IPRAN) network make network paths and fault location complicated. The IP network troubleshooting function provides visual search results and smart fault diagnosis for the IPRAN dynamic network, helping engineers to improve the O&M efficiency.

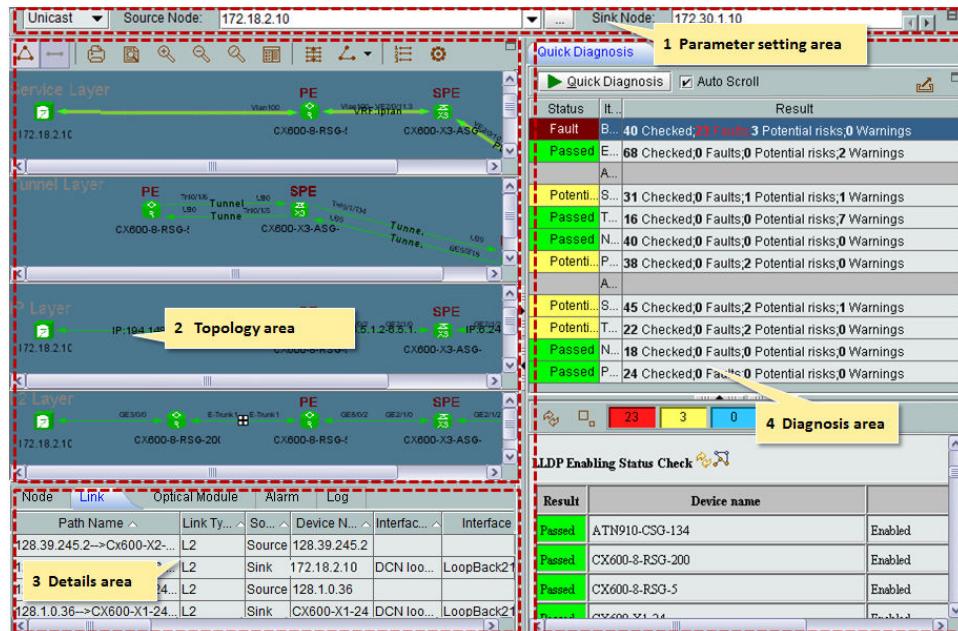
IP network troubleshooting provides the following functions:

- Service path visualization: E2E service paths and backup paths are displayed in the topology. Backup paths support five backup modes: primary/secondary PW, VRRP, E-APS, TE hot standby, and VPN FRR. The paths can be displayed as service-layer, tunnel-layer, IP-layer, and link-layer paths, showing more detailed path information. If a path is incomplete or the current path is a secondary path, a message will be displayed asking you whether to display complete non-backup and historical paths.
- Multicast service path visualization: Shared trees and shortest-path trees of multicast services are displayed in the topology. The service path can be expanded as service layer, IP layer, and link layer.
- Display of NE and link status: After you select an NE or link in the topology, a dialog box is displayed showing the performance data about the NE or the type, source, and destination information about the link. The performance data, alarm information, and optical module information about all NEs and links in the topology are displayed on tabs in the details area to help you with preliminary fault locating.
- Fast fault diagnosis: After you click **Quick Diagnosis**, path and service check items are executed layer by layer in the corresponding networking environments to detect problems. The results about each check item are displayed in a table, the check items with errors detected are marked red, and handling suggestions are provided for troubleshooting. If you click an underscored check result, the associated window in the NE Explorer is displayed helping you rectify the fault quickly.
- Partial fault detection: The packet comparison data, port loopback test, ping test, interface packet loss/error code, TDM PW statistics, path detection, smart ping, and ACL traffic statistics can be used to locate specific fault points.
- Performance Detection (IP FPM): The IP network troubleshooting function supports IP FPM segment-by-segment performance detection on quality deterioration faults. With the IP FPM data collected from NEs, the quality deterioration information, such as the

packet loss ratio, delay, and jitter, about nodes or network segments on a service path is displayed in E2E or segment-by-segment mode.

Figure 7-22 shows the IP Network TroubleShooting window.

Figure 7-22 IP Network TroubleShooting window



For details about the "IP Network Trouble Shooting" function, see [IP Network TroubleShooting](#).

Transport Service Fault Diagnosis

The U2000 provides a test diagnosis tool for diagnosing SDH and WDM path faults in transport domains. Using the service-level alarm analysis function, the U2000 helps to improve the fault response speed and reduce maintenance costs.

The test diagnosis tool can be used in the following scenarios:

- Alarm monitoring

An O&M engineer receives a large number of alarms reported by an NE and needs to determine whether the alarms impact services. The test diagnosis tool helps to locate alarms that impact services and try to find out the root alarm.

- Service monitoring

An O&M engineer finds that the color of an alarm icon changes when monitoring services using the U2000 and needs to determine the alarm impacts on services. The test diagnosis tool helps to locate the root alarm by analyzing path connection status and fault point. If the root alarm cannot be located, the U2000 displays the alarm of a hop on the path, prompting the O&M engineer to use the fault diagnosis function.

TP-Assist Packet Service Fault Diagnosis

The TP-Assist solution has been optimized. For PWE3, VPLS, and native Ethernet services, the U2000 provides an intelligent service fault diagnosis function to quickly locate faults and

provides troubleshooting suggestions. In addition, the U2000 improves the fault locating efficiency of transport packet services and reduces related skill requirements.

The test diagnosis tool can be used in the following scenarios:

- E-Line Service: Native E-Line, PWE3
- E-LAN Service: VPLS, Native E-LAN
- Composite Service: Native E-Line+E-LAN, PWE3+VPLS, Native E-LAN + VPLS + PWE3, PWE3 + static L3VPN

7.6 Performance Management

The performance of a network may deteriorate because of internal or external factors and faults may occur. To achieve good network performance for live networks and future networks while controlling costs, network planning and monitoring are necessary. In addition, network efficiency needs to be measured in terms of the throughput rate, resource usage, and error rate. The performance management function enables you to detect the deteriorating tendency in advance and solve the potential threats so that faults can be prevented. In addition, high-precision (10^{-6}) performance measurement based on service packets is implemented to collect performance indicators, including the packet loss rate, delay, and jitter.

Benefit

NMS provides performance monitoring functions to support performance management at both the NE and network levels. This function is applicable to Access NE, Router/Switch NE and Transfer NE. By creating a performance instance, you can enable the NMS to collect performance data from network devices at specified intervals.

- **Monitoring NE performance.** This function supports the following NE-level performance indicators:
 - CPU usage
 - Memory usage
 - Hard disk usage
- **Monitoring network traffic.** This function is used to collect the traffic statistics of network ports, including:
 - Inbound traffic
 - Outbound traffic.
 - Packet error rate
- **Monitoring SLA data.** This function supports multiple types of SLA data, including:
 - Delay, jitter, and loss ratio of ICMP, TCP, UDP, and SNMP packets
 - Connection delay and download speed of Internet services such as HTTP and FTP
- **Collecting interface-based traffic and performance indicators.** This function supports interface-based traffic in BGP/MPLSVPN, VPLS, and PWE3 services, and performance indicators such as delay, packet loss ratio, and jitter in BGP/MPLS VPN SLA service. Indicator varieties with NE type.
- **Setting performance thresholds.** This function allows you to set thresholds for specific performance indicators. The NMS also provides default global settings for batch configuration. You can set the following parameters:

- Upper and lower thresholds
- Alarm thresholds
- **Maintaining data.** With this function, you can:
 - Store performance statistics
 - Dump performance statistics
 - Regularly compress performance statistics

External Performance Management Capability

The U2000 supports the following performance collection modes:

- Using the SNMP protocol, SNMP performance collection is used for most IP equipment and access equipment.



- NEs must respond to collection requests sent from the U2000 in 0.05s. Otherwise, the actual performance collection capability compromises.
- The performance collection capability listed in the preceding table is based on SNMPv1 and SNMPv2c. The SNMPv3-based performance collection capability achieves only two thirds. For example, on a large-scale network, the performance collection capability for SNMPv1 and SNMPv2c is 150,000, and for SNMPv3 is 100,000 when max/min data aggregation is disabled.
- Using a file transfer protocol supported by equipment, bulk performance collection is used for large-capacity performance management.
- Using Qx which is a proprietary protocol of Huawei, Qx performance collection is used for MSTP, WDM, RTN, PTN and OTN equipment.

For details about collection capability, see [Table 7-7](#).

Table 7-7 Collection capabilities

Network Scale	SNMP Performance Collection Capability (Without Max/Min Data Aggregation Enabled, Max Equivalent Statistics Record/15 Minutes)	SNMP Performance Collection Capability (With Max/Min Data Aggregation Enabled, Max Equivalent Statistics Record/15 Minutes)	BULK Performance Collection Capability (Max Equivalent Statistics Record/15 Minutes)	Qx Performance Collection Capability (Max Equivalent Statistics Record/15 Minutes, U2000 Polling Time/30 minutes)
Small-scale network: less than 500 equivalent NEs	5,000	3,000	<ul style="list-style-type: none">● IP equipment: 16,000● Access equipment: 66,000	5,000

Network Scale	SNMP Performance Collection Capability (Without Max/Min Data Aggregation Enabled, Max Equivalent Statistics Record/15 Minutes)	SNMP Performance Collection Capability (With Max/Min Data Aggregation Enabled, Max Equivalent Statistics Record/15 Minutes)	BULK Performance Collection Capability (Max Equivalent Statistics Record/15 Minutes)	Qx Performance Collection Capability (Max Equivalent Statistics Record/15 Minutes, U2000 Polling Time/30 minutes)
Common-scale network: 500-2000 equivalent NEs	20,000	13,000	<ul style="list-style-type: none"> ● IP equipment: 66,000 ● Access equipment: 266,000 	20,000
Medium-scale network: 2000-6000 equivalent NEs	60,000	40,000	<ul style="list-style-type: none"> ● IP equipment: 200,000 ● Access equipment: 800,000 	40,000
Large-scale network: 6000-15000 equivalent NEs	150,000	100,000	<ul style="list-style-type: none"> ● IP equipment: 500,000 ● Access equipment: 2,000,000 	80,000
Super-large-scale network: 15000-30000 equivalent NEs	150,000	100,000	<ul style="list-style-type: none"> ● IP equipment: 500,000 ● Access equipment: 2,000,000 	100,000

 **NOTE**

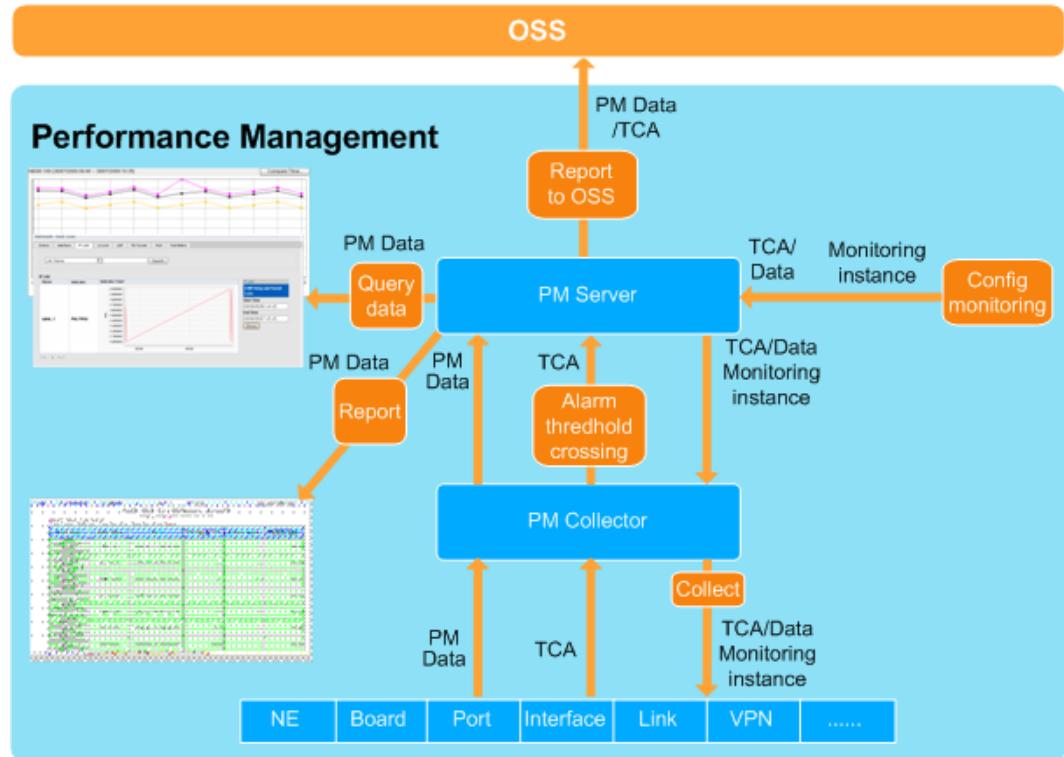
For details about the hardware platforms available for the U2000, see [11.3 Management Capabilities of Standard Delivery Models](#) and [11.4 Management Capabilities of Compatible Models](#).

An equivalent statistics record is a basic unit to describe the performance management capability of the PMS. [Figure 7-24](#) shows the relationship between the equivalent statistics records and instances.

Performance Management Process

The U2000 uses a graphical user interface (GUI) to monitor key network indicators and display statistics on the collected performance data.

Figure 7-23 Performance management process



The following is a function description of performance management modules.

Performance Monitoring Policy Settings

You can perform the following operations on the U2000:

- Customize the performance threshold template. Specifically, you can customize a maximum of 16 performance threshold templates in addition to the default performance threshold template.
- Select the performance threshold template for an NE and set the performance thresholds.
- Customize the RMON performance attribute template.
- Set the performance thresholds for a specified board.
- Set the start and end time for monitoring NE performance.
- Set whether to prompt unavailable time (UAT) and threshold-crossing events in a timely manner.
- Set the start and end time for monitoring Ethernet performance.
- Set the monitoring status of Ethernet performance events.
- Set the ATM performance monitoring time.

- Set the ATM performance monitoring period.
- Set the monitoring status of ATM performance events.
- Set the real-time ATM performance monitoring.
- Set performance thresholds based on ports or channels.

SDH Performance Monitoring

You can perform the following operations on the U2000:

- View the SDH current 15-minute and 24-hour performance data, historical 15-minute and 24-hour performance data, UAT, and 15-minute and 24-hour threshold-crossing events.
- Monitor the performance of ATM ports in real time, and view the historical performance data of ATM ports.
- Monitor the performance of ATM VPs and VCs in real time, and view the historical performance data of ATM VPs and VCs.
- Monitor the performance of Ethernet ports in real time, and view the historical performance data of Ethernet ports.
- View the Ethernet performance data in charts or tables.
- Monitor the Ethernet RMON performance.
- Manage lower-order performance of boards.

WDM Performance Monitoring

You can perform the following operations on the U2000:

- View the WDM current 15-minute and 24-hour performance data, historical 15-minute and 24-hour performance data, UAT, and 15-minute and 24-hour threshold-crossing events.
- Monitor the performance of Ethernet ports in real time, and view the historical performance data of Ethernet ports.
- View the Ethernet performance data in charts or tables.
- Monitor the Ethernet RMON performance.

RTN Performance Monitoring

You can perform the following operations on the U2000:

- View the RTN current 15-minute and 24-hour performance data, historical 15-minute and 24-hour performance data, UAT, and 15-minute and 24-hour threshold-crossing events.
- Monitor the performance of Ethernet ports in real time, and view the historical performance data of Ethernet ports.
- View the Ethernet performance data in tables.
- Monitor the Ethernet RMON performance.

PTN Performance Monitoring

You can perform the following operations on the U2000:

- View the performance of a specified Ethernet service.
- View the performance of a specified pseudo wire (PW).
- View the performance of a specified ML PPP.
- View the performance of a specified tunnel.
- View the performance of a specified circuit emulation service (CES).
- View the performance of specified quality of service (QoS).
- View the performance of specified PW OAM.
- View the performance of specified MPLS OAM.
- View the performance of specified Ethernet OAM.
- View the performance of a specified ATM PWE3 service.
- View the performance of a specified layer 2 virtual private network (L2VPN) service.
- View the performance of a specified ATM IMA service.
- View the performance of a specified SDH-like service.
- View the performance of a specified regenerator section, multiplex section, and higher-order path.
- View the performance of a specified lower-order path.
- View the performance of a specified E1.
- View the performance of a specified laser.
- View the performance of a specified management layer.
- Monitor the Ethernet RMON performance.
- Reset the performance register on a board.

Performance Data Dumping

The performance data saving time varies based on the collection period. If the collection period is 5 minutes, 10 minutes, or 30 minutes, only the performance data generated within the latest one day is saved by default. If the collection period is one hour or one day, only the performance data generated within the latest 8 days or the latest 30 days is saved by default.

You can save the performance data to a file automatically or manually.

The conditions for an immediate dump must be set for a manual dump.

The following items must be set for an automatic dump:

- Conditions for an overflow dump
- Conditions for a periodic dump
- Dump location

Performance Data Analysis

- Analyze historical performance data.
- Forecast long-term performance and medium-term performance according to the empirical formula that is created based on the historical performance data of the optical transceiver.
 - If the performance data is available, the time for generating the performance and the deviation range can be calculated.

- If the time is available, the performance data at that time and the deviation range can be calculated.

Performance Register Resetting

- Reset the board performance register.
- Reset the ATM performance register.
- Reset the Ethernet performance register.

Performance Monitoring Template Management

Performance monitoring template: a collection of performance indicators. The indicators are included in various indicator groups. You can manage a performance monitoring task easily by setting this type of template.

There are different types of performance monitoring templates. Some of the template may contain indicators and indicator groups for collecting performance data of network resources. Some of the template monitor data and threshold of the specified resources.

Template-Based SLA Parameters

This function collects most SLA parameters into templates. In this manner, you do not need to create SLA parameters when creating an instance, which improves operation efficiency.

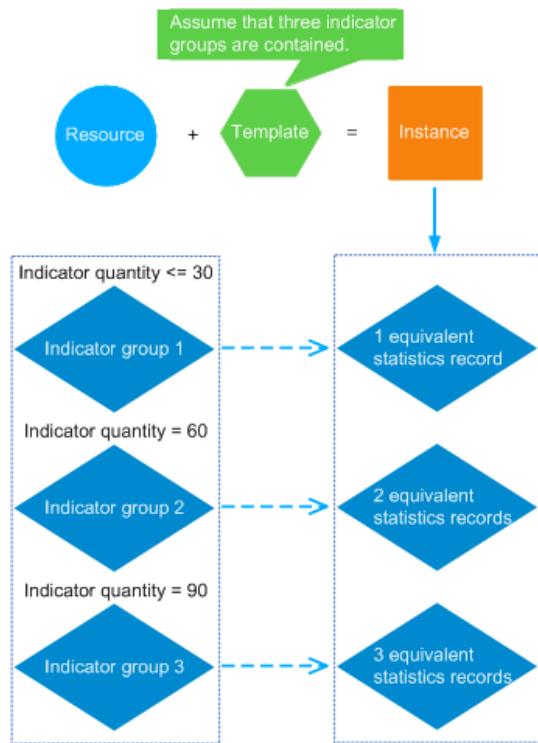
Monitoring Instance Management

Instance: An instance consists of a resource and a template. By means of an instance, you can collect data of certain resource performance indicators. A template can contain multiple indicator groups. [Figure 7-24](#) shows the relationship between the templates, instances, indicator groups, and equivalent statistics records.

NOTE

- Resource: A model of telecom resource such as device, card, port, or link in the performance management domain. A resource can be either physical or logical entity. Logical resources contain the physical resources. A resource has associated indicators that capture performance data values. A performance monitoring system collects values of these indicators for a resource.
- Template: A collection of indicators which exhibit in the form of indicator group. You can configure template to manage the performance monitoring task easily.
- Indicator group: During performance measurement, the indicator group specifies what to be measured. Each indicator group consists of one or more indicators with similar properties.
- Instance: A performance indicator is associated with a resource. It gives the measure of performance aspect of monitored resource, for example, traffic, availability, central processing unit (CPU) usage, and so on. It is calculated from the performance data collected from the monitored resource. A performance indicator has properties, such as the data type, precision value (only for float), maximum value, and minimum value.

Figure 7-24 Relationships between a template, an instance, and a task



- An indicator group that contains no more than 30 indicators equals an equivalent statistics record.
- For an indicator group with over 30 indicators, the conversion algorithm is as follows:
Number of indicators/30
If the remainder is less than 15, the remainder equals 0.5 equivalent record. Total number of equivalent records = Integer of (number of indicators/30) + 0.5
If the remainder is greater than or equal to 15, the remainder equals 1 equivalent record. Total number of equivalent records = Integer of (number of indicators/30) + 1
For example, if an indicator group has 32 indicators, the integer of (number of indicators/30) is 1 and the remainder is 2. The total number of equivalent records is 1.5.

Monitoring instances enable you to collect performance statistics on resources of specified equipment according to a preset monitoring template and schedule policy. One monitoring instance collects statistics on only one resource. You can perform the following operations on the U2000:

- Create monitoring instances for resources, such as NEs, boards, ports, and links, and for the IP SLA of the PTN and third-party equipment.
- Modify monitoring instances.
- Query monitoring instances.
- Delete monitoring instances.
- Suspend monitoring instances.
- Resume monitoring instances.
- Synchronize resources corresponding to monitoring instances.
- Query threshold.
- Query the VPN SLA test result.

- Control the management capability; that is, control the number of monitoring instances that can be created by a license.
- Exporting the instance information.
- Counting the number of instance.
- Displaying the KPI.

Schedule Policy Management

The schedule policy enables you to set the time segments and periods at which the data is collected. The schedule policy can be applied to resources when a monitoring instance is created or modified.

Viewing Historical Performance Data

You can collect the network performance data within a specified period and ascertain the network performance. Historical performance data provides reference data for predicting a change in performance of a network.

The U2000 can query performance data based on parameters, such as the NE name, time, and performance data type. Currently, the period of 5-minute, 10-minute, 15-minute, 30-minute, 1-hour and 1-day historical performance data can be queried. You can view the historical performance data of a network in a graph, bar chart, or table, and save the performance data in file formats of CSV, HTML, PDF, TXT XML and PNG.

In addition, you can compare the performance data from different periods in a graph or bar chart or compare the indicators of different resources in the same diagram.

You can view the historical performance in single resource or in multiple resource.

Viewing Real-Time Performance Data

You can view real-time performance data in a table, graph, or bar chart, and save the performance data in file formats of CSV, HTML, PDF, TXT, and XML.

You can set display mode as line, column, table.

Data Lifecycle Management

You can back up performance data to a specified storage medium manually or automatically when excessive performance data is saved in the database of the U2000.

Data can be dumped in the following two ways:

- **Automatic Dumping:** Performance data is dumped automatically based on preset parameters, such as specific periods of time (days) and database usage.
- **Manual Dumping:** Performance data is dumped based on the user-defined conditions, such as file type and end date.

Monitoring Network Performance

You can view the performance data of NEs, interfaces, IP links, L2 links, static, tunnels, dynamic tunnels, and test cases on the same network by network grouping. In addition, you can perform various tests on a network, such as tests for UDP jitter and FTP ping, to evaluate the quality of networks and services and analyze the correlation between the quality of networks and services.

- Create a network group.
Associate the monitoring instances of resources of different types within the same network according to the customized grouping rules, such as an area-based rule or service-based rule. Then, you can browse and compare data easily.
- Analyze interface performance trends.
After the network interface indicators are set, a performance trend analysis graph for either the current time, or 12 hours before the current time can be generated. The performance trend analysis graph helps you quickly understand the general interface performance trends.
- View the results of network monitoring test cases.
You can view the results of network monitoring test cases. In this manner, you can obtain the information about network-related indicators, evaluate network performance, and analyze the correlation between the indicators and network performance.

TCA Threshold Setting

U2000 supports to set thresholds for performance, the U2000 uses TCA monitoring template to configure the thresholds. TCA monitoring template is a collection of indicators with specified thresholds. You can configure a TCA monitoring template for specified resources to monitor the TCAs of the resources. The U2000 generates a TCA when the performance data exceeds the defined threshold in the TCA monitoring template.

DB Size Calculator

The U2000 can predict the database size. Specifically, the U2000 calculates the required database space based on the number of collection instances (number of interface resources), collection period, life cycle and the number of indicators of each instance. In addition, the U2000 can calculate the performance data life cycle based on the number of collection instances (number of interface resources), collection period, number of indicators of each instance and available database space.

7.7 Inventory Management

The U2000 supports unified inventory management of physical and service resources on the entire network. The U2000 provides clear and easily-accessible information to users so that they can acquire an accurate and complete understanding of the network-wide resources. The inventory information serves as a reference for service and expansion planning.

- You can perform the following operations on the U2000:
 - Maintain inventory information
 - Query inventory information
 - Collect inventory statistics
 - Save inventory information to XLS, TXT, HTML, or CSV files
 - Print inventory information

 **NOTE**

The supported file format may vary with inventory information.

- The U2000 supports auto-discovery of a new asset (such as a new device, board, etc). If an existing asset is updated, an NE icon will remind you of that the data on the U2000 is

asynchronous with the data on the NE. With the U2000, you can quickly identify the causes of data synchronization.

- The U2000 can be used to export inventory reports, including information about NEs, boards, subboards, ports, subracks, and the optical/electrical module.

 **NOTE**

- The optical/electrical module supports only the MSTP series, WDM series, WDM (NA) series, RTN series, PTN series, Router series and Switch series NEs.
- Inventory reports of the optical/electrical module in the MSTP series, WDM series, WDM (NA) series, RTN series and PTN series (except PTN 6900 series) NEs can be exported.
- Inventory reports of the optical/electrical module in the Router series and Switch series NEs cannot be exported.

Figure 7-25 shows the inventory management window of the U2000.

Figure 7-25 Inventory management window and its functions

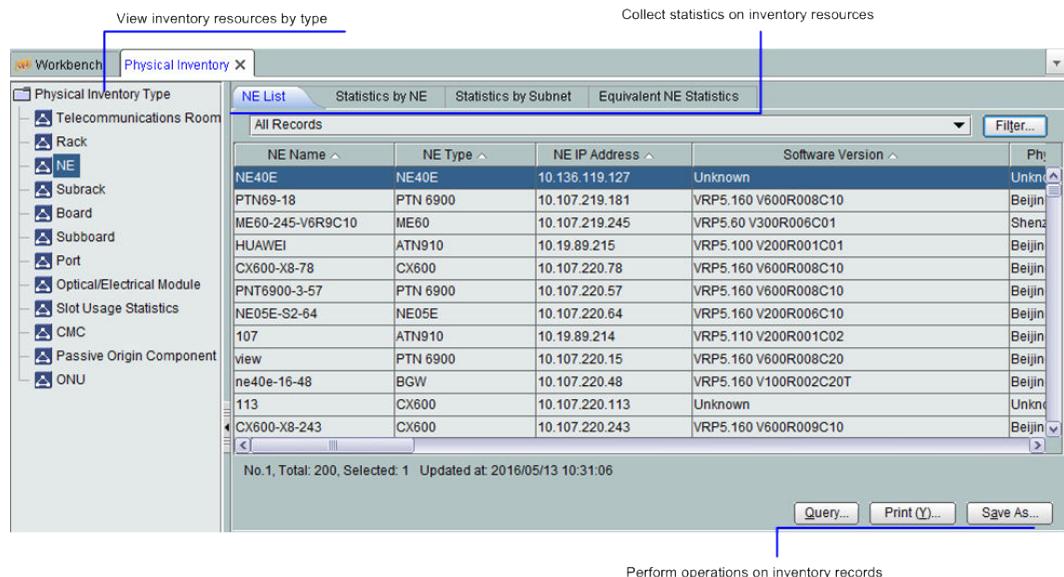


Table 7-8 Statistical items for resource inventory management

Resource	Statistical Item
Telecommunications Room	Telecommunications Room Name, Station, Country, Province, City, Location, Room Number, Cabling Mode, Antistatic Floor, Thickness of the Antistatic Floor (mm), Remark, and Customized Column.
Rack	Rack Name, Telecommunications Room, Rack Type, Number of Shelves, Height (mm), Width (mm), Depth (mm), Power Box Type, Voltage, Number of Batteries, Internal Battery, Internal Power Supply, Internal MDF, Internal Transmission, Remark, and Customized Column.
Subrack	Subrack Name, Subrack Type, NE, Subrack ID, Software Version, Alias, Subrack Status, Telecommunications Room, Rack, Subrack No., Subnet, Subnet Path, Equipment No., Remark, and Customized Column.

Resource	Statistical Item
NE	NE Name, NE Type, NE IP Address, NE MAC Address, NE ID, Software Version, Physical Location, Create Time, Fiber/Cable Count, Run Status, Subnet, Subnet Path, Alias, Remark, Patch Version List, Customized Column, LSR ID, Maintenance Status, Gateway Type, Gateway, Optical NE, Subrack Type, Conference Call, Orderwire Phone, and NE Subtype.
Board	Board Name, Board Type, NE, NE Type, Subrack ID, Slot ID, Hardware Version, Software Version, Serial Number, Alias, Remark, Customized Column, Subrack Type, NE ID, Board Bar Code, BIOS Version, FPGA Version, Board Status, Board BOM Item, Management, Produce Date, Manufacture Date, and Create Time.
Subboard	Subboard Name, Subboard Type, Subrack ID, Slot Number, Subslot Number, Subboard Status, NE, Hardware Version, Software Version, Serial Number, Alias, Subboard Description, Remark, Customized Column, Subboard BOM Item, Subboard Produce Date, and Subborad Bar Code.
Port	NE Name, NE Type, Shelf No., Slot No., SubSlot No., Port No., Port Name, Port Type, Port Rate, Port Level, Management, Alias, Remark, and Customized Column.
Optical/ Electrical Module	SFP Information: Port, SFP Type, Fiber/Cable Type, Logical Type, Physical Type, Serial Number, CLEI Code, BOM Code, Manufacturer, Date of Manufacture, User Label, Description, and User-defined Info. Router and Switch Optical/Electrical Module: Serial No., Optical/Electrical Type, NE Name, Port Name, Port Description, Port Type, Receive Optical Power, Reference Receive Optical Power, Reference Receive Time, Receive Status, Upper Threshold for Receive Optical Power, Lower Threshold for Receive Optical Power, Transmit Optical Power, Reference Transmit Optical Power, Reference Transmit Time, Transmit Status, Upper Threshold for Transmit Optical Power, Lower Threshold for Transmit Optical Power, SingleMode/MultiMode, Speed, Wave Length, Transmission Distance, Fiber Type, Manufacturer, Optical Mode Authentication, Port Remark, Port Custom Column, OpticalDirection Type.
Slot Used Statistics	NE Name, NE Type, Total Slot Count, Used Slot Count, Vacant Slot Count, Slot Usage %.
CMC	CMC Name, Alias, OLT Name, Extending Port, Type, Status, Networking Mode, SN, Hardware Capability, CMC IP, OLT IP, and Note.
ONU	Terminal Type, ONU Version, Amount, Type.
Fiber/Cable/ Microwave Link	Name, Level/Capacity, Rate (bit/s), Direction, Source NE, Source Port, Sink NE, Sink Port, Length, Designed Loss(EOL), Fiber/Cable Type, Medium Type, Created on, Creator, Maintainer, Remarks, Alarm Severity, Disabled Status, Alarm Generation Time, and Maintain State.

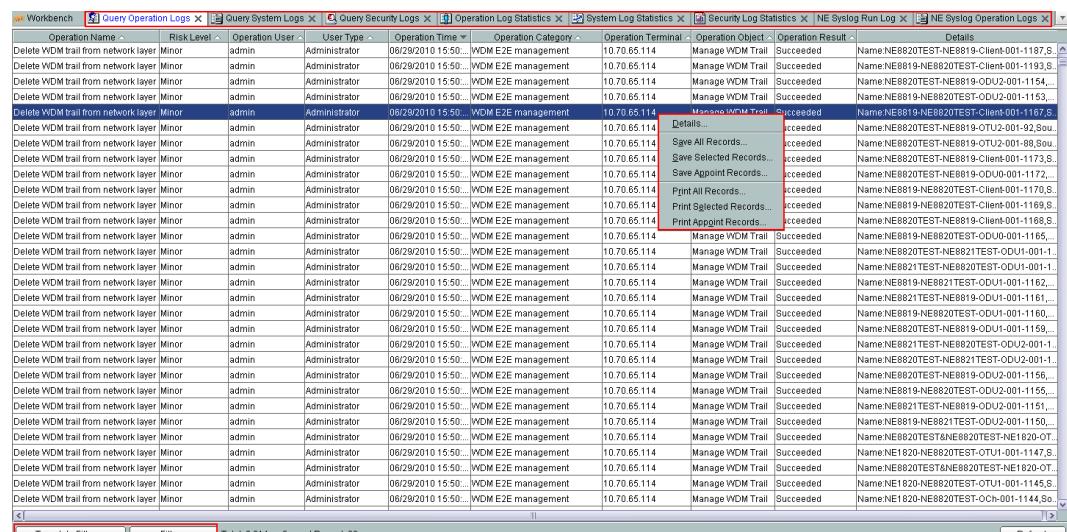
Resource	Statistical Item
Link	<p>Alarm Severity, Link Name, Link Type, Network Protocol Type, Source NE, Source IP, Source Port, Source Port IP, Source Port Alias, Sink NE, Sink IP, Sink Port, Sink Port IP, Sink Port Alias, Link Level, Link Rate (bit/s), Remaining Upstream Bandwidth (Kbit/s), Remaining Downstream Bandwidth (Kbit/s), Build Time, Remarks, User Label, Owner, weight(1-1000).</p> <p>NOTE Including Virtual Link, L2 link, IP Link.</p>
Router/Switch Interface	<p>Interface Name, NE Name, Description, IPv4 Address, IPv6 Address, MAC Address, Interface Type, Rate, Administrative Status, IPv4 Operating Status, IPv6 Enable Status, IPv6 Operating Status, Remarks and MTU.</p>

7.8 Log Management

Logs are used to record the information about operations that were performed and important events that occurred on the U2000. The U2000 allows administrators to query and save logs and collect statistics on logs periodically. This action facilitates fault analysis and detection of unauthorized logins and operations. Specifically, by browsing and collecting statistics on logs, you can query the client from which a user logged in to the U2000 server and query the operations performed by the user after login. You can also dump and print logs. Logs also can record operations that the OSS performed on NEs through NBIs.

Figure 7-26 shows the log management window and functions of the U2000.

Figure 7-26 Log management window and functions



Log Classification

The logs of the U2000 are classified into operation logs, system logs, security logs, and NE logs. The logs can be saved to TXT, HTML, CSV, PDF, XLSX, and XLS files.

- Operation logs record the non-security-related operations that users performed, such as creating a subnet and enabling or disabling the alarm sound.
- System logs record the operations that the U2000 automatically performed, such as scheduled tasks and system tasks.
- Security logs record the security-related operations that users performed, such as login, logout, lockout, and unlocking.
- NE Syslog operation logs record the operation results of managed NEs. You can acquire the NE operation logs from the U2000 client instead of having to do so from each NE. This function is applicable to access OLT, MDU, MSAN, and DSLAM series NEs.
- NE Syslog running logs record the running information of NEs managed by the U2000. The U2000 obtains all Syslog running logs from NEs. Therefore, you can acquire the Syslog running logs of the managed NEs from the U2000 instead of having to do so from each NE. This function is applicable to routers, switches, and service gateway NEs.
- NE security log: NE security logs record security-based operations that all NE users perform on an NE. You can view the NE security logs on the U2000, rather than viewing them on each NE. The U2000 allows users to browse security logs of transport NEs.

The logs of the U2000 includes the following parameters, see [Table 7-9](#).

Table 7-9 The parameters of the logs

Type	Parameter
Operation Log	RecordID, User, User Type, Terminal, Start Time, Category, Operation, Operation Object, Result, Details, End Time
System Log	RecordID, Level, Source, Time, Result, Basic Information, Detailed Information
Security Log	RecordID, User, User Type, Event Level, Terminal, Start Time, EventType , Security Event, Operation, Object, Result, Details, End Time
NE Syslog Operation Log	Device name, Time, User Name, Access Method, IP Address, User Command, User Command Details
NE Syslog Run Log	<ul style="list-style-type: none">● Parameters for multi-file query logs: NE Name, NE Alias, IP Address, User Name, User IP Address, Details, Time Sent● Parameters for single-file query logs: NE Name, IP Address, Digest, Details, Module Name, Level, Time Sent

Type	Parameter
NE Security Log	NE, User Name, Event Name, Resource Name, Operation Time, Operation Result

Querying and Collecting Statistics on Logs

U2000 administrators can set filter criteria to sort logs by operation user, operation terminal, operation result, risk level, operation time, operation name, operation object, or a combination of all of the preceding items. The administrators can learn about the operations performed on the U2000 by the current user.

Forwarding Logs

- U2000 log forwarding: The U2000 can forward its operation logs to the Syslog server to save the operation information, which releases storage space on the U2000 server. The logs serve as a reference for maintenance.
- NE log forwarding: The U2000 can forward the information about various NEs to the Syslog server in the format that complies with the system log protocol. The U2000 administrators and maintenance personnel can view the status of NEs according to the importance of the NE information. This function is applicable to SDH, Marine and WDM NEs.

Dumping and Exporting Logs

The log dumping function enables you to delete the logs that are no longer needed, automatically at a scheduled time, or manually. This function prevents logs from occupying too much space. The log exporting function enables you to export logs to a file for viewing or fault locating. The functions for dumping and exporting logs in the **Task Management** window on the U2000 server are highlighted in [Figure 7-27](#). [Figure 7-28](#) illustrates the log dump process.

Figure 7-27 Functions for dumping and exporting logs in the **Task Management** window

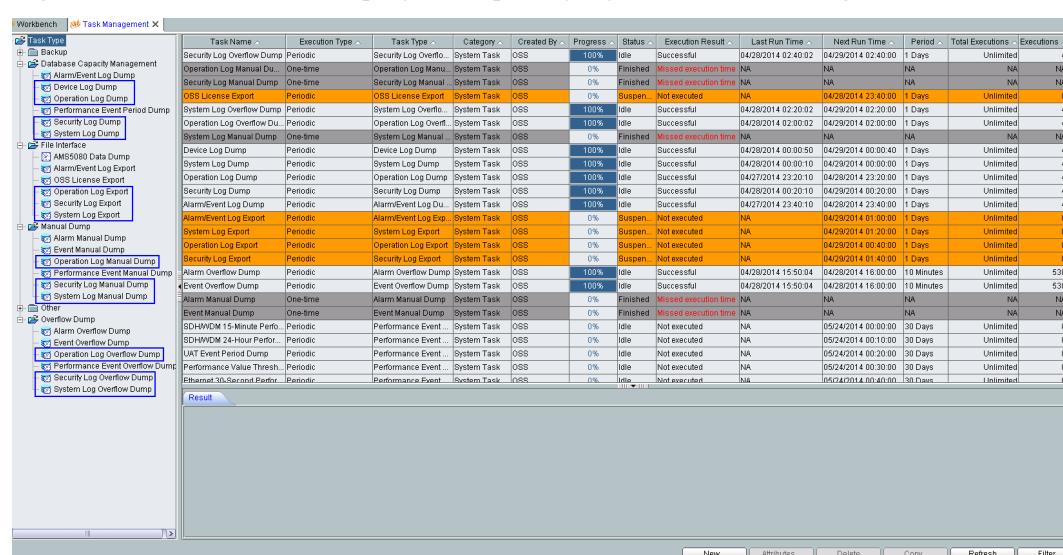
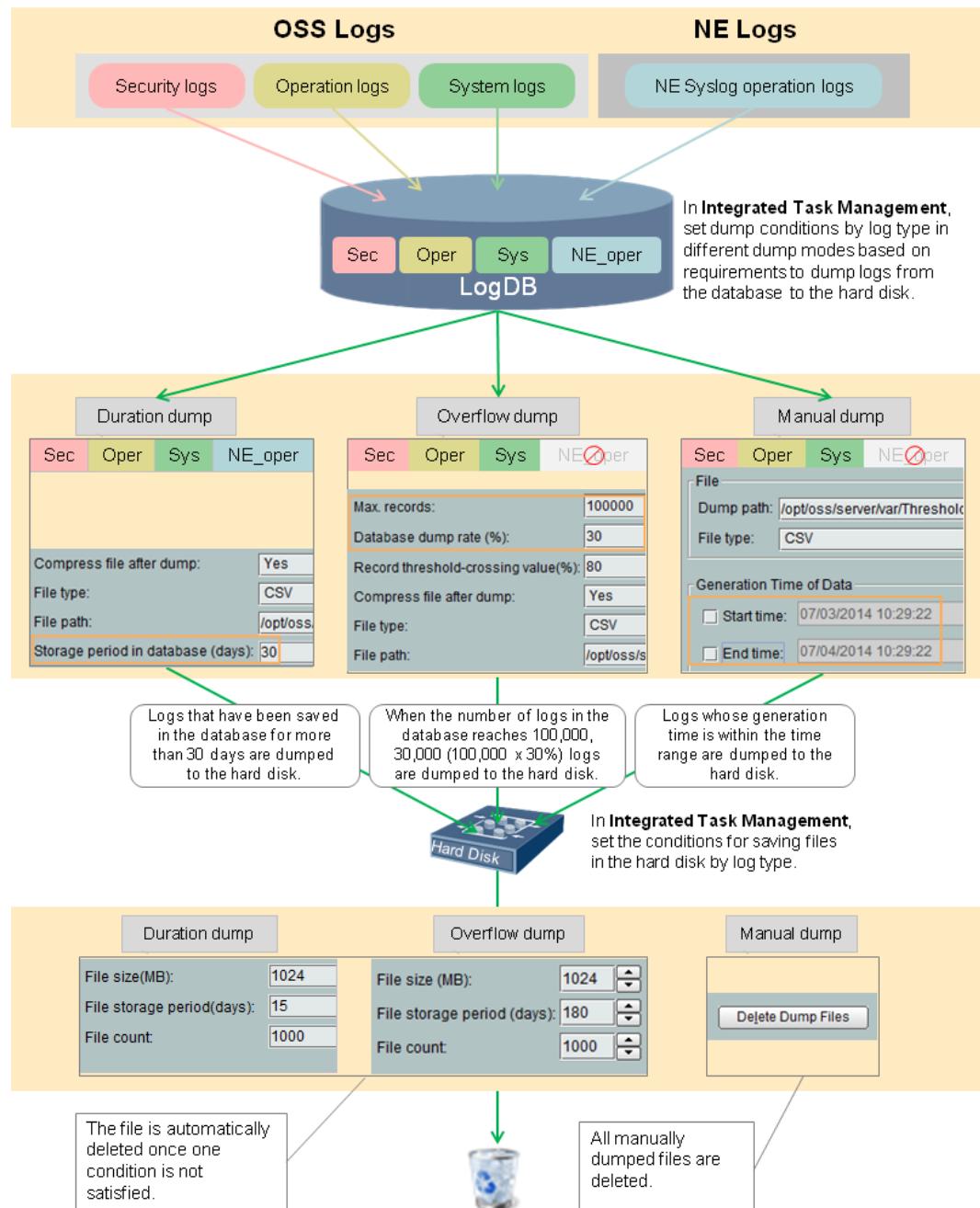


Figure 7-28 Log dump process



Task Type	Task Name	Default Path for Saving Dump/Export File	Rules for Naming Dumped/Exported Files
Database Capacity Management/Overflow Dump	Security Log Dump	<ul style="list-style-type: none"> OSS server running the Solaris or SUSE Linux operating system: \$IMAP_ROOT/var/ThresholdExport/Log/YYYYMMDD 	<ul style="list-style-type: none"> YYYYMMDDHHMMSS-security-log-dateThreshold_info.xml YYYYMMDDHHMMSS-security-log-dateThreshold(UTF-8)-<number>.zip
	Operation Log Dump	<ul style="list-style-type: none"> OSS server running the Windows operating system: %IMAP_ROOT%\var\ThresholdExport\Log\YYYYMMDD 	<ul style="list-style-type: none"> YYYYMMDDHHMMSS-operation-log-dateThreshold_info.xml YYYYMMDDHHMMSS-operation-log-dateThreshold(UTF-8)-<number>.zip
	System Log Dump		<ul style="list-style-type: none"> YYYYMMDDHHMMSS-system-log-dateThreshold_info.xml YYYYMMDDHHMMSS-system-log-dateThreshold(UTF-8)-<number>.zip
Device Log Dump		<ul style="list-style-type: none"> OSS server running the Solaris or SUSE Linux operating system: \$IMAP_ROOT/var/ThresholdExport/Dol/YYYYMMDD OSS server running the Windows operating system: %IMAP_ROOT%\var\ThresholdExport\Dos\YYYYMMDD 	<ul style="list-style-type: none"> DevLogTimerDumpYYYYMMDDHHMMSS-01-<number>.zip DevLogTimerDumpYYYYMMDDHHMMSS-01_(UTF-8)-<number>.zip
Manual Dump	Security Log Manual Dump	<ul style="list-style-type: none"> OSS server running the Solaris or SUSE Linux operating system: \$IMAP_ROOT/var/ThresholdExport/Log/YYYYMMDD OSS server running the Windows operating system: %IMAP_ROOT%\var\ThresholdExport\Log\YYYYMMDD 	<ul style="list-style-type: none"> YYYYMMDDHHMMSS-security-log-manual_info.xml YYYYMMDDHHMMSS-security-log-manual(UTF-8)-<number>.zip

Task Type	Task Name	Default Path for Saving Dump/Export File	Rules for Naming Dumped/Exported Files
	Operation Log Manual Dump		<ul style="list-style-type: none"> ● YYYYMMDDHHMMSS-operation-log-manual_info.xml ● YYYYMMDDHHMMSS-operation-log-manual(UTF-8)-<number>.zip
	System Log Manual Dump		<ul style="list-style-type: none"> ● YYYYMMDDHHMMSS-system-log-manual_info.xml ● YYYYMMDDHHMMSS-system-log-manual(UTF-8)-<number>.zip
File Interface	Security Log Export	<ul style="list-style-type: none"> ● OSS server running the Solaris or SUSE Linux operating system: \$IMAP_ROOT/var/fileint/seculogs/YYYYMMDD ● OSS server running the Windows operating system: %IMAP_ROOT%\var\fileint\seculogs\YYYYMMDD 	<ul style="list-style-type: none"> ● YYYYMMDDHHMMSS-security-log-conditional_info.xml ● YYYYMMDDHHMMSS-security-log-conditional(UTF-8)-<number>.zip
	Operation Log Export	<ul style="list-style-type: none"> ● OSS server running the Solaris or SUSE Linux operating system: \$IMAP_ROOT/var/fileint/userlogs/YYYYMMDD ● OSS server running the Windows operating system: %IMAP_ROOT%\var\fileint\userlogs\YYYYMMDD 	<ul style="list-style-type: none"> ● YYYYMMDDHHMMSS-operation-log-conditional_info.xml ● YYYYMMDDHHMMSS-operation-log-conditional(UTF-8)-<number>.zip

Task Type	Task Name	Default Path for Saving Dump/Export File	Rules for Naming Dumped/Exported Files
	System Log Export	<ul style="list-style-type: none">OSS server running the Solaris or SUSE Linux operating system: \$IMAP_ROOT/var/fileint/syslogs/YYYYMMDDOSS server running the Windows operating system: %IMAP_ROOT%\var\fileint\syslogs\YYYYMMDD	<ul style="list-style-type: none">YYYYMMDDHHMMSS-system-log-conditional_info.xmlYYYYMMDDHHMMSS-system-log-conditional(UTF-8)-<number>.zip

 **NOTE**

- After the logs are exported, they are not deleted from the database.
- \$IMAP_ROOT** is the installing path of U2000 for Solaris or SUSE Linux operating system, such as **/opt/oss/server**. **%IMAP_ROOT%** is the installing path of U2000 for Windows operating system, such as **D:\oss\server**.
- If each file contains more than 5000 rows, the **.zip** file is split into two or more files. <number> in the file name continuously increases. Examples: **20140321144204-operation-log-dateThreshold(UTF-8)-1.zip** and **20140321144204-operation-log-dateThreshold(UTF-8)-2.zip**.
- Logs can be dumped/exported to a CSV, XML, TXT, or HTML file and then are compressed to a .zip package.

7.9 Database Management

Database management includes managing NE databases and U2000 databases, and maintaining data consistency between the U2000 and NEs.

NOTICE

The user information (including phone numbers and addresses) on the U2000 and all user names and passwords are also backed up. Backup data of the U2000 may use personal information of users. Therefore, you are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the personal data of users is fully protected.

NE Database Management

To ensure NE data security, the U2000 can back up and restore NE data.

In NE software management, you can back up and restore NE data on a server, including:

- Backing up the NE database to a local or remote server manually or automatically.
- Restoring the NE database from a local or remote server.

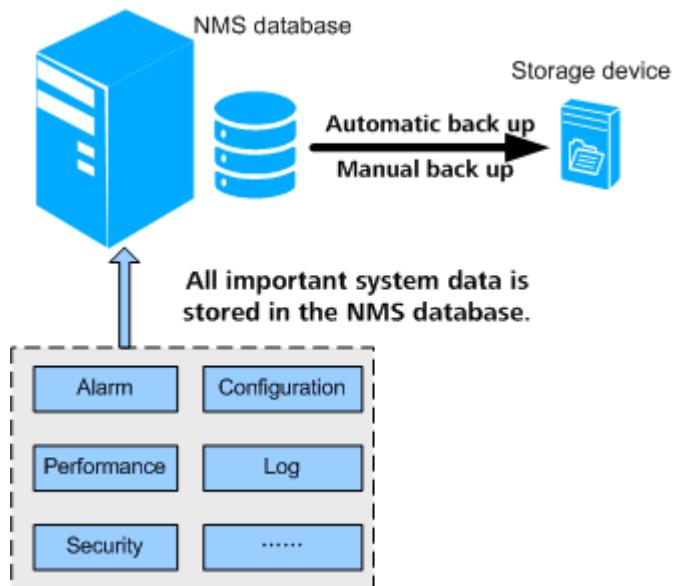
You can use the system control and communication unit (SCC) or compact flash (CF) board on the NE to back up and restore the NE database for some types of transport access NE, including:

- Backing up the NE database to the SCC board manually.
- Backing up the NE database to the CF board manually or automatically.
- Restoring the NE configuration data from the SCC board or CF board.

NMS Database Management

The database of the U2000 supports two types of storage files. One type is used to store data and the other type is used to store the logs that record the runtime information of the database. To ensure data security, periodically back up the database. **Figure 7-29** illustrates the NMS database management.

Figure 7-29 NMS database management



The U2000 provides a database backup and restoration tool. The tool facilitates database maintenance and ensures the stability and security of the U2000. It provides the following NMS database management functions:

- Backs up the U2000 database to a local or remote server in the following ways:
 - Immediate backup
 - Scheduled backup through task scheduling
- Restores the U2000 database from a local or remote server.
- Dumps data in the U2000 database, including logs (such as operation logs, system logs, security logs, and alarm/event logs) and other data (such as performance data). Dumped data are saved to files and deleted from the database. This prevents database space insufficiency.
 - Manual dump
 - Periodic dump

- Imports or exports script files: The U2000 offers the function of importing and exporting script files. The script files can be used to back up or restore network configurations about the U2000, including the user name, password, path information, and topology coordinates, to achieve smooth upgrade of the configurations during the U2000 upgrade.

The main usage of the script files is as follows:

- Realizing the upgrade of the configuration data with zero loss during the U2000 upgrade. This is an important method for the U2000 upgrade. This is the main usage of the script files.
- After the network data is modified, restoring the customized information of the U2000, such as the trail name, fiber name, port name, and the customer information.
- By modifying the script files, realizing the division and combination of the U2000 data and realizing the import of the desired data only, such as the NE list (with no configuration data), fiber connection, protection subnet, or trail.
- Supporting the simplified implementation of the project design.

Description about script files is as follows:

- The scripts exported from the U2000 of an earlier version can be imported to the U2000 of a later version. But an error may occur if the scripts exported from the U2000 of a later version is imported to the U2000 of an earlier version. The U2000 of an earlier version does not support the features and functions that are added and the parameters that are modified in the U2000 of a later version. After the scripts are imported, an error message is displayed. But this does not affect the import of other information.
- The scripts generated on Windows and on UNIX are compatible.
- T2000 scripts can be imported to the U2000. U2000 scripts cannot be imported to the T2000.
- Initializes the U2000 database: Clears and initializes the U2000 database before restoring the database in the event that database data is in disorder or there is corrupted data.
- Remote cold backup and fast recovery: Back up U2000 data to the remote site, which enables the U2000 to quickly recover from an exception. If the primary site fails, perform a switchover between the primary U2000 and the secondary U2000.

Maintaining Data Consistency Between the U2000 and NEs

If the configuration data is not synchronous between the U2000 and the NE, the NE icon will have a  sign. The U2000 provides a variety of functions to ensure the security and consistency of the NE configuration data. These functions include the uploading, downloading, consistency check, synchronization, duplication, preconfiguration, and the initialization of the NE data on the U2000. The basic process of each function is described as follows:

- Uploading: The data on NEs is reported to the U2000 and overwrites the original NE data on the U2000. The data that is present on the U2000 but absent on the NEs is not deleted.
- Downloading: The NE data on the U2000 is applied to the NEs; the original data on the NEs is overwritten.
- Consistency check: Verifies that the NE data on the U2000 is consistent with the data on the NEs. If it is inconsistent, the U2000 will synchronize or upload the NE configuration data.

- Synchronization: Uploads the inconsistent data (including the conflicting data and the data that is present on NEs but absent on the U2000) to the NE layer on the U2000. The data that is present on both the U2000 and the NEs is not uploaded, and the data that is present on the U2000 but absent on the NEs is not deleted.
- Duplication: For NEs of the same type and of the same software version, if the configuration data of an NE to be configured is the same as that of a configured NE, you can configure the new NE by duplicating the data of the configured NE. Duplicating the NE data only changes the data on the U2000 and does not affect the data on the NE. To make the duplicated data take effect on the NE, you need to apply the configuration.
- Preconfiguration: The configuration data of an NE is saved only at the NE layer on the U2000 and does not affect the actual configuration data on the NE. The preconfiguration function is generally used for large-scale service adjustment or expansion.
- Initialization of the NE data on the U2000: The NE data is deleted from the NE layer on the U2000. The NE will be unconfigured after the initialization.

 **NOTE**

The IP NEs only support data synchronize function, that is, the data on NEs is reported to the U2000 and overwrites the original NE data on the U2000.

The PTN RTN, NG WDM (NA), and NG WDM product series do not support preconfiguring and downloading configuration data. The U2000 reliably performs database package backup to resolve the data restoration issues because of the following principles:

- The configuration data backed up in database packages contains all NE data while the configuration data on the U2000 does not.
- The backed-up databases are directly downloaded to the NEs. This method is highly efficient compared to downloading the configuration data from the U2000 to the NEs where the configuration data has to be converted into Qx interface information first.
- On the U2000, only one copy of configuration data is available, while in database package restoration mode, configuration data can be backed up to several copies for users to select as needed.

7.10 NE Communication Parameter Management

The U2000 communicates with managed NEs successfully only after the connection parameters are correctly set.

You can perform the following operations on the U2000:

- Query and set the SNMP parameters
- Manage the default SNMP parameter template
- Query and set the NE Telnet/STelnet parameters
- Configure the Telnet/STelnet parameters in batches
- Manage the Telnet/STelnet parameter template
- Manage the FTP/TFTP/SFTP parameter template
- Manage the NETCONF parameter template
- Query and set the NE NETCONF parameters
- Set CloudOpera CSM Communication

7.11 DCN Management

The U2000 communicates with NEs and manages and maintains network nodes through a DCN network.

In a DCN network, both the U2000 and NEs are considered as nodes. These nodes are connected to each other through Ethernet or data communications channels (DCCs). In an actual network, the U2000 and NEs may be located on different floors of the same building, in different buildings, or in different cities. This makes the U2000 usually communicate with NEs through an external DCN network that consists of equipment such as switches and routers. As such, the DCN network between NEs is referred to as an internal DCN network.

Huawei's NEs support DCN networking through the following communication protocols:

- HWECC. Data transmitted in the DCC is encapsulated through HWECC. HWECC is a private communication protocol developed by Huawei for DCN networking of transmission NEs.
- TCP/IP (IP over DCC). Data transmitted in the DCC is encapsulated through Transmission Control Protocol/Internet Protocol (TCP/IP).
- OSI (OSI over DCC). Data transmitted in the DCC is encapsulated through Open Systems Interconnection (OSI).

All of Huawei's transmission NEs support HWECC, and the physical transmission channels support D1 to D3 bytes by default. If the NE ID is set, ECC communication can be conducted by only inserting optical fibers. Because HWECC is a private protocol, it cannot meet the requirement for managing the network consisting of devices from different vendors.

IP and OSI are standard communication protocols, which enable the management of hybrid device networking. In addition, these two standard protocols can be adopted on networks consisting of only Huawei's transmission devices.

 **NOTE**

In the case of a hybrid network consisting of transmission NEs from different vendors that do not support IP or OSI, Huawei provides solutions such as transparent transmission of DCC bytes and Ethernet service channels' transparent transmission of management information.

The U2000 provides graphic and visualized DCN management functions for MSTP, WDM, microwave, submarine, and PTN products.

The graphic DCN management functions supported by the U2000

- Modify gateway NE (GNE) parameters
- Change the GNE of a non-GNE
- Set a secondary GNE for a non-GNE
- Convert a GNE to a non-GNE
- Convert a non-GNE to a GNE
- Check the GNE switching status
- Test the communication between the U2000 and a GNE
- Check the network communication status

The visualized DCN management functions supported by the U2000

The DCC view offers visualized DCN management functions supported by the U2000. The DCC view displays the DCC network in a topology view where relationships among NEs are intuitively shown, which facilitates management and maintenance. The visualized DCN management functions include:

- Check the communication status and relationships among NEs based on the status of DCC links and DCC subnets.
- Synchronize data from the Main Topology to the DCC view, including the network-wide DCC data and DCC subnet data.
- Save the DCC view at a time point as a snapshot to facilitate maintenance and troubleshooting.
- Switch to the **DCN Management** window of NE Explorer for setting the DCN attributes of NEs.
- Provide GUI-based troubleshooting functions.
 - **Ping** function to test the connection status between an NE and its GNE.
 - **Trace route** function to test the route connection status of the DCC channel between two NEs.
 - **Test Reachable NEs** function to test reachable NEs for an NE whose communication with others is unstable. In the scenarios of DCC storms, you can use this test to find out two NEs that should not have communication and locate faults using traceroute function.
 - Support the **ECC Fault Recovery Wizard**, providing troubleshooting suggestions on embedded control channel (ECC) storms and rapid connection reset to improve fault rectification efficiency.

DCN management involves the following operations for ATN and CX series NEs

- Automatically add non-gateway NEs to the U2000 in batches. Users do not need to plan data before ATN series NEs are powered on and added to the U2000 for management.
- Show the running status and connection status of NEs in the DCN view.

7.12 NE Software Management

NE Software Management, also called DC, is an independent subsystem of the U2000. The DC is used to manage NE software and upgrading or downgrading NE software. Managing NE software includes saving, backup and policy management. Upgrading or downgrading NE software includes loading, restoration, task management and managing Software etc. For security, recommend to use SFTP as the transfer protocol between U2000 and NE.

The main function is listed as followings.

- Saving: After the system is configured, the configuration data is saved in the memory or hard disks of NEs so that the data will not be lost when the system is restarted. The U2000 saves data in the following ways:
 - Manually performing the save operation
 - Automatically performing the save task
 - Automatically performing the save policy

- **Backup:** Backs up NE data (such as configuration data/data file) to storage devices other than NEs. The backup data is used for restoring NE data. If the U2000 has the rights to manage the NE and no loading, backup, or restoration operation is being performed on the NE, the NE will accept the request to backup the data. The U2000 then transmits the contents to be backed up to the specified backup directory on the server by using transfer protocol. And the backup data can be also backed up to the client, or to the third part server. The allowed size of backup files depends on the space size of the disk where the backup directory is located. The U2000 backs up data in the following ways:
 - Manually performing the backup operation
 - Automatically performing the backup task
 - Automatically performing the backup policy
- **Policy management:** Setting policies in advance enables the system to perform operations on NEs periodically or when trigger conditions are met. This is applicable to routine NE maintenance. A policy is periodic. It is used for operations that are performed frequently, such as data saving and data backup. Users can select a policy based on the scenarios at the sites.
- **Loading:** Loads software for upgrading an NE. If the U2000 has the rights to manage the NE upgrading and no loading, backup, or restoration operation is being performed on the NE, the NE will accept the request to load the software. The U2000 then transmits the contents to be loaded to the NE by using transfer protocol. The U2000 loads data in the following ways:
 - Automatically loading by an upgrade task
 - Automatically loading by an auto upgrade task
- **Activating:** Restart the NE to activate the new loaded NE. If the U2000 has the rights to manage the NE upgrading and no loading, backup, or restoration operation is being performed on the NE, the NE will accept the request to activate the NE. The U2000 activates the NE in the following ways:
 - Automatically activating by an auto upgrade task
- **Restoration:** Restores NE data from the backup to an NE. If the U2000 has the rights to manage the NE and no loading, backup, or restoration operation is being performed on the NE, the NE will accept the request to restore the data. The U2000 then transmits the contents to be restored to the NE by using transfer protocol. The U2000 restores data in the following ways:
 - Manually performing the recovery operation
 - Automatically performing the recover task
- **Task management:** The U2000 encapsulates all operations performed during an upgrade or a downgrade of an NE software or patch into a task. An NE is upgraded or downgraded according to the created task and the operations configured for the task. The tasks can be performed manually or set up recurring tasks. A task is not periodic. It is used for operations that are not performed frequently, such as data upgrading. Users can select a task based on the scenarios at the sites.
- **Managing Software:** NE software can be managed in a centralized manner, such as the process of loading NE software from NMS client or NMS server to the software library. In this manner, the process of loading software is simple and fast.
- **NE License Management:** In NE License management, you can query, apply for, install, and change an NE License. In addition, you can adjust the capacities defined in the License. The License controls the validity period or functions of an NE. Therefore, you need to view the License state and change the expired License. Otherwise, services will be affected.

7.13 Report Management

The U2000 provides reports on alarms, logs, and resources. You can print the data or save the data as a file. The reports in tabular format can be filtered by equipment type and saved in XLS, TXT, HTML, or CSV files.

You can view reports on the U2000 in the following ways:

- Viewing resource reports on the U2000 client
- Viewing iWeb reports by using the Internet Explorer browser. This type of report includes alarm reports, log reports, performance reports, and resource reports of equipment in the IP domain.

Resource Report (transport domain)

Type	Report
SDH report	Port resource report
	Statistics report of SDH tributary port resources
	Lower order cross-connections statistic report
	SDH fiber/microwave link resource usage report
	Statistics report of trails between SDH NEs
	Statistics report of SDH protection subnet resources
	Statistics report of SDH circuit resources
Microwave report	Microwave link report
	Microwave license capacity report
	Microwave Air Interface Capacity License report
	ODU Board Information report
	Microwave Configuration report
	Microwave link bandwidth resource report
MSTP Ethernet report	Statistics report of Ethernet port resources
	Statistics report of service resources between Ethernet NEs
WDM statistics report	WDM protection group switching state report
	WDM NE master/slave shelf information report
	Statistics report of WDM client-side port resources
	Statistics report of WDM link resources
	Statistics report of inter-station wavelength resources

Type	Report
	Statistics report of WDM bandwidth resources
	Browse WDM channel resource
	Wavelength resource usage report
	OTU board wavelength information report
Cable transmitting warp report	
Project document	Board manufacturer information
	Export electronic labels
	Clock tracing diagram
	Networking diagram
	Timeslot allocation diagram
	NE inventory report
	Microwave One-Click Acceptance Test

Resource Report (IP domain)

Type	Report
PTN statistics report	Interface resource report
	Network resource statistics report
	Port resource report
	LAG resource report
	MAC Address Forwarding Entries Report
Project document	Export electronic labels
	NE inventory report

Resource Report (access domain)

Type	Report
Access service statistics	DSL Port Status Report
	DSL Port Rate Report
	Idle Port Report
	DSLAM Real Multicast User Report

Type	Report
	Optical Splitting of PON Port Report
	Online ONT Report
	ETH Port Status Report
	Narrowband Port Status Report
	1588v2 Clock Used Report
	Jumbo Frame Used Report
	ETH License Used Report
	Cable Report
	ONT Replacement Report
	Optical Module Info of PON port
	ONU Optics Module Info
	ONU Info
	Collecting the ONT WiFi&AP Usage Report
	ALS License Usage
	Info of NE Status
	PON Port Usage
Project document	Export electronic labels
	Hardware report
	NE inventory report

Resource Report Diagram

[Figure 7-30](#) and [Figure 7-31](#) show the diagrams of the NE-level resource report and the network-level resource report.

Figure 7-30 Diagram of the NE resource report

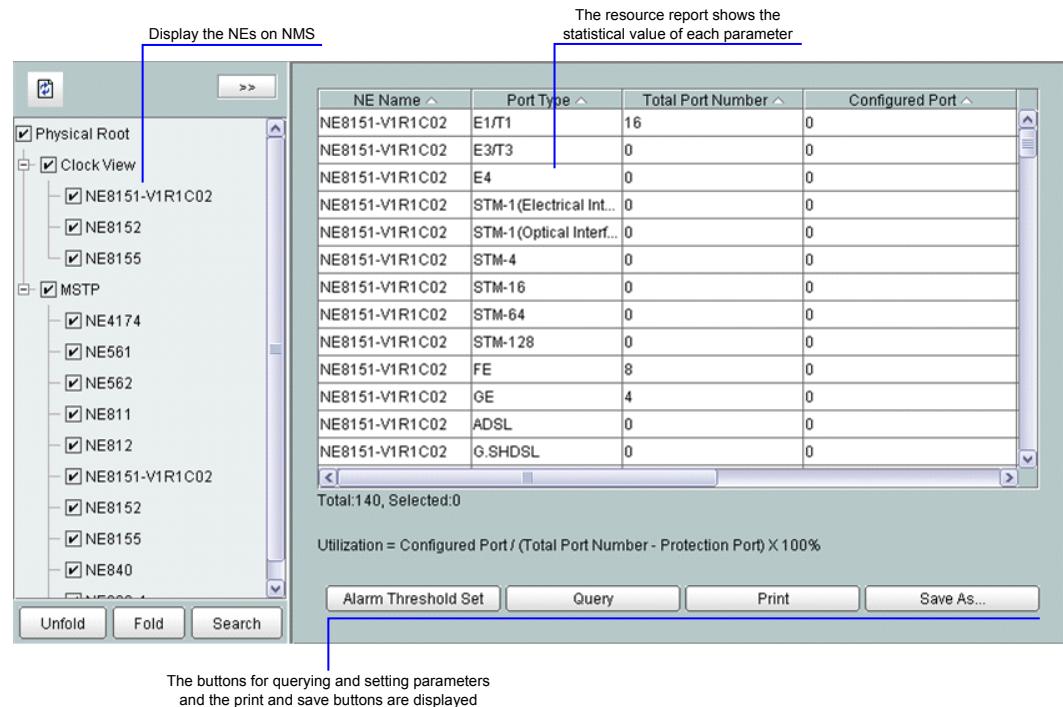
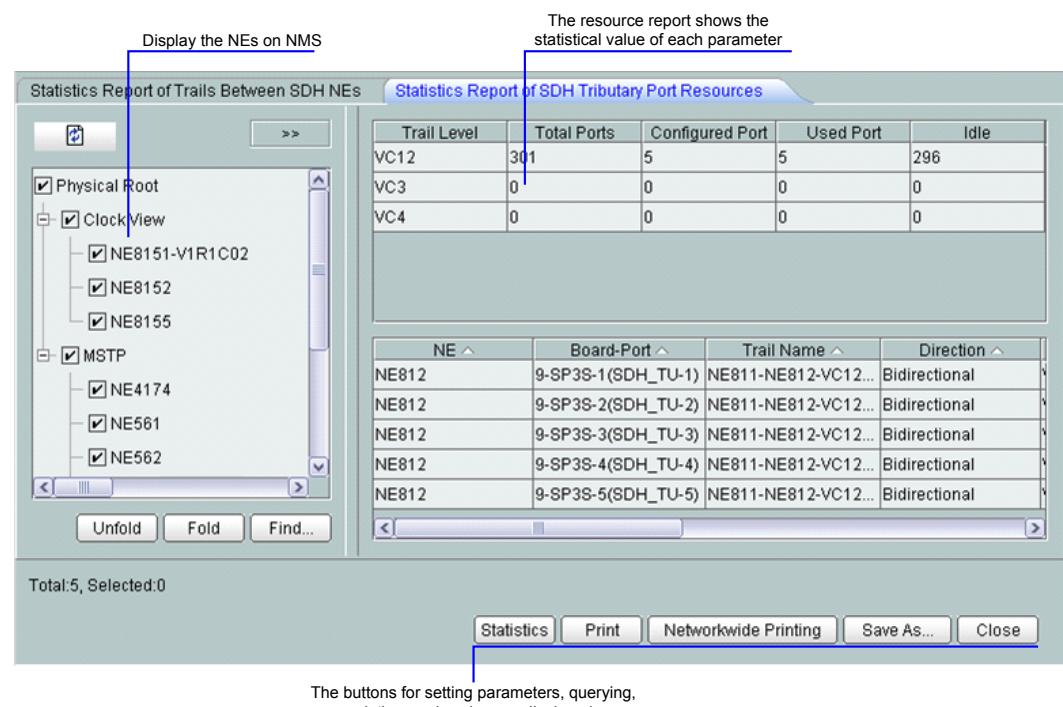


Figure 7-31 Diagram of the network resource report



7.13.1 SDH Report

The SDH report includes various statistics reports on different dimensions, such as on the SDH NEs, cards, ports. These reports offer useful data for the project maintenance.

Figure 7-32 Port Resource Report window and its functions

The screenshot shows a table titled "Port Resource Report" with the following columns: NE Name, Port Type, Total Port Number, Configured Port, Protection Port, Idle, and Utilization(%). The data is as follows:

NE Name	Port Type	Total Port Number	Configured Port	Protection Port	Idle	Utilization(%)
NE(12-2)	E1	0	0	0	0	0
NE(12-2)	E3/T3	0	0	0	0	0
NE(12-2)	E4	0	0	0	0	0
NE(12-2)	STM-1(Electrical Interfaces)	0	0	0	0	0
NE(12-2)	STM-1(Optical Interfaces)	0	0	0	0	0
NE(12-2)	STM-4	0	0	0	0	0
NE(12-2)	STM-16	0	0	0	0	0
NE(12-2)	STM-64	0	0	0	0	0
NE(12-2)	STM-128	0	0	0	0	0
NE(12-2)	T1	0	0	0	0	0
NE(12-2)	FE	0	0	0	0	0
NE(12-2)	GE	4	1	0	3	25
NE(12-2)	10GE LAN	0	0	0	0	0
NE(12-2)	10GE WAN	0	0	0	0	0
NE(12-2)	40GE	0	0	0	0	0
NE(12-2)	100GE	0	0	0	0	0
NE(12-2)	ADSL	0	0	0	0	0
NE(12-2)	G.SHDSL	0	0	0	0	0
NE(12-2)	ATM STM-1	0	0	0	0	0
NE(12-100)	E1	0	0	0	0	0
NE(12-100)	E3/T3	0	0	0	0	0
NE(12-100)	E4	0	0	0	0	0
NE(12-100)	STM-1(Electrical Interfaces)	0	0	0	0	0
NE(12-100)	STM-1(Optical Interfaces)	4	1	0	3	25

No. 0, Total: 38, Selected: 0, Updated at: 12/11/2014 11:08:12

Utilization = Configured Port / (Total Port Number - Protection Port) X 100%

Buttons: Alarm Threshold Settings, Query, Print, Save As...

Figure 7-33 Statistics Report of SDH Tributary Port Resources window and its functions

The screenshot shows a table titled "SDH Tributary Port Resources Statistics Report" with the following columns: Trail Level, Total Ports, Configured Port, Used Port, and Idle. The data is as follows:

Trail Level	Total Ports	Configured Port	Used Port	Idle
VC12	0	0	0	0
VC3	0	0	0	0
VC4	0	0	0	0

No. 0, Total: 3, Selected: 0 Updated at: 2014/12/11 11:15:19

Buttons: Statistics, Network-wide Printing, Print, Save As...

Figure 7-34 Lower Order Cross-Connection Statistics Report window and its functions



Figure 7-35 SDH Fiber/Microwave Link Resource Usage Report window and its functions



Figure 7-36 SDH Trail Statistics Between NEs window and its functions

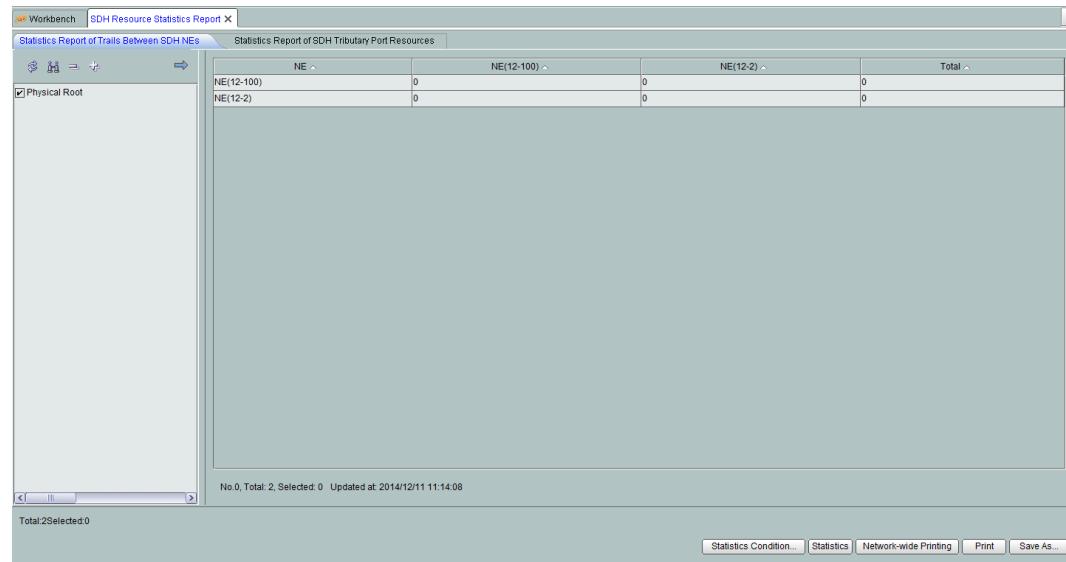


Figure 7-37 Statistics Report of SDH Protection Subnet Resources window and its functions

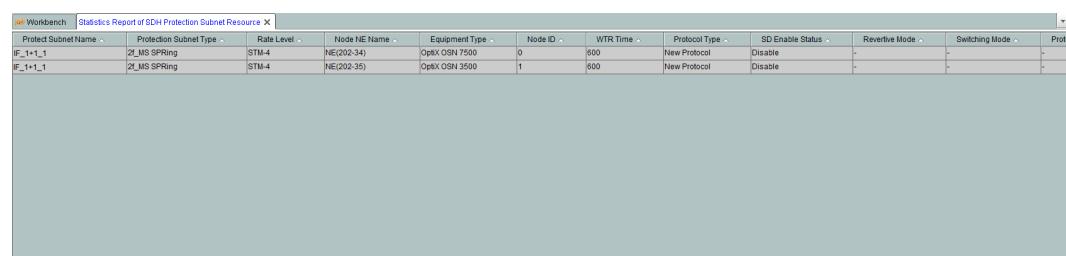


Figure 7-38 Statistics Report of SDH Circuit Resources window and its functions

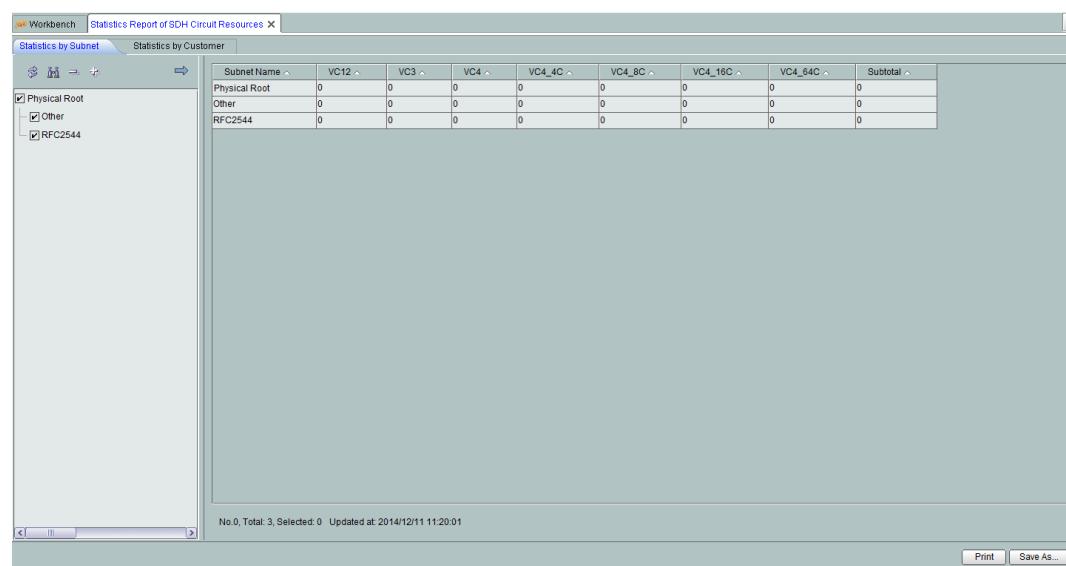


Table 7-10 SDH Report

Report Name	Navigation Path	Statistical Item
Port Resource Report	Choose Inventory > SDH Report > Port Resource Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > SDH Report > Port Resource Report from the main menu (application style).	NE Name, Port Type, Total Port Number, Configured Port, Protection Port, Idle, Utilization(%), Idle port detail information
Statistics Report of SDH Tributary Port Resources	Choose Inventory > SDH Report > Statistics Report of SDH Tributary Port Resources from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > SDH Report > Statistics Report of SDH Tributary Port Resources from the main menu (application style).	Trail Level, Total Ports, Used Port, Configured Port, Idle, NE, Board-Port, Trail Name, Direction, Trail Level, Service Status, Opposite NE, Opposite Board-Port
Lower Order Cross-Connection Statistics Report	Choose Inventory > SDH Report > Lower Order Cross-Connections Statistic Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > SDH Report > Lower Order Cross-Connections Statistic Report from the main menu (application style).	NE Name, NE Type, Subnet, Lower Order Cross-Connection Count(G), Maximum VC4 Number of Lower Order Cross-Connections, Used VC4 Number of Lower Order Cross-Connections, Remaining VC4 Number of Lower Order Cross-Connections, Used VC3 Count, Remaining VC3 Count, Used VC12 Count, Remaining VC12 Count, Used Lower Order Cross-Connections (%)(Equivalent VC12)

Report Name	Navigation Path	Statistical Item
SDH Fiber/Microwave Link Resource Usage Report	<p>Choose Inventory > SDH Report > SDH Fiber/Microwave Link Resource Usage Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > SDH Report > SDH Fiber/Microwave Link Resource Usage Report from the main menu (application style).</p>	Fiber Name, Level, Source NE, Source Board, Source Port, Sink NE, Sink Board, Sink Port, Direction, VC12, VC3, VC4, VC4_4C, VC4_8C, VC4_16C, VC4_64C, Utilization Percent (Equivalent VC-12), Occupancy (Equivalent VC-12), Remaining (Equivalent VC-12), Used High Order Path Number, Threshold Value, Relevant Protection Subnet, Recommendation, Trail Name, Level, Source, Sink, Used VC12, Idle VC12, Higher Order Timeslot, Use Ratio, Contain discrete service
Statistics Report of Trails Between SDH NEs	<p>Choose Inventory > SDH Report > Statistics Report of Trails Between SDH NEs from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > SDH Report > Statistics Report of Trails Between SDH NEs from the main menu (application style).</p>	NE, Total, Trail Level
Statistics Report of SDH Protection Subnet Resources	<p>Choose Inventory > SDH Report > Statistics Report of SDH Protection Subnet Resources from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > SDH Report > Statistics Report of SDH Protection Subnet Resources from the main menu (application style).</p>	Protect Subnet Name, Protection Subnet Type, Rate Level, Node NE Name, Equipment Type, Node ID, WTR Time, Protocol Type, SD Enable Status, Revertive Mode, Switching Mode, Protection Mode, Working Mode, Enable Reverse Switching
Statistics Report of SDH Circuit Resources	<p>Choose Inventory > SDH Report > Statistics Report of SDH Circuit Resources from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > SDH Report > Statistics Report of SDH Circuit Resources from the main menu (application style).</p>	Subnet Name, VC12, VC3, VC4, VC4_4C, VC4_8C, VC4_16C, VC4_64C, Subtotal

7.13.2 Microwave Report

The microwave report includes various statistics reports on different dimensions, such as on the microwave equipment and links. These reports offer useful data for the project maintenance.

Figure 7-39 Microwave Link Report window and its functions

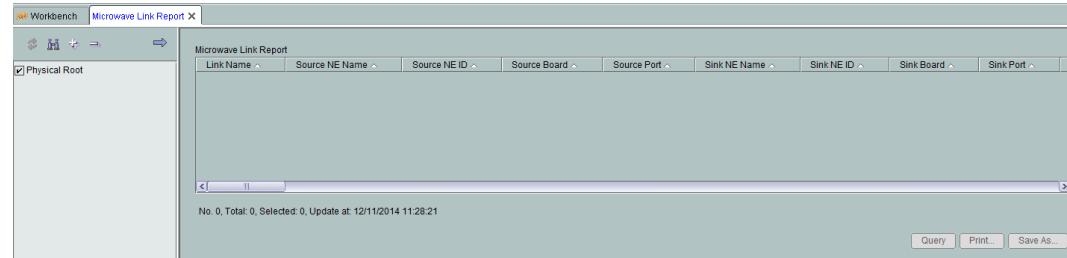


Figure 7-40 Microwave License Capacity Report window and its functions

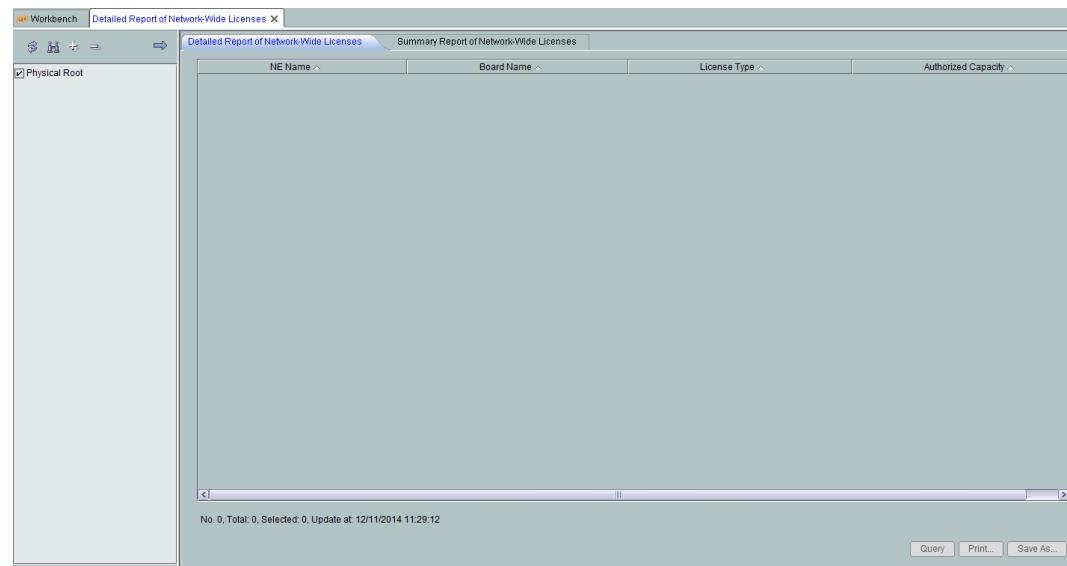


Figure 7-41 Microwave Air Interface Capacity License Report window and its functions



Figure 7-42 ODU Board Information Report window and its functions



Figure 7-43 Export Microwave Configuration Report window and its functions

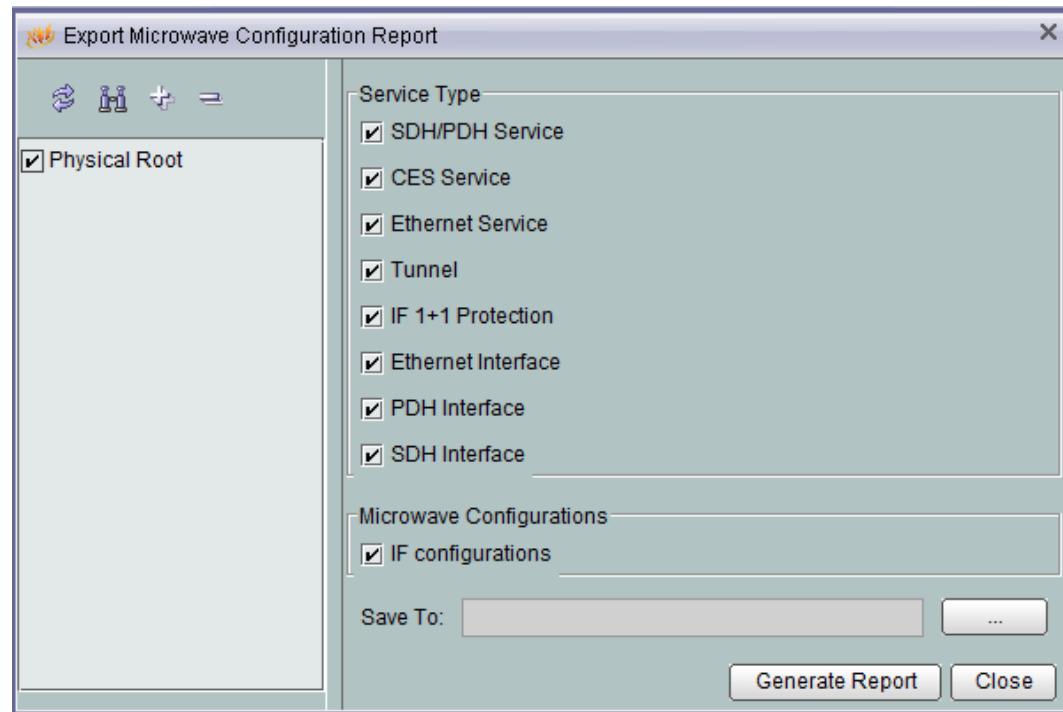


Figure 7-44 Bandwidth Resource Report window and its functions

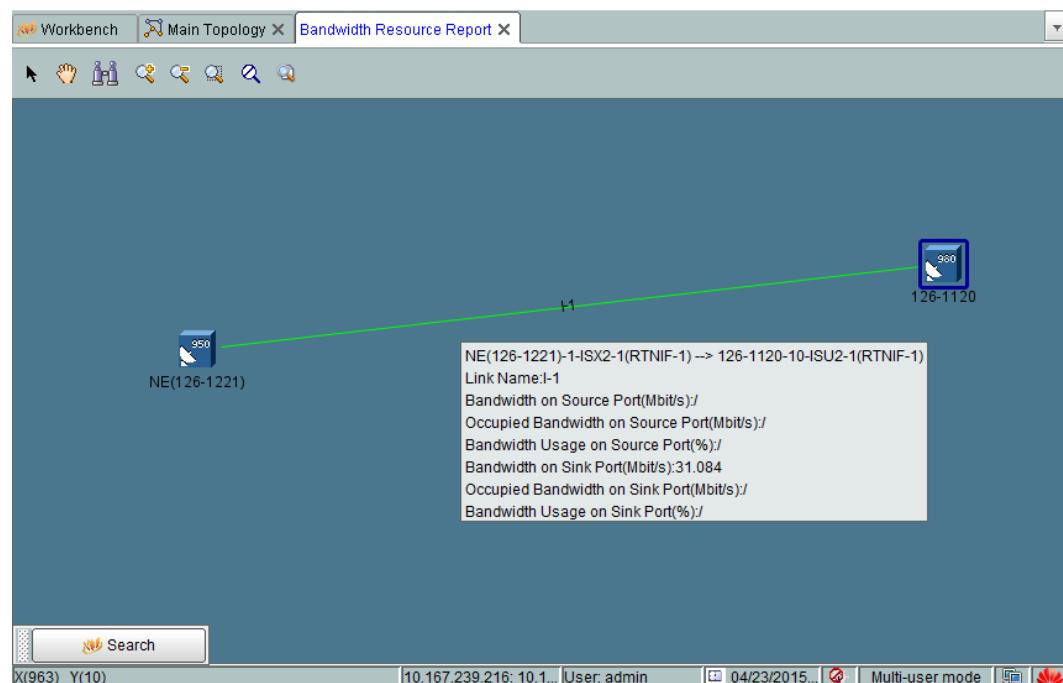


Figure 7-45 Base Station Report



Table 7-11 Microwave Report

Report Name	Navigation Path	Statistical Item
Microwave Link Report	<p>Choose Inventory > Microwave Report > Microwave Link Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Microwave Report > Microwave Link Report from the main menu (application style).</p>	<p>Link Name, Source Physical Location, Source NE ID, Source Board, Source Port, Sink NE Name, Sink NE ID, Sink Board, Sink Port, Level, Source Protect Type, Up and down Rate Ratio(TX:RX), Source Protect Type, Sink Protect Type, Source Protection Group ID, Sink Protection Group ID , Source Protect Unit Type, Sink Protect Unit Type, Source ODU Frequency Range (MHz), Sink ODU Frequency Range (MHz), Source Equipment Information , Sink Equipment Information, Source Station Type, Sink Station Type, Source NE Frequency (MHz), Sink NE Frequency (MHz), Source NE Radio Work Mode, Sink NE Radio Work Mode, Source NE Preset Value of Transmit Power, Sink NE Preset Value of Transmit Power, Source NE Current Value of Transmit Power, Sink NE Current Value of Transmit Power, Source NE Current Value of Receive Power, Sink NE Current Value of Receive Power, Source NE Max Value of Transmit Power of 24-Hour PM, Sink NE Max Value of Transmit Power of 24-Hour PM, Source NE Min Value of Transmit Power of 24-Hour PM, Sink NE Min Value of Transmit Power of 24-Hour PM, Source NE Max Value of Receive Power of 24-Hour PM, Sink NE Max Value of Receive Power of 24-Hour PM, Source NE Min Value of Receive Power of 24-Hour PM, Sink NE Min Value of Receive Power of 24-Hour PM, Source NE Guaranteed E1 Capacity, Sink NE Guaranteed E1 Capacity, Source NE Occupied E1 Capacity, Sink NE Occupied E1 Capacity, Source NE E1 Capacity Usage(%), Sink NE E1 Capacity Usage(%), Source NE Ethernet Capacity (Mbit/s)(Mbit/s), Sink NE Ethernet Capacity (Mbit/s)</p>

Report Name	Navigation Path	Statistical Item
		(Mbit/s), Source NE Max. Ethernet Throughput (kbps), Sink NE Max. Ethernet Throughput (kbps), Source NE Min. Ethernet Throughput (kbps), Sink NE Min. Ethernet Throughput (kbps), Source NE Average Ethernet Throughput (kbps), Sink NE Average Ethernet Throughput (kbps), Source NE ATPC, Sink NE ATPC, Source NE AM Status, Sink NE AM Status, Highest-Order AM Scheme for Source NE, Highest-Order AM Scheme for Sink NE, Lowest-Order AM Scheme for Source NE, Lowest-Order AM Scheme for Sink NE
Microwave License Capacity Report	Choose Inventory > Microwave Report > Microwave License Capacity Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Microwave Report > Microwave License Capacity Report from the main menu (application style).	NE Name, Board Name, License Type, Authorized Capacity, Authorized Capacity Collection
Microwave Air Interface Capacity License Report	Choose Inventory > Microwave Report > Microwave Air Interface Capacity License Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Microwave Report > Microwave Air Interface Capacity License Report from the main menu (application style).	NE, Board, Consumed Licenses(M), Capacity Threshold

Report Name	Navigation Path	Statistical Item
ODU Board Information Report	Choose Inventory > Microwave Report > ODU Board Information Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Microwave Report > ODU Board Information Report from the main menu (application style).	NE, NE Type, Board, Frequency (GHz), The range of the frequency point (MHz), Produce Time, Product SN, Factory Information, Factory Information, Software Version
Export Microwave Configuration Report	Choose Inventory > Microwave Report > Export Microwave Configuration Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Microwave Report > Export Microwave Configuration Report from the main menu (application style).	SDH/PDH Service, CES Service, Ethernet Service, Tunnel, IF 1+1 Protection, Ethernet Interface, PDH Interface, SDH Interface
Bandwidth Resource Report	In the Main Topology, right-click a microwave link and choose Bandwidth Resource Report from the shortcut menu.	Hovering over a microwave link displays the following parameters: Link Name, Bandwidth on Source Port(Mbit/s), Occupied Bandwidth on Source Port(Mbit/s), Bandwidth Usage on Source Port(%), Bandwidth on Sink Port (Mbit/s), Occupied Bandwidth on Sink Port(Mbit/s), Bandwidth Usage on Sink Port(%)
Base Station Report	Choose Inventory > Base Station Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Base Station Report from the main menu (application style).	NE-Board-Port, OMIP, Base Station, MAC Address, MTU, Port Working Mode, VLANs, Remarks, Data Source, Updated On

7.13.3 WDM Statistic Report

The WDM statistics report includes various statistics reports on different dimensions, such as on the WDM NEs, cards and ports. These reports offer useful data for the project maintenance.

Figure 7-46 WDM NE Master/Slave Shelf Info window and its functions

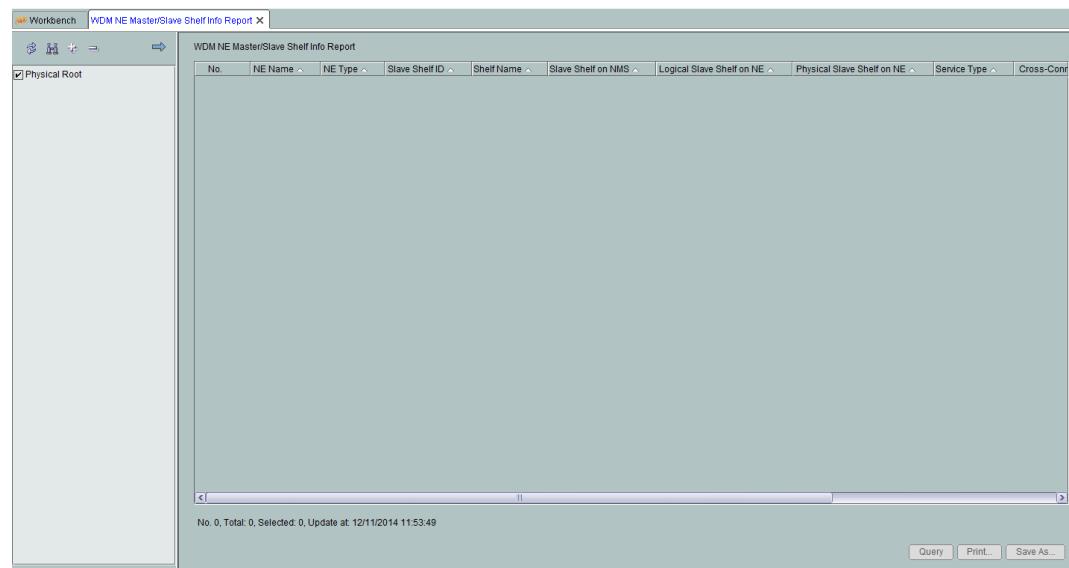


Figure 7-47 WDM Protection Group Switching Status Report window and its functions

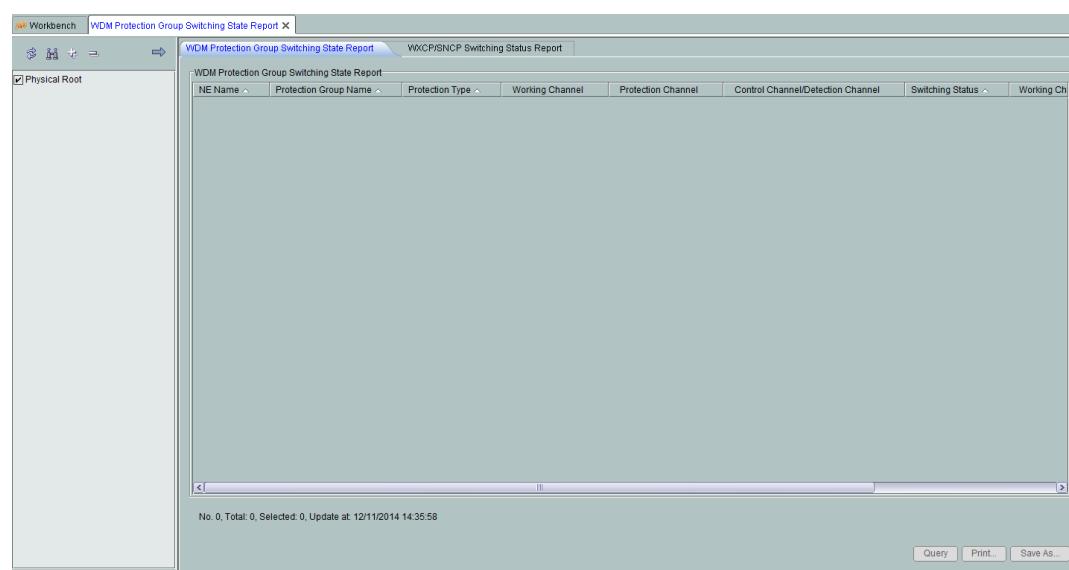


Figure 7-48 WXCP/SNCP Switching Status Report window and its functions



Figure 7-49 OTU Board Wavelength Info Report window and its functions



Figure 7-50 WDM Client Port Resource Statistics window and its functions

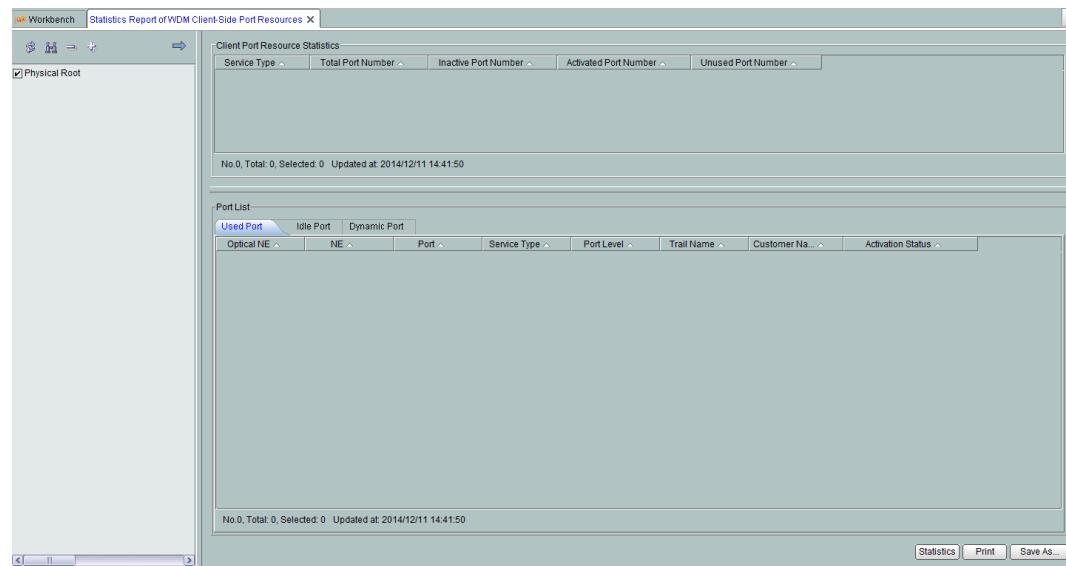


Figure 7-51 WDM Link Resource Statistics window and its functions



Figure 7-52 WDM Statistics on Inter-Station Wavelength Resource window and its functions



Figure 7-53 Statistics Report of WDM Bandwidth Resources window and its functions

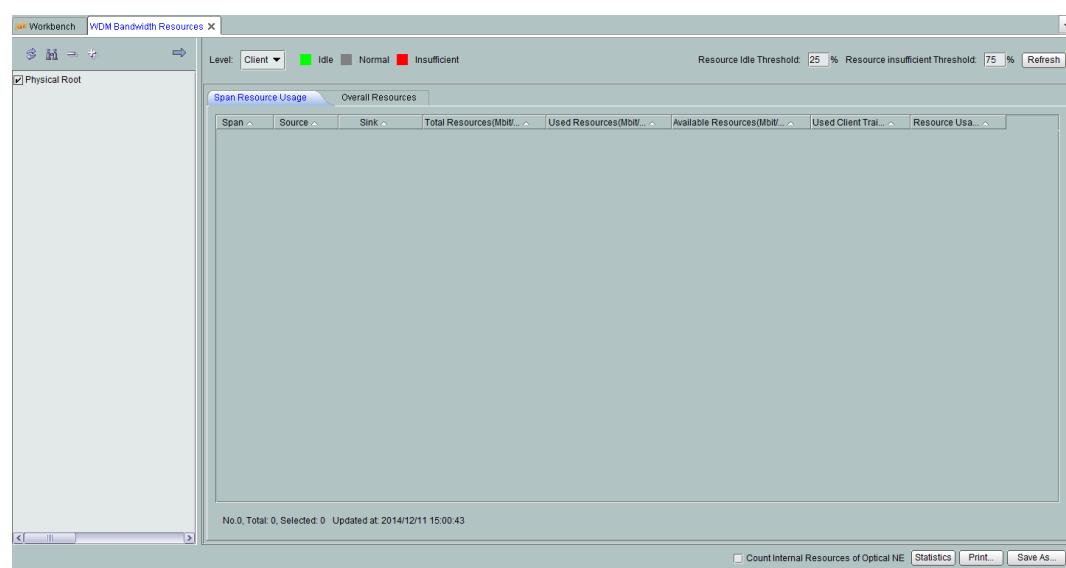


Figure 7-54 Browse WDM Channel Resource window and its functions

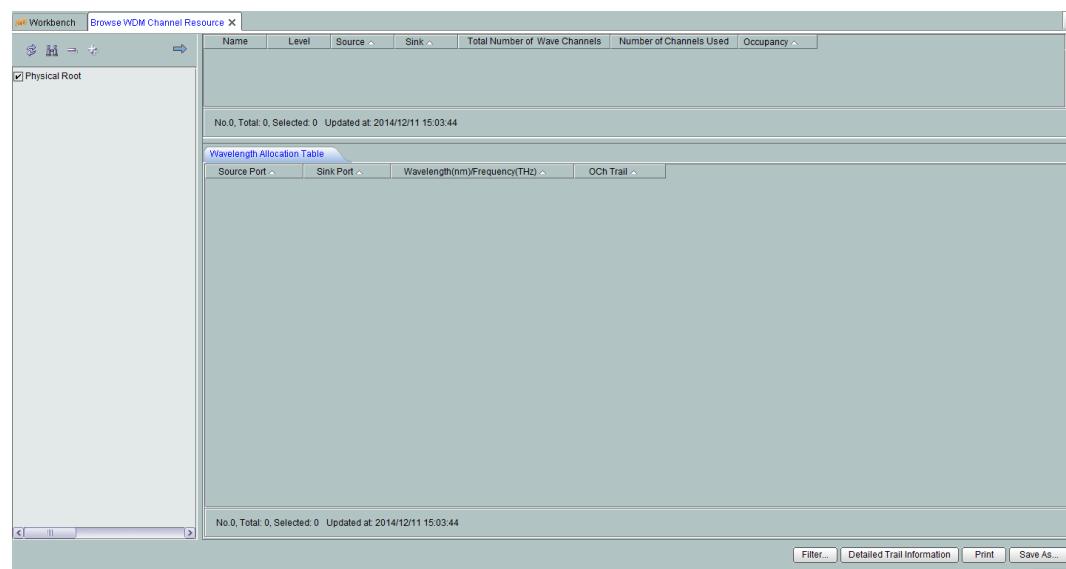


Figure 7-55 Wavelength Resource Usage Report window and its functions



Table 7-12 WDM Statistic Report

Report Name	Navigation Path	Statistical Item
WDM NE Master/ Slave Shelf Info Report	Choose Inventory > WDM Statistic Report > WDM NE Master/Slave Shelf Info Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > WDM NE Master/Slave Shelf Info Report from the main menu (application style).	No., NE Name, NE Type, Slave Shelf ID, Shelf Name, Slave Shelf on NMS, Logical Slave Shelf on NE, Physical Slave Shelf on NE, Service Type, Cross-Connect Capacity, 1588V2, Lower Order Cross-Connection
WDM Protection Group Switching Status Report	Choose Inventory > WDM Statistic Report > WDM Protection Group Switching State Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > WDM Protection Group Switching State Report from the main menu (application style).	NE Name, Protection Group Name, Protection Type, Working Channel, Protection Channel, Control Channel/Monitoring Channel, Switching Status, Working Channel Status, Protection Channel Status
WXCP/ SNCP Switching Status Report	Choose Inventory > WDM Statistic Report > WDM Protection Group Switching State Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > WDM Protection Group Switching State Report from the main menu (application style).	NE Name, Protection Type, Working Cross-Connection, Protection Cross-Connection, Level, Current Status, Current Channel, Working Channel State, Protection Channel State
OTU Board Wavelength Info Report	Choose Inventory > WDM Statistic Report > OTU Board Wavelength Info Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > OTU Board Wavelength Info Report from the main menu (application style).	NE Name, NE Type, NE ID, Slot No., Board Name, Port Name, Port No., Wavelength(Band/No./Wavelength/Frequency)

Report Name	Navigation Path	Statistical Item
WDM Client Port Resource Statistics	<p>Choose Inventory > WDM Statistic Report > Statistics Report of WDM Client-Side Port Resources from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > Statistics Report of WDM Client-Side Port Resources from the main menu (application style).</p>	Service Type, Total Port Number, Inactive Port Number, Activated Port Number, Unused Port Number, Optical NE, NE, Port, Service Type, Port Level, Trail Name, Customer Name, Activation Status, Physical Port, Logical Port, NM Fixed Port, Physical Port Speed(Mbit/s), Logical Port Speed(Mbit/s), NM Fixed Port Speed(Mbit/s)
WDM Link Resource Statistics	<p>Choose Inventory > WDM Statistic Report > Statistics Report of WDM Link Resources from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > Statistics Report of WDM Link Resources from the main menu (application style).</p>	Station, Level, Direction, Name, Source, Sink, Rate, Activated Time, Customer, Service Status, Used/Idle
WDM Statistics on Inter-Station Wavelength Resource	<p>Choose Inventory > WDM Statistic Report > Statistics Report of Inter-Station Wavelength Resources from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > Statistics Report of Inter-Station Wavelength Resources from the main menu (application style).</p>	Level, Direction, Source, Sink, Name, Wavelength(Band/No./ Wavelength/Frequency), Maximum Channels, Number of Occupied Channels
Statistics Report of WDM Bandwidth Resources	<p>Choose Inventory > WDM Statistic Report > Statistics Report of WDM Bandwidth Resources from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > Statistics Report of WDM Bandwidth Resources from the main menu (application style).</p>	Span, Source, Sink, Total Resources, Used Resources, Available Resources, Used Client Trails, Resource Usage, Level, Total resources, Total used resources, Total available resources, Average resource usage, Dispersion

Report Name	Navigation Path	Statistical Item
Viewing WDM Channel Resources	Choose Inventory > WDM Statistic Report > Browse WDM Channel Resource from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > Browse WDM Channel Resource from the main menu (application style).	Name, Level, Source, Sink, Total Number of Wave Channels, Number of Channels Used, Occupancy, Wavelength Allocation Table, Source Port, Sink Port, Wavelength(nm)/Frequency(THz), OCh Trail
Wavelength Resource Usage Report	Choose Inventory > WDM Statistic Report > Wavelength Resource Usage Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > WDM Statistic Report > Wavelength Resource Usage Report from the main menu (application style).	NE Name, Total Channels(Out) , Occupied(Out), Percent(Out), Total Channels(In) , Occupied(In) , Percent(In)

7.13.4 MSTP Ethernet Report

The MSTP Ethernet report includes various statistics reports on different dimensions, such as on the MSTP Ethernet ports and NEs. These reports offer useful data for the project maintenance.

Figure 7-56 Resource Statistics of the Services Between Ethernet NEs window and its functions



Figure 7-57 Resource Statistics of Ethernet Ports window and its functions



Table 7-13 MSTP Ethernet Report

Report Name	Navigation Path	Statistical Item
Resource Statistics of the Services Between Ethernet NEs	Choose Inventory > MSTP Ethernet Report > Statistics Report of Service Resources Between Ethernet NEs from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > MSTP Ethernet Report > Statistics Report of Service Resources Between Ethernet NEs from the main menu (application style).	Source NE, Sink NE, EPL Number, EVPL Number, EVPL(QinQ) Number, Equivalent Bandwidth(M)
Resource Statistics of Ethernet Ports	Choose Inventory > MSTP Ethernet Report > Statistics Report of Ethernet Port Resources from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > MSTP Ethernet Report > Statistics Report of Ethernet Port Resources from the main menu (application style).	NE Name, Board Name, Used MAC Port, Unused MAC Port, Used Trunk Port, Unused Trunk Port

7.13.5 PTN Statistic Report

The PTN statistic report includes various statistics reports on different dimensions, such as interface resource report, network resource statistic report and MAC address forwarding entries report. These reports offer useful data for the project maintenance.

Figure 7-58 Interface Resource Report window and its functions

The screenshot shows the 'Interface Resource Report' window within the iManager U2000 interface. The left sidebar displays a tree structure with 'Physical Root' and 'PTN' selected. The main area is a table with the following columns: NE Name, Device Type, Slot Number, Subslot Number, Port Number, Port Name, Port Type, and Layer Rate. The table lists numerous entries, mostly 'OptiX PTN 3900' devices, with various port configurations. At the bottom of the window, a status bar shows 'No. 0, Total: 1133, Selected: 0, Update at: 04/03/2015 15:39:53' and buttons for Filter, Query, Print..., and Save As... .

NE Name	Device Type	Slot Number	Subslot Number	Port Number	Port Name	Port Type	Layer Rate
NE(10-1955)	OptiX PTN 3900	-	-	11	xutest	MLPPP	-
NE(10-1955)	OptiX PTN 3900	-	-	12	12	MLPPP	-
NE(217-42)	OptiX PTN 3900-B	-	-	12	Denmar_shidan	MLPPP	-
NE(217-42)	OptiX PTN 3900-B	-	-	21	df3a23	MLPPP	-
NE(217-42)	OptiX PTN 3900-B	-	-	22	test1	MLPPP	-
NE(217-42)	OptiX PTN 3900-B	-	-	23	fyt	MLPPP	-
NE(10-1955)	OptiX PTN 3900	-	-	22	333	MLPPP	-
NE(10-1955)	OptiX PTN 3900	-	-	13	13	MLPPP	-
NE(9-158)	OptiX PTN 3900-B	-	-	6	test1	Serial	-
NE(9-158)	OptiX PTN 3900-B	-	-	22	22	Serial	-
NE(217-42)	OptiX PTN 3900-B	-	-	5	Denmar_shidan	Serial	-
NE(10-1955)	OptiX PTN 3900	-	-	2	ddd23	Serial	-
NE(10-1955)	OptiX PTN 3900	-	-	63	TEST20	Serial	-
NE(217-39)	OptiX PTN 3900-B	-	-	3	222	Serial	-
NE(190-32187)	OptiX PTN 910-F	2	-	16		Ethernet	GE
NE(190-32187)	OptiX PTN 910-F	2	-	15		Ethernet	GE
NE(190-32187)	OptiX PTN 910-F	2	-	14		Ethernet	GE
NE(190-32187)	OptiX PTN 910-F	2	-	13		Ethernet	GE

Figure 7-59 Network Resource Statistic Report window and its functions

The screenshot shows the 'Network Resource Statistics Report' window within the iManager U2000 interface. The left sidebar displays a tree structure with 'Physical Root' and 'PTN' selected. The main area is a table with the following columns: NE Name, Node Quantity, ISIS Peer Quantity, DCN Link Quantity, DCN Node Quantity, Tunnel Quantity, and L2VPN P. The table lists various network elements (NE) with their respective resource counts. At the bottom of the window, a status bar shows 'No. 0, Total: 12, Selected: 0, Update at: 04/03/2015 15:46:04' and buttons for Filter, Query, Print..., and Save As... .

NE Name	Node Quantity	ISIS Peer Quantity	DCN Link Quantity	DCN Node Quantity	Tunnel Quantity	L2VPN P
NE(20-1)	1	0	16	37	813	21
NE(217-216)	1	0	4	9	412	60
NE(217-84)	1	0	1	9	1078	19
NE(9-158)	0	0	0	1	28	7
@222	-	-	0	1	12	6
NE(10-1955)	1	0	0	1	584	62
NE(217-69)PTN39	1	0	3	7	5136	1565
NE(190-32187)	1	0	0	1	0	0
NE(217-39)	0	0	0	1	688	43
NE(217-74)	1	0	1	7	1481	226
NE(210-210)	1	0	0	1	0	0
NE(217-70)	1	0	2	7	4454	803

Figure 7-60 Port Resource Report window and its functions

The screenshot shows the 'Port Resource Report' window. On the left is a tree view of network elements under 'Physical Root'. Under 'PTN', several interfaces are listed: E3/T3, E4, STM-1(Electrical Interface), STM-1(Optical Interfaces), STM-4, STM-16, STM-64, STM-128, T1, FE, GE, 10GE LAN, 10GE WAN, 40GE, 100GE, and ADSL. The right side is a table with columns: NE Name, Port Type, Total Port Number, Configured Port, Protection Port, Idle, and Utilization(%). The utilization column uses color coding: green for 0-20%, yellow for 21-40%, orange for 41-60%, red for 61-80%, and dark red for 81-100%. A status bar at the bottom indicates 'Utilization = Configured Port / (Total Port Number - Protection Port) X 100%'. Buttons at the bottom include 'Alarm Threshold Settings', 'Query', 'Print', and 'Save As...'.

NE Name	Port Type	Total Port Number	Configured Port	Protection Port	Idle	Utilization(%)
NE(20-1)	E3/T3	0	0	0	0	0
NE(20-1)	E4	0	0	0	0	0
NE(20-1)	STM-1(Electrical Interface)	0	0	0	0	0
NE(20-1)	STM-1(Optical Interfaces)	0	0	0	0	0
NE(20-1)	STM-4	0	0	0	0	0
NE(20-1)	STM-16	0	0	0	0	0
NE(20-1)	STM-64	0	0	0	0	0
NE(20-1)	STM-128	0	0	0	0	0
NE(20-1)	T1	0	0	0	0	0
NE(20-1)	FE	0	0	0	0	0
NE(20-1)	GE	24	13	0	11	54
NE(20-1)	10GE LAN	20	12	0	8	60
NE(20-1)	10GE WAN	0	0	0	0	0
NE(20-1)	40GE	2	2	0	0	100
NE(20-1)	100GE	0	0	0	0	0
NE(20-1)	ADSL	0	0	0	0	0

Figure 7-61 LAG Resource Report window and its functions

The screenshot shows the 'LAG Resource Report' window. On the left is a tree view of network elements under 'Physical Root'. Under 'PTN', several LAGs are listed: asa, fsf003, luofang-LAG-10, LTE-SGW-Master-wangbo, LTE-OMC-Master-wangbo, PTN_SIT_AUTOTEST, test1, TEST, and luofang-LAG-10. The right side is a table with columns: NE Name, LAG ID, LAG Name, LAG Type, Master Port, and Master Port Status. A status bar at the bottom indicates 'No.6,Total:11,Selected:1,Update at:03-04-2015 16:00:26'. Buttons at the bottom include 'Query', 'Print...', and 'Save As...'.

NE Name	LAG ID	LAG Name	LAG Type	Master Port	Master Port Status
NE(217-39)	7		Static	5-82EG16-13(PORT-13)	/
NE(217-42)	1	asa	Static	6-81EG8-1(PORT-1)	/
NE(217-42)	2	fsf003	Static	3-EFF8-1(asap)	/
NE(217-70)	1	luofang-LAG-10	Manual	3(VE-sd-l2ve)	/
NE(20-1)	1	LTE-SGW-Master-wangbo	Static	18-86EX2-1(SGW_LAG_MAS..)	/
NE(20-1)	2	LTE-OMC-Master-wangbo	Static	21-86EFG8-1(PORT-1)	/
NE(20-1)	6	PTN_SIT_AUTOTEST	Static	6-86EX4-3(PORT-3)	/
NE(9-158)	1	test1	Static	5-81EG8-1(PORT-1)	/
NE(10-1955)	1	TEST	Static	1-82EG16-5(66666)	/
NE(10-1955)	2	TEST	Static	7-82EG16-1(PORT-1)	/
NE(217-69)PTN39	1	luofang-LAG-10	Manual	3(VE-sd-l2ve)	/

Figure 7-62 MAC Address Forwarding Entries Report window and its functions

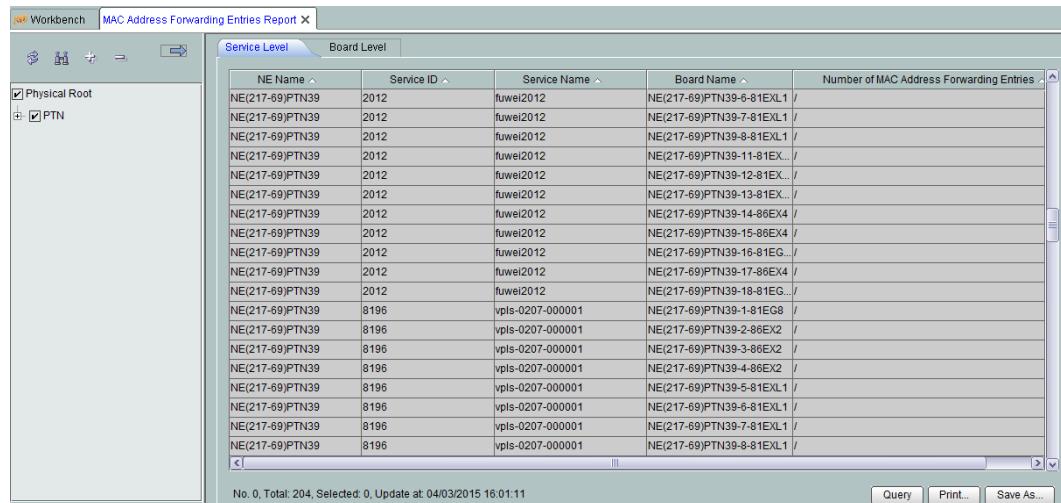


Table 7-14 PTN Statistic Report

Report Name	Navigation Path	Statistical Item
Interface Resource Report	Choose Inventory > PTN Statistic Report > Interface Resource Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > PTN Statistic Report > Interface Resource Report from the main menu (application style).	NE Name, Device Type, Slot Number, Subslot Number, Port Number, Port Name, Port Type, Layer Rate, MAC Address, IP Address, IP Mask, Optical Module Status, Working Mode, Frame Format
Network Resource Statistic Report	Choose Inventory > PTN Statistic Report > Network Resource Statistics Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > PTN Statistic Report > Network Resource Statistics Report from the main menu (application style).	NE Name, Node Quantity, ISIS Peer Quantity, DCN Link Quantity, DCN Node Quantity, Tunnel Quantity, L2VPN PW Quantity, L2VPN T-LDP Peer Quantity, L3VPN VRF Quantity, L3VPN Local Private Route Quantity, L3VPN Private Route Capacity, L3VPN BGP Peer Quantity

Report Name	Navigation Path	Statistical Item
Port Resource Report	Choose Inventory > PTN Statistic Report > Port Resource Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > PTN Statistic Report > Port Resource Report from the main menu (application style).	NE Name, Port Type, Total Port Number, Configured Port, Protection Port, Idle, Utilization(%), Slot Number, Board Type, Idle Port Number
LAG Resource Report	Choose Inventory > PTN Statistic Report > LAG Resource Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > PTN Statistic Report > LAG Resource Report from the main menu (application style).	NE Name, LAG No., LAG Name, LAG Type, Master Port, Master Port Status, Standby Port, Standby Port Status
MAC Address Forwarding Entries Report	Choose Inventory > PTN Statistic Report > MAC Address Forwarding Entries Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > PTN Statistic Report > MAC Address Forwarding Entries Report from the main menu (application style).	Service Level: NE Name, Service ID, Service Name, Board Name, Number of MAC Address Forwarding Entries Board Level: NE Name, Board Name, Number of MAC Address Forwarding Entries

7.13.6 Access Service Statistics Reports

Access service statistics reports provide information such as the device quantity, device type, service, port activation rate, and port fault rate to present network status regularly. This helps carriers plan services and expansion.

Physical inventory reports

For details about physical inventory reports, see [7.7 Inventory Management](#).

Service statistics reports

Navigation path: Choose **Inventory > Access Service Statistics** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Inventory > Access Service Statistics** from the main menu (application style).. In the **Access Service Statistics** window, select a report type for statistics collection under **Statistical Type** in the navigation tree.

Figure 7-63 Access service statistics type

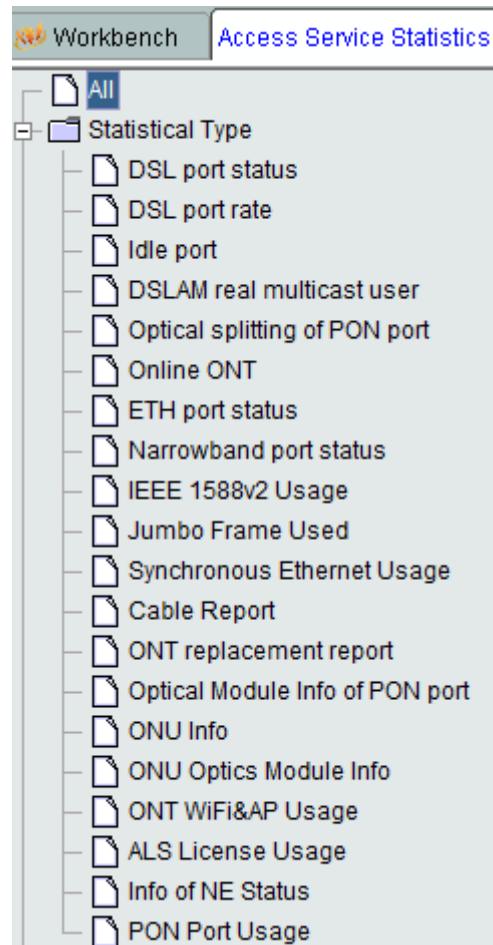


Table 7-15 Access service statistics reports

Report Name	Report Function	Statistical Item
DSL Port Status Report	Collecting statistics on the number of xDSL ports that are activated, being activated, deactivated, blocked, and in other states (such as faulty and under loopback tests).	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Port Type, Activated, Activating, Deactivated, Blocked, Other, Remarks

Report Name	Report Function	Statistical Item
DSL Port Rate Report	Collecting statistics on ports at different rates according to the maximum downstream rate preset in the line profile of xDSL ports, evaluate the service distribution of ports, and learn service development at all network levels.	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Port Type, < 128K, 128K-512K, 512K-1M, 1M-2M, 2M-4M, 4M-8M, > 8M, Remarks
Idle Port Report	Collecting the number and distribution of idle xDSL and ETH_FE ports helps to learn the service applications of customers. An idle port is the port that is last activated before the preset activation time and is in the deactivated state.	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Port Type, Idle, Occupied, Remarks
DSLAM Real Multicast User Report	Collecting statistics on the number of multicast users that watch programs within a specified period. The statistics can be used to analyze service data.	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Number of Multicast Users, Number of Multicast Users Watching Programs, Remarks
Optical Splitting of PON Port Report	Collecting statistics on optical splitting resources, used optical splitting resources, idle optical splitting resources, and remaining guaranteed bandwidths of PON ports to learn information about resources available for service provisioning.	OLT Device Name, Name, Optical Splitting Resources, Used Optical Splitting Resources, Idle Optical Splitting Resources, Remaining Guaranteed Bandwidth (Kbit/s)

Report Name	Report Function	Statistical Item
Online ONT Report	Collecting statistics on the number of online and offline ONTs. You can collect statistics on the number of online ONT users and the split ratio of PON ports to learn information about resources available for service provisioning.	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Port Type, ONT Online, ONT Offline, Other, Remarks
ETH Port Status Report	Collecting statistics on the number of Ethernet ports that are online, offline, not installed, and in other states (such as faulty and under loopback tests).	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Port Type, ETH Online, ETH Offline, ETH Not Installed, Other, Remarks
Narrowband Port Status Report	Collecting statistics on the narrowband port usage. The narrowband ports must be registered with the media gateway (MG) successfully and be configured with services.	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Port Type, POTS Configured, POTS Unconfigured, Other, Remarks
1588v2 Clock Used Report	Checking whether the IEEE 1588v2 function is enabled on NEs and learn license consumption.	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Usage Status, Other, Remarks
Jumbo Frame Used Report	Checking the number of jumbo frames on ports and learn license consumption.	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Port Type, Position, Usage Status, Remarks
ETH License Used Report	Checking whether the synchronous Ethernet clock function is enabled on NEs and learn license consumption.	Submap 0, Submap 1, Submap 2, Submap 3, NE Name, NE Type, NE IP, Port Type, ETH Online, ETH Offline, ETH Not Installed, Other, Remarks

Report Name	Report Function	Statistical Item
Cable Report	<p>Collecting cable traffic on network-wide CMC devices within the specified period of time. This report supports four types: OLT-based, CMC-based, OLT-based (with upstream aggregate traffic) and CMC Upstream Channel SNR Abnormality Report.</p>	<p>OLT-based traffic report CMC-based traffic report OLT-based traffic report(with upstream aggregate traffic) CMC Upstream Chanel SNR Abnormality Report</p> <ul style="list-style-type: none"> ● OLT-based traffic report: Device Name, DCMTS Number, Band User Number(Peak Online), TV User Number(Peak Online), Voice User Number(Peak Online), Router User Number(Peak Online), Unclassified User Number(Peak Online), Total Number(Peak Online), CM Total Number, Port, Max Rx Rate(Mbps), Band Utilization Rate ● CMC-based traffic report: OLT, Sequence, Port, PortSendRate(Peak)(Mbps), CMC Position, CM Total Number, CM Offline, CM Online ● OLT-based traffic report(with upstream aggregate traffic): Device Name, DCMTS Number, Band User Number(Peak Online), TV User Number(Peak Online), Voice User Number(Peak Online), Router User Number(Peak Online), Unclassified User Number(Peak Online), Total Number(Peak Online), CM Total Number, Aggregated Ports, Max Rx Rate(Mbps), Band Utilization Rate ● CMC Upstream Chanel SNR Abnormality Report: OLT, Sequence, Port, CMC Position, The times of SNR is less than abnormality threshold(Upstream Channel 1), The times of SNR is less than abnormality threshold(Upstream Channel 2), The times of SNR is less than abnormality threshold(Upstream Channel 3), The times of SNR is less than abnormality threshold(Upstream Channel 4)

Report Name	Report Function	Statistical Item
ONT Replacement Report	Collecting statistics on the number of Huawei ONTs, ONT-Replaced users, and ONT replacements.	NeName, NeType, NeIP, Number of Huawei ONTs, Number of ONT-Replaced Users, Number of ONT Replacements,
Optical Module Info of PON port	Collecting the optical module information of PON port.	Topology, NeName, NeType, NeIP, FRAME, SLOT, PORT, ONUID, ONU Name, ONU Alias, ONUTYPE, Vendor ID, Terminal Type, Software Version, Authentication Mode, SN/MAC, Password/Key, LOID, CheckCode, Ranging(m), Temperature(C), Biascurrent(mA), Voltage(V), TxOpticalPower(dBm), RxOpticalPower(dBm), OLTRxONUOpticalPower(dBm), VendorPN, ModuleType, ModuleSubtype, UsedType, EncapsulationType, OpticalPowerPrecision(dBm)
ONU Optics Module Info	Collecting the information about ONU optical modules, including voltage, biascurrent, temperature, transmit optical power and receive optical power.	NeName, NeType, NeIP, FRAME, SLOT, PORT, Name, UserLabel, RunStatus, OperStatus, AutofindOntEn, Temperature(C), TxBiasCurrent(mA), SupplyVoltage(V), TxPower(dBm), TYPE, SUBTYPE, IDENTIFIER, CONNECTOR, DistNearest, DistFarthest, DnFecEn, ChgPasswordAge, LENGTH9MICRON, LENGTH50MICRON, LENGTH62MICRON5, VENDORNAME, VENDOROUI, VENDORPN, VENDORSN, VENDORREV, WAVELENGTH
ONU Info	Collecting the ONU information, including ONU name, ONU alias, terminal type, running status, last up time, last down time, last down cause, signaling IP, MGC IP.	Topology, OLT Name, OLT Alias, OLT IP, FRAME, SLOT, PORT, ONUID, ONUTYPE, ONU Name, ONU Alias, ONU IP, Vendor ID, Terminal Type, Software Version, Authentication Mode, SN/MAC, Password/Key, LOID, CheckCode, Running Status, Time Added to NMS, Last Up Time, Last Down Time, Last Down Cause, Signaling IP, MGC IP1, MGC IP2

Report Name	Report Function	Statistical Item
Collecting the ONT WiFi&AP Usage Report	Collecting statistics on the ONT WiFi&AP usage.	SubMap0, SubMap1, NeName, NeType, NeIP, Number of Huawei ONTs, Number of ONTs that can Detect WiFi and APs, Number of ONTs that Generate WiFi Traffic, Number of ONTs who Have External APs, Number of External APs, Remark
ALS License Usage	Collecting statistics on the ALS license consumption of live-network NEs.	NeName, NeIP, ONT Interoperability Per xPON ONT License, ONT Interoperability Per 10G xPON ONT License, ONT Hosting License Based on Per ONT, Per MELT Test Port License, Per IPv6 Host License, Consumption of DOCSIS Upstream Extension Channel Resource License, Channels Disabled as Lack of DOCSIS Upstream Extension Channel Resource License, Consumption of DOCSIS Downstream Extension Channel Resource License, Channels Disabled as Lack of DOCSIS Downstream Extension Channel Resource License, Consumption of DOCSIS 3.1 Upstream Extension Frequency Band Resource License, Channels Disabled as Lack of DOCSIS 3.1 Upstream Extension Frequency Band Resource License, Consumption of DOCSIS 3.1 Downstream Extension Frequency Band Resource License, Channels Disabled as Lack of DOCSIS 3.1 Downstream Extension Frequency Band Resource License, Per MPLS Host License, Vectoring Per Port License, Per Virtual Access NE License
Info of NE Status	Collecting statistics on the NE name, IP address, and NE status. By comparing the statistics results before and after the upgrade, you can check the change of NE status.	NeName, NeIP, Device Status

Report Name	Report Function	Statistical Item
PON Port Usage	Collecting the use of PON ports, including the number of PON boards, PON ports, used PON ports, idle PON ports and PON port usage.	Topology, OLT Name, OLT Alias, OLT IP, OLT Type, PON Boards, PON Ports, Used PON Ports, Idle PON Ports, PON Port Usage

Access service resources

This interface provides the capabilities of managing network-wide access resources, including ports, connections, and users. You can quickly query the usage of a certain type of resource on network-wide devices, synchronize network-wide resources of a certain type of device, locate to a specific resource for more operations, or save resources to a file and print it.

Table 7-16 Access service resources

Navigation Path	Resource Information Available for Export
Choose Configuration > Access Service Management > Ethernet Port from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > Ethernet Port from the main menu (application style).	Ethernet port information: Device Name, Name, Alias, Port Type, Working Mode, Port Rate (Mbit/s), Type of Connected Cable, Default VLAN ID Aggregation group information: Device Name, Name, Aggregation Mode, Work Mode
Choose Configuration > Access Service Management > ADSL Port from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > ADSL Port from the main menu (application style).	ADSL port information (including the profiles referenced): Device Name, Name, Alias, Line Profile, Alarm Profile, Extended Profile, Port Type ADSL bonding group information: Device Name, Name, Alias, Bind Scheme, Peer Bind Scheme, Discovery Code, Bonding Group Profile, Rate Alarm
Choose Configuration > Access Service Management > VDSL2 Port from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > VDSL2 Port from the main menu (application style).	VDSL2 port information (including the profiles referenced): Device Name, Name, Alias, Line Template, Alarm Template, Type VDSL2 bonding group information: Device Name, Name, Alias, Admin Scheme, Peer Admin Scheme, Discovery Code, Bonding Group Profile, Rate Alarm

Navigation Path	Resource Information Available for Export
<p>Choose Configuration > Access Service Management > ATM G.SHDSL Port from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > ATM G.SHDSL Port from the main menu (application style).</p>	<p>ATM G.SHDSL port information (including the profiles referenced): Device Name, Name, Alias, Bind Status, Line Profile, Endpoint Alarm Profile, Type</p>
<p>Choose Configuration > Access Service Management > TDM G.SHDSL Port from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > TDM G.SHDSL Port from the main menu (application style).</p>	<p>TDM G.SHDSL port information: Device Name, Name, Alias, Rate, Work Mode, Frame Mode/Synchronization Mode, Loopback Status, Line Mode, Auto Active</p>
<p>Choose Configuration > Access Service Management > ISDN BRA Port from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > ISDN BRA Port from the main menu (application style).</p>	<p>VoIP BRA port information: Device Name, Name, Alias, MG ID, Terminal ID, Telephone No., SG ID, Interface ID, Service Configured, TID Layered, Overload Priority V5 BRA port information: Device Name, Name, Alias, V5 Interface ID, EF Addr., Port Group No., V5.1 TS 1, V5.1 TS 2, Tel. No., Remote Power, User Port Configuration</p>
<p>Choose Configuration > Access Service Management > EPON UNI Port from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > EPON UNI Port from the main menu (application style).</p>	<p>EPON UNI port information: OLT Device Name, Name, Alias, Max. Distance, ONU Auto Discovery</p>

Navigation Path	Resource Information Available for Export
<p>Choose Configuration > Access Service Management > EPON ONU from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > EPON ONU from the main menu (application style).</p>	<p>EPON ONU information: OLT Device Name, Frame, Slot, Port, ONU ID, Name, Alias, Vendor ID, Terminal Type, Software Version, Is E8C Device, EPON ONU Capacity Profile, EPON DBA Profile, Line Profile, ONU Service Level Profile, Service Profile, MAC, Key, LOID, Checkcode, CIR Value</p> <p>Information about automatically discovered EPON ONUs: OLT Device Name, Location, MAC Address, Key, LOID, Checkcode, Vendor ID, Terminal Type, Software Version, OUI Version, Extended ONU Model, Rate Type, Isolation Status</p>
<p>Choose Configuration > Access Service Management > GPON UNI Port from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > GPON UNI Port from the main menu (application style).</p>	<p>GPON UNI port information: Device Name, Name, Alias, Min.Distance, Max.Distance, Downstream FEC, ONU Auto Discovery</p>
<p>Choose Configuration > Access Service Management > GPON ONU from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > GPON ONU from the main menu (application style).</p>	<p>GPON ONU information: Device Name, Frame, Slot, Port, ONU ID, Name, Alias, SN, Password, LOID, Checkcode, Vendor ID, Terminal Type, Software Version, Is E8C Device, ONU Service Level Profile, Line Profile, Service Profile, ONU Power Reduction Profile</p> <p>Information about automatically discovered GPON ONUs: Device Name, Location, SN, Password, LOID, Checkcode, Vendor ID, Terminal Type, Software Version, Isolation Status, Rate Type</p>
<p>Choose Configuration > Access Service Management > CM Terminal from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > CM Terminal from the main menu (application style).</p>	<p>CM terminal information: Device Name, CMC Name, CM ID, MAC Address, CM Description, IPv4 Address, IPv6 Address, RF Port, DOCSIS Version, QoS Version, First Online Time, Last Registration Time, Service Type ID</p>

Navigation Path	Resource Information Available for Export
Choose Configuration > Access Service Management > Splitter from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > Splitter from the main menu (application style).	Optical splitter information: NE Name, Frame, Slot, Port, Splitter Name, Splitter Alias, Split Ratio, Vendor, Version, Type, Remarks
Choose Configuration > Access Service Management > EoC CNU from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > EoC CNU from the main menu (application style).	EoC CNU information: EoC Terminal Name, Frame, Slot, Port, CNU ID, Name, Alias, Authentication Mode, SN, MAC, Line Profile, Vendor ID, Terminal Style, SoftwareVersion
Choose Configuration > Access Service Management > TDM STM-1 from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > TDM STM-1 from the main menu (application style).	TDM STM-1 port information: Device Name, Name, Alias, Line Status, Transmitting Clock, Loopback Type, Physical Port Type, Optical Port Type, Line Type, Rate, Optical Port Shutdown Status, Tributary Numbering Mode, Port IP
Choose Configuration > Access Service Management > STM-x/OC-x from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > STM-x/OC-x from the main menu (application style).	STM-x/OC-x port information: Device Name, Name, Alias, Type, Line State, Tx Clock, Loopback Type, Physical Port Type, Line Type, Interface Type, Rate
Choose Configuration > Access Service Management > PRI E1/T1 from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > PRI E1/T1 from the main menu (application style).	PRI E1/T1 port information: Device Name, Name, Alias, Loopback Status VoIP ISDN PRA port information: Device Name, Name, Alias, MG ID, Terminal ID, SG ID, Interface ID, Service Configured, TID Layered V5 ISDN PRA port information: Device Name, Name, Alias, V5 Interface ID, EF Address, Port Group No., User Port Configuration

Navigation Path	Resource Information Available for Export
<p>Choose Configuration > Access Service Management > TDMoIP E1/T1 from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > TDMoIP E1/T1 from the main menu (application style).</p>	<p>TDMoIP E1/T1 port information: Device Name, Name, Alias, Line Coding Mode, Clock Type, Frame Mode</p> <p>V5 ISDN PRA port information: Device Name, Name, Alias, V5 Interface ID, EF Address, Port Group No., User Port Configuration</p>
<p>Choose Configuration > Access Service Management > IMA E1/T1 from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > IMA E1/T1 from the main menu (application style).</p>	<p>IMA group information: Device Name, Frame, Slot, Group, E1 Clock Mode, CRC4 Mode, Scramble Mode, Group Block State, Group Loopback State, InterfaceMode, VCSubSpace</p> <p>IMA link information: Link, Tx. Link ID, Rx. Link ID</p>
<p>Choose Configuration > Access Service Management > FE1 from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > FE1 from the main menu (application style).</p>	<p>SDL E1 and HSL E1 port information: Device Name, Name, Alias, Frame Type, Loopback Status</p>
<p>Choose Configuration > Access Service Management > E3/T3 from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > E3/T3 from the main menu (application style).</p>	<p>E3/T3 port information: Device Name, Name, Alias, Type, Line State, Tx Clock, Loopback Type, Physical Port Type, Line Type, Line Coding, Interface Type, Rate</p>
<p>Choose Configuration > Access Service Management > CES V.35 from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > CES V.35 from the main menu (application style).</p>	<p>CES V.35 port information: Device Name, Name, Alias, Clock Type, N Value, Filling Rate, Clock Inverted Status, Blocked Status</p>

Navigation Path	Resource Information Available for Export
<p>Choose Configuration > Access Service Management > HSL V.35 from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > HSL V.35 from the main menu (application style).</p>	<p>HSL V.35 port information: Device Name, Name, Alias, Work Mode, Clock Mode, NValue, Port Model, Active Status</p>
<p>Choose Configuration > Access Service Management > POTS from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > POTS from the main menu (application style).</p>	<p>VoIP PSTN port information: Device Name, Name, Alias, MG ID, Terminal ID, Telephone No., Service Configured, Overload Priority V5 PSTN port information: Administrative Status, Device Name, Name, Alias, V5 Interface ID, L3 Addr., V5.1 TS, Telephone No., Polarity Reversal, User Port Configuration</p>
<p>Choose Configuration > Access Service Management > PVC from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > PVC from the main menu (application style).</p>	<p>P2P PVC/PVP information: Device Name, Name, Alias, Connection Type, PVP/PVC, Tx Traffic Name, Rx Traffic Name, Src. Interface, Src. VPI, Src. VCI, Dest. Interface, Dest. VPI, Dest. VCI</p>
<p>Choose Configuration > Access Service Management > Service Port from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > Service Port from the main menu (application style).</p>	<p>Service port information: Device Name, Name, Alias, Port Type, Interface Info, Service Type, Service Para, Upstream Traffic Profile, Downstream Traffic Profile, VLAN ID, Inner VLAN ID, Max. Learnable MAC Addresses</p>
<p>Choose Configuration > Access Service Management > Native TDM Connection from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > Native TDM Connection from the main menu (application style).</p>	<p>Native TDM connection information: Device Name, Name, Alias, Network Interface Type, Network Interface Info, User Interface Info</p>

Navigation Path	Resource Information Available for Export
Choose Configuration > Access Service Management > VLAN from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > VLAN from the main menu (application style).	VLAN information: Device Name, VLAN ID, Name, Alias, Type, Attribute, Super VLAN ID
Choose Configuration > Access Service Management > MultiCast User from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Access Service > Access Service Management > MultiCast User from the main menu (application style).	Multicast user information: Device Name, Name, Alias, User Configuration Mode, Time of Last Quick Leave, Authority, Max. Online Program, Fast Leave Mode, Log Switch, VPI, VCI, GEM Port

7.13.7 Project Document Statistics Reports

The project document report includes various statistics reports such as NE inventory report, electronic labels, board manufacturer information, clock tracing diagram, timeslot allocation diagram, networking diagram, microwave One-Click acceptance test, hardware report. These reports offer useful data for the project maintenance.

Figure 7-64 Board Manufacturer Information

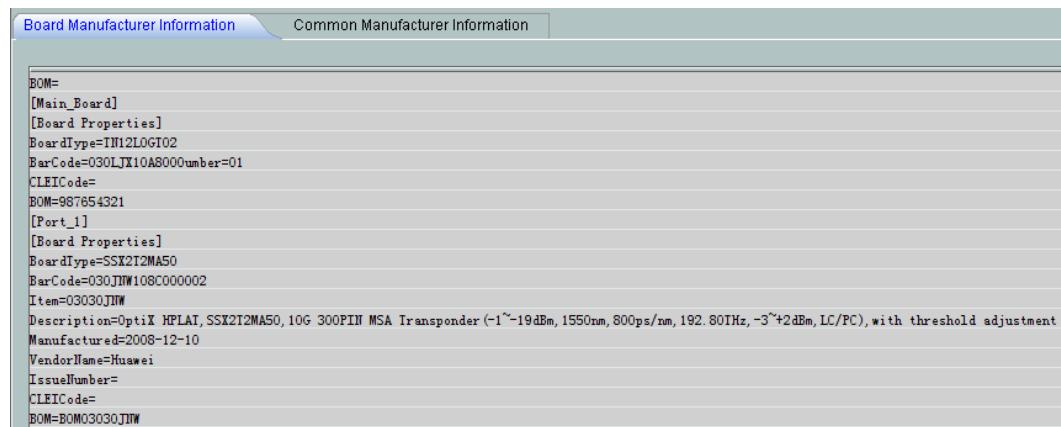


Figure 7-65 Clock Tracing Diagram

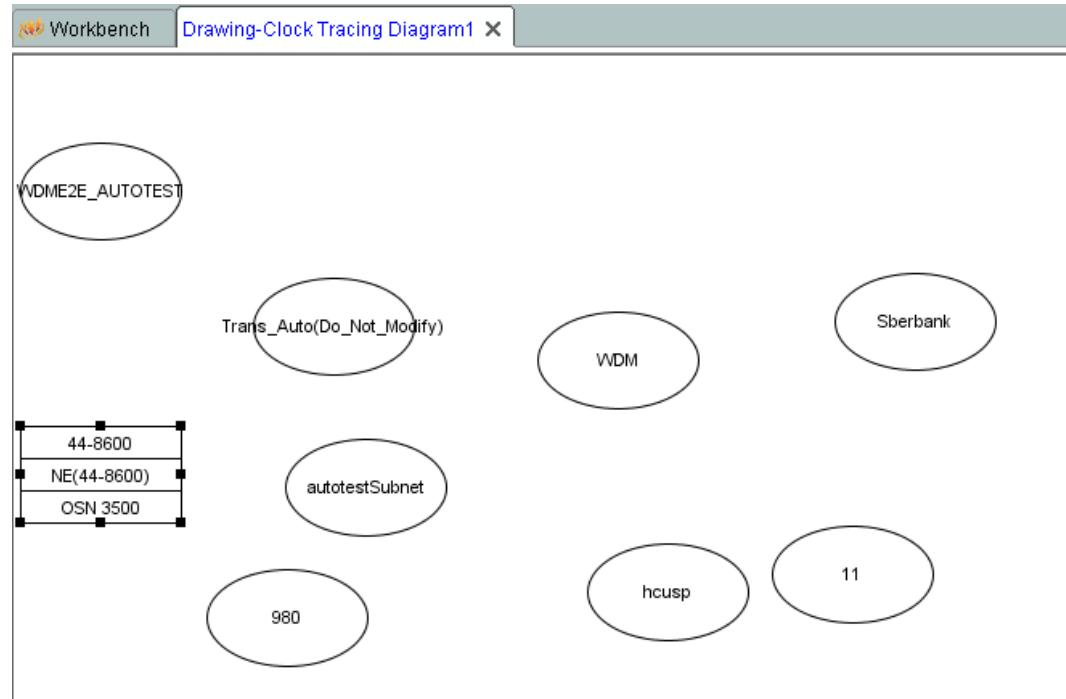


Figure 7-66 Networking Diagram

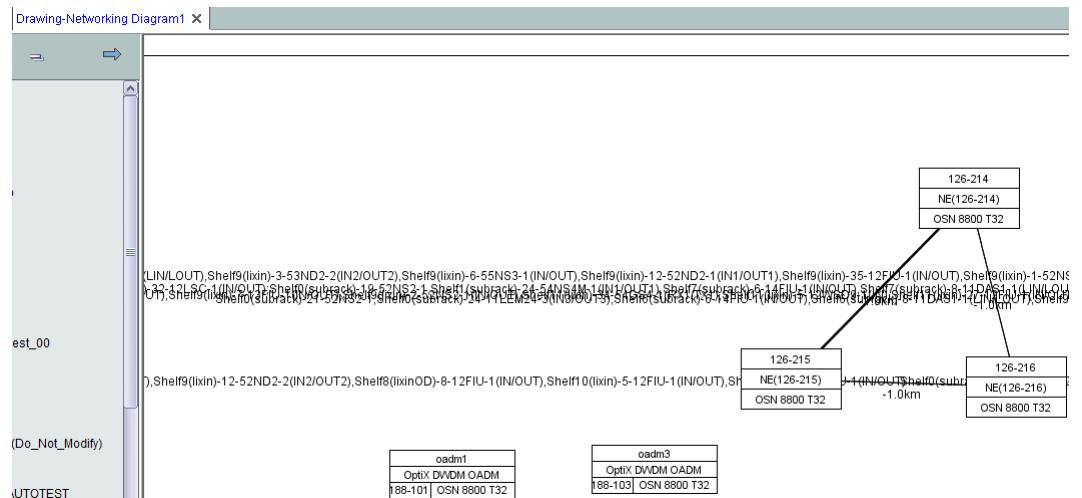


Figure 7-67 One-Click Microwave Link Acceptance Test

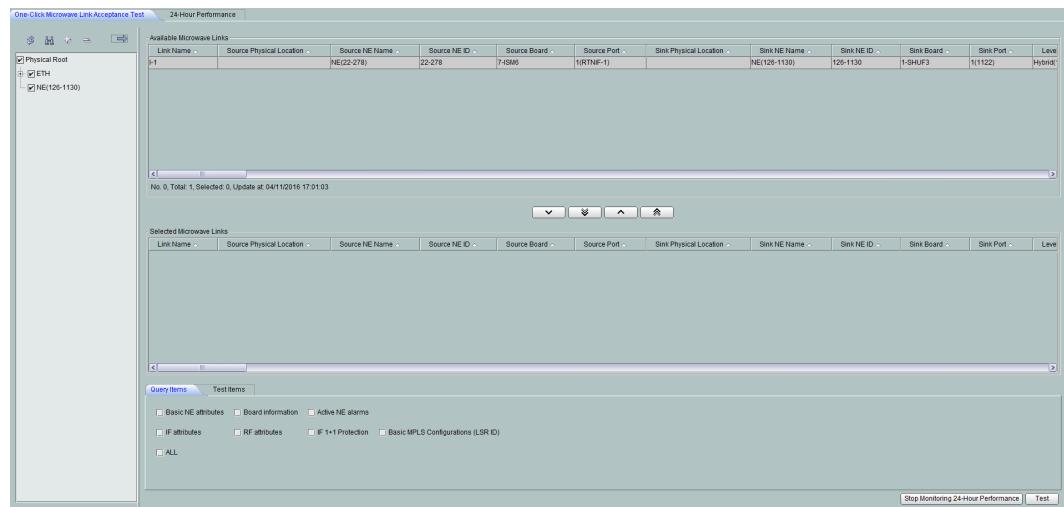


Table 7-17 Project Document Statistics Reports

Report Name	Navigation Path	Statistical Item
Board Manufacturer Information	Choose Inventory > Project Document > Board Manufacturer Information from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Project Document > Board Manufacturer Information from the main menu (application style).	Such as the bar code, type, manufacture date, BOM code, and manufacturer information of the optical module.
Export Electronic Label	Choose Inventory > Project Document > Export Electronic Label from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Project Document > Export Electronic Label from the main menu (application style).	-

Report Name	Navigation Path	Statistical Item
Export NE Inventory Information	<p>Choose Inventory > Project Document > Export NE Inventory Information from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Project Document > Export NE Inventory Information from the main menu (application style).</p>	-
Clock Tracing Diagram	<p>Choose Inventory > Project Document > Clock Tracing Diagram from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Project Document > Clock Tracing Diagram from the main menu (application style).</p>	Such as ID, extended ID, name, equipment type.
Networking Diagram	<p>Choose Inventory > Project Document > Networking Diagram from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Project Document > Networking Diagram from the main menu (application style).</p>	Such as NE name, type, ID, extended ID and fiber or cable length.
Hardware Report	<p>Choose Inventory > Project Document > Export Hardware Report from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Project Document > Export Hardware Report from the main menu (application style).</p>	NE Name, NE IP, NE Type, NE Version, Board Kind Frame, Slot, Board Type, Board Name, Hardware Version, Software Version, Barcode, Board Status

Report Name	Navigation Path	Statistical Item
Timeslot Allocation Diagram	Choose Inventory > Project Document > Timeslot Allocation Diagram from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Project Document > Timeslot Allocation Diagram from the main menu (application style).	-
One-Click Microwave Link Acceptance Test	Choose Inventory > Project Document > One-Click Microwave Link Acceptance Test from the main menu (traditional style); alternatively, double-click Fix-Network NE Configuration in Application Center and choose Inventory > Project Document > One-Click Microwave Link Acceptance Test from the main menu (application style).	-

7.14 System Monitoring

The U2000 provides a GUI-based system monitoring tool, which is used to manage the U2000 and query the system information.

The function of managing system processes enables you to perform the following operations as shown in [Figure 7-68](#).

- Monitor the processes, databases and server information about the U2000 in real time. For the running status of the U2000 server, see [System Information Monitoring](#).
- Start and stop processes automatically or manually.
 - When the U2000 is started, all the processes start automatically.
 - If this process stops abnormally, the U2000 restarts a process automatically only when **Startup Mode** is set to **Automatic**.
 - Processes can be started or stopped manually as needed.
- Shut down the U2000.

Figure 7-68 System monitoring processes

The screenshot shows a software interface titled "System Monitoring". The menu bar includes "File", "Administration", "Window", and "Help". A toolbar below the menu has buttons for "Start All Services", "Stop All Services", "Shutdown OSS", "Refresh", "Settings...", and "Auto Sampling Settings...". The main window displays a table of running processes. The columns are "Process Name", "Process Group", "Description", and "Status". The status column uses green dots to indicate "Running" for most processes, except for a few which have red or yellow dots. The table lists numerous processes such as nemgr_trans_1 through nemgr_trans_4, nemgr_v8pln_1, nemgr_v8trans_1, Nemgr_vmt_1, nemgr_webtrans_1, neproxy, nesvc_v8trans_1, netconproxy, Nml_ason_otn, Nml_ason_sdh, Nml_common, Nml_cps, Nml_eow, Nml_eth, Nml_ip, Nml_nativeeth, Nml_otn, and Nml_sdh.

Process Name	Process Group	Description	Status
nemgr_trans_1	Transmit Basic Service	This process provides the function ...	Running
nemgr_trans_2	Transmit Basic Service	This process provides the function ...	Running
nemgr_trans_3	Transmit Basic Service	This process provides the function ...	Running
nemgr_trans_4	Transmit Basic Service	This process provides the function ...	Running
nemgr_v8pln_1	PTN NE Manager	Provides the NE management func...	Running
nemgr_v8trans_1	Transmit Basic Service	This process provides the function ...	Running
Nemgr_vmt_1	Router NE Manager	Provides the NE management func...	Running
nemgr_webtrans_1	Transmit Basic Service	Provides the Web server manage...	Running
neproxy	Transmit Extended Service	DataCollector Neproxy Process	Running
nesvc_v8trans_1	Transmit SDH Service	This process provides the sdh serv...	Running
netconproxy	Basic Service Group	Provides the proxy function of using...	Running
Nml_ason_otn	Transmit Extended Service	This process provides the OTN AS...	Running
Nml_ason_sdh	Transmit Extended Service	This process provides the SDH AS...	Running
Nml_common	Network Manager	Supports end-to-end common ma...	Running
Nml_cps	Network Management	Supports management of composi...	Running
Nml_eow	Transmit Network Manager	Provides the end-to-end Ethernet s...	Running
Nml_eth	Transmit Network Manager	Supports end-to-end configuration ...	Running
Nml_ip	IP Network Management	Supports end-to-end IP managem...	Running
Nml_nativeeth	Transmit Network Manager	Supports end-to-end configuration ...	Running
Nml_otn	Transmit Network Manager	Supports end-to-end configuration ...	Running
Nml_sdh	Transmit Network Manager	Supports end-to-end configuration ...	Running

System Information Monitoring

The U2000 provides a GUI-based system monitoring function. Users can view the service process status and resource usage (such as the CPU, memory, hard disks, and database) of the U2000 in real time, and learn the running status of all the components installed on the U2000 server.

When items monitored by the U2000 are abnormal, the corresponding status icons turn red. By default, the U2000 sets thresholds for certain monitored items such as the CPU usage and database usage. When a value of the monitored item reaches the corresponding threshold, the system sends an alarm and the corresponding status icon turns red. Users can modify the thresholds if necessary.

The system monitoring tool of the U2000 also provides the following monitoring functions, as shown in the following figure.

- Service Monitor
- Process Monitor
- Hard Disk Monitor
- Database Monitor
- Server Monitor
- Component Information
- Operation Logs
- Session Monitor

Figure 7-69 System monitoring information

The screenshot shows a grid-based interface for monitoring system resources. The columns represent various metrics such as Service Name, Process Name, Process Group, Description, Status, Startup Mode, Start Time, Process ID, Handles, CPU Usage (%), Memory Usage (MB), Database Connections, Threads, File System, Total Space(MB), Used Space(MB), Free Space (MB), Usage (%), Status, Database Name, Total Data Space (MB), Free Data Space (MB), Data Space Usage (%), Total Log Space (MB), Free Swap, Server Name, Server Status, OS, Total Physical Memory (MB), Free Physical Memory (MB), Total Swap Memory (MB), Free Swap, Component, Version, User Name, Operation Name, Operation Time, Client, and Operation Terminal.

Service Name		Process Name		Process Group		Description		Status	Startup Mode	Start Time
DCServer	DCServer	Basic Service Group	Provides the management function...	Running	Automatic	07/05/2016 16:09:47				
DesktopService0101	ds0101_agent	Basic Service Group	Supports data presentation and op...	Running	Automatic	07/05/2016 11:08:39				

Process Name		Process ID	Handles	CPU Usage (%)	Memory Usage (MB)	Database Connections	Threads
BmsAccess_301	3646	105	0.04	472	43		
BmsAccess_401	3649	98	0.05	397	43		

File System		Total Space(MB)	Used Space(MB)	Free Space (MB)	Usage (%)	Status
T5220224122 (Active SunOS5.10)						
/dev/md/dsk/d30(/)	20,170	8,650	11,520	43	Normal	
/dev/md/dsk/d35(/opt/backup)	77,660	17,907	59,753	24	Normal	

Database Name		Total Data Space (MB)	Free Data Space (MB)	Data Space Usage (%)	Total Log Space (MB)	Fr
ason_oth_db	100	85	15	100		
ason_sdh_db	100	84	16	100		

Server Name		Server Status	OS	Total Physical Memory (MB)	Free Physical Memory (MB)	Total Swap Memory (MB)	Free Swap
T5220224122	Active	SunOS5.10	32,640	3,762	42,165		

Component		Version
Fault Management	V300R005C60	

User Name	Operation Name	Operation Time	Client
admin	Log In to the Server	07/07/2016 10:59:37	10.57.117.129

User Name	Operation Terminal
admin	10.57.117.129(Local client)

7.15 Network Management System Maintenance Suite

The network management system maintenance suite (MSuite) is a tool offered by the U2000 for commissioning, deployment, maintenance of HA systems and distributed systems, and database management.

The NMS Maintenance Suite adopts the client/server model, and it is installed automatically when the U2000 is installed.

The NMS Maintenance Suite offers the following functions:

- Managing the NMS: Initialize Database, Change Password, Lock Deploy Client, Log Out and Exit.
- Deploying and maintaining the NMS: Change Database Administrator Password, Change Database User Password, Configure NTP, Deploy and Undeploy.
- Northbound interface (NBI): Configuring CORBA NBI interface, CORBA NBI interface, XML NBI interface, and TEXT NBI interface.
- Managing the database: Backup System Database, Restore System Database.
- Managing certificate file: Internal NMS Certificate, SBI Certificate, U2100 Certificate, Other Certificate and Certificate Validity Period Check.
- Tools: Commissioning Tool and Config Manager.

NTP Scheme

Networking modes are complicated and there are a number of NEs. The NEs on a network use the centralized operation maintenance mode. Therefore, the time of NEs must be consistent so

that the U2000 can correctly manage the alarm and performance data reported by the NEs and data is in order.

The NTP solutions vary according to the schemes adopted in the actual installation and deployment of a U2000. When planning the NTP service, observe the following principles.

- In the scenario where standard external clock sources are available:
 - Single-server system: Configure the U2000 server to function as the NTP time server at the medium level. Configure U2000 clients to function as NTP clients.
 - High availability system: Configure the server on the primary site to function as the NTP time server at the medium level. Configure the server on the secondary site and U2000 clients to function as NTP clients.
- In the scenario where no external clock source is available:
 - Single-server system: Configure the U2000 server to function as the NTP time server at the highest level. Configure U2000 clients to function as NTP clients.
 - High availability system: Configure the server on the primary site to function as the NTP time server at the highest level. Configure the server on the secondary site and U2000 clients to function as NTP clients.

 **NOTE**

- In the Windows OS, the U2000 cannot be configured as the NTP server. If the U2000 is deployed in the Windows OS, the U2000 server and clients all need to be configured as NTP clients to trace the external clock source.
- If NEs are configured as NTP clients to trace the clock of the U2000 server, the running efficiency of the U2000 server is affected. In the scenarios where the U2000 manages lots of NEs, the standard clock source is recommended for tracing.
- The time of the NTP server and the time of an NTP client can be in different time zones and different time. Make sure that the time is consistent with the standard date and time zone of the local area, and that the difference between the NTP server time and the local standard time is less than 2 minutes.

8 Network Feature Configuration and Management

About This Chapter

The U2000 can manage NE features and network features for transport, access, IP and third-party devices in a centralized manner.

NOTE

For details about the configuration and management features, see the latest version of *iManager U2000 V200R016C60 Product Documentation* at <http://support.huawei.com/carrier> for carrier or <http://support.huawei.com/enterprise> for enterprise.

[8.1 MSTP Network Feature Management](#)

This topic describes the functions and features of MSTP NE management and network management.

[8.2 WDM/OTN Network Feature Management](#)

This topic describes the functions and features of WDM NE management and network management.

[8.3 RTN Network Feature Management](#)

This topic describes the functions and features of RTN NE management and network management.

[8.4 PTN Network Feature Management](#)

This topic describes the functions and features of PTN NE management and network management.

[8.5 Router Feature and Switch Feature Management](#)

This topic describes router features and switch features.

[8.6 Security NE Feature Management](#)

This topic describes features supported by security NEs.

[8.7 FTTx Network Feature Management](#)

This topic describes the functions and features of FTTx NE management and network management.

[8.8 D-CCAP Network Feature Management](#)

This topic describes the functions and features of D-CCAP NE management and network management.

[8.9 MSAN Network Feature Management](#)

This topic describes the functions and features of MSAN NE management and network management.

[8.10 DSLAM Network Feature Management](#)

This topic describes the functions and features of DSLAM NE management and network management.

[8.11 BITS/RPS/EDFA Network Feature Management](#)

This topic describes the functions and features of building integrated timing supply (BITS) / remote power system (RPS) / erbium-doped optical fiber amplifier (EDFA) NE management and network management.

[8.12 Third-Party NE Management](#)

The U2000 in the transport and access domains do not support third-party NE management. Only the U2000 in the IP domain supports third-party router management.

8.1 MSTP Network Feature Management

This topic describes the functions and features of MSTP NE management and network management.

8.1.1 MSTP NE Management

NE management consists of the attributes, communications, services, protections, and clock configurations of each NE. The configuration data is stored in the database of the U2000 and the database of the corresponding NE.

Basic NE Configurations

The U2000 supports the following operations:

- Modify NE attributes, including:
 - NE name
 - NE ID
 - Extended NE ID
 - Remarks
 - Preconfiguration attributes
-  **NOTE**
 - NE IDs that need to be set using a DIP switch can be modified on the U2000.
 - When the preconfiguration function is enabled for an NE, all configurations are performed offline on the NE without affecting any services. These configurations will not be applied to the NE but only saved in the U2000 database. This function is mainly used for training, or when the NE has not been physically installed.
- Synchronize NE time: Specify the interval or exact time to automatically align the time of all NEs with the system time of the U2000 server, NTP server, or standard NTP server. You can also set the time and period for automatic NE time synchronization.
 - If you use the scheme of synchronizing with the U2000 server, all NEs use the U2000 server time as the standard time. The NE time can be synchronized with the

U2000 server time manually or automatically. The U2000 server time refers to the system time of the workstation or computer where the U2000 server is located. This scheme features easy operation, and is applicable in networks that require a low accuracy with regard to time.

- If you use the scheme of synchronizing with the NTP server or synchronizing with the standard NTP server, the NE time and the U2000 time are synchronized with the NTP server time or the standard NTP server time automatically. The NTP server can be the U2000 server or a special time server. This scheme enables the U2000 and NEs to have a time accuracy of one nanosecond in theory, and applies to a network with high requirement for time accuracy.
- Display boards in plug-and-play (PnP) mode: After being inserted into slots, boards along with their information are automatically displayed in the NE Panel.
- Perform a change in board type for boards that supports this board replacement function. Functions include:
 - Querying the actual board type of a board that is used as another type of board.
 - Replacing a board with another type of board that has the same rate and same number of ports.
 - Replacing a board with another type of board that has a higher rate or more ports.
- Automatically disable NE functions: NE functions that affect services, such as loopback and automatic laser shutdown (ALS), are disabled at the scheduled time.
- Set environmental monitoring-related parameters, including:
 - PMU interface
 - EMU interface
 - CAU interface
 - TCU interface
 - Temperature attributes
- Manage virtual NEs, including:
 - Creating virtual NEs.
 - Adding boards on virtual NEs.
 - Creating fibers between virtual NEs and other NEs.
 - Creating synchronous digital hierarchy (SDH) services for virtual NEs.
 - Creating protection subnets.
 - Searching for and creating trails that traverse virtual NEs.
- Support the management of inband DCN.
- Graphically display performance events related to optical power.
- Create boards with adjustable bandwidths for preconfigured NEs.
- Support outdoor racks.
- Support auxiliary interfaces.

NE License Authorization

In the **NE License Authorization** window provided by the U2000, you can control the basic functions, enhanced functions, and service access licenses of the TP Assistant, which greatly increases device O&M efficiency.

OSPF Protocol Configuration

The open shortest path first (OSPF) protocol can be used as the network protocol for the U2000.

You can perform the following operations on the U2000:

- Manage the OSPF routing and set relevant parameters.
- Enable or disable port-level OSPF and link state advertisement (LSA).
- Import static routes.

Orderwire Configuration

You can perform the following operations on the U2000:

- Set and query the orderwire phone numbers, call waiting time, and orderwire phone port availability.
- Set and query network-wide conference call numbers.
- Set and query the length of subnet numbers and the related subnet of an optical interface.
- Set and query the SDH network node interface (NNI) orderwire phone numbers.
- Configure or query the F1 data port.
- Configure or query the broadcast data port.

Board Protection Configuration

You can perform the following operations on the U2000:

- Configure board 1+1 protection.
- Configure 1:N tributary protection switching (TPS) protection for a tributary board.
- Configure board-level protection.
- Configure port protection.
- Configure 1+1 IF protection and 1+N IF protection.
- Query the data backup status between the active and standby SCC boards.

SDH Interface Configuration

The U2000 supports the following operations:

- Query and configure SDH interface boards that are installed on NEs.
- Configure SDH interfaces.
- Configure circuit emulation service (CES) interfaces.
- Configure plesiochronous digital hierarchy (PDH) interfaces.
- Modify the optical/electrical attributes of the port on a board.
- Configure overhead interfaces, including:
 - Orderwire phone number
 - Hotline number
 - Special line number
 - Conference call number

- Subnet number length
- F1 data port
- Broadcast data port
- Communication port
- Data port
- Out-ring route
- Configure the interface of an optical amplifier board.
- Manage the optical power of a board.
- Set tone and data access (TDA) interfaces, including:
 - TDA clock source
 - TDA power feeding
- Query and set overhead bytes, including:
 - Regenerator section overhead (J0)
 - Lower-order path overhead (V5, J2)
 - VC4 higher-order path overhead (J1, C2) and its pass-through or termination
 - VC3 higher-order path overhead (J1, C2)
- Support pseudo-random binary sequence (PRBS).
- Support pre-alerts for port optical power.
- Set and query TUG structures in transmit and receive directions.
- Support lower-order loopback.
- Query the port status of line boards and data boards.
- Manage power consumption.
- Set and query the optical power threshold of line boards.
- Support automatic laser shutdown.
- Configuring Service Mapping for an SDH Port: The port mapping function enables the U2000 to mount traditional SDH and packet services on lower-order ODUk trails dynamically and map virtual ports to physical ports.

SDH Service and Protection Configuration

You can perform the following operations on the U2000:

- Configure VC12, VC3, VC4 or 3*AU3 services. For release 4.0 NEs (version 4.bb.cc.dd), selecting protection groups for these services is also supported.
- Manage Transmux services, including M13/E13 Transmux and M13/E13 Transmux Server services.
- Configure VC4-4C, VC4-8C, VC4-16C, or VC4-64C concatenated services; bind or unbind services, and select protection groups for them. For release 4.0 NEs (version 4.bb.cc.dd), selecting protection groups for these services is also supported.
- Configure other services, such as enterprise system connection (ESCON) services, 64 Kbit/s services (including TDA board services, Nx64 Kbit/s services), and DSL services.
- Manage subnetwork connection multiple protection (SNCMP) services.
- Activate or deactivate services.
- Manage subnetwork connection protection (SNCP) services.

- Manage subnetwork connection tunnel protection (SNCTP) services.
- Convert SNCP services to normal services or normal services to SNCP services.
- Configure Ethernet ring protection switching (ERPS): Based on the conventional Ethernet mechanism, ERPS uses the Ethernet OAM function and the ring automatic protection switching (R-APS) protocol to achieve fast protection switching on Ethernet ring networks.
- Configure multiple multiplex section protection (MSP) rings by VC4 at a single optical port, which can increase the network resource usage.
- Configure REG. If REG is configured for a line board on the U2000, each pair of optical ports (receiving port and transmitting port) of the line board provides more functions than normal. With REG, SDH signals received by the receiving port are directly passed through the regeneration section layer, amplified, and then sent to the transmitting port. The whole process is completed on the board alone without any help from the SCC board or a cross-connect board.
- Query the capacity of higher order and lower-order cross-connections of an NE.

ATM Interface, Service, and Protection Configuration

You can perform the following operations on the U2000:

- Manage ATM interface boards, including:
 - Querying ATM interface boards on NEs
 - Configuring ATM interface boards for NEs
- Query bandwidth of ATM boards.
- Set parameters of ATM interfaces.
- Configure ATM traffic.
- Configure ATM cross-connections, including:
 - Creating an SDH NNI on the ATM processing board
 - Configuring ATM cross-connections
 - Configuring ATM protection groups
 - Configuring ATM protection pairs
 - Configuring the same services for SDH boards as those on ATM boards
 - Activating or deactivating ATM cross-connections
- Configure ATM path binding.
- Perform ATM operation, administration, and maintenance (OAM), including:
 - Setting and querying the segment end attributes of a connection point.
 - Setting and querying the activation status of continuity check (CC) at a connection point.
 - Performing a remote loopback test.
 - Setting and querying the loopback location identifier (LLID) of an NE.
 - Uploading, downloading, or copying the NE OAM data or performing a consistency check on the data.
- Configure an inverse multiplexing over ATM (IMA) group.

Ethernet Interface and Service Configuration

The U2000 supports the following operations:

- Query and configure Ethernet interface boards on NEs.
- Configure Ethernet transparent transmission boards that transmit high-rate services.
- Configure Ethernet internal interfaces, including:
 - Basic attributes
 - Tag attributes
 - Network attributes
 - Encapsulation and mapping
 - Link capacity adjustment scheme (LCAS)
 - Bound path
 - Advanced attributes
- Configure Ethernet external interfaces, including:
 - Basic attributes
 - Traffic control
 - Tag attributes
 - Network attributes
 - Advanced attributes
- Configure point-to-point link-state pass through (LPT) or point-to-multipoint LPT.
- Configure or create E-Line services (including Ethernet private line (EPL) services and Ethernet virtual private line (EVPL) services) and configure the bound paths.
- Configure Ethernet private LAN (EPLAN) services: You can create a virtual bridge (VB) and set the following parameters:
 - Service mounting
 - VLAN filtering table
 - VLAN unicast
 - MAC address disabling
 - Bound paths
 - Self-learning MAC address
 - MAC address table capacity of the VB port
 - MAC address table capacity of the VLAN
- Configure Ethernet Layer 2 switching, including:
 - Aging time
 - Spanning Tree Protocol
 - Multiple Spanning Tree Protocol
 - IGMP Snooping Configuration
- Configure QinQ services: QinQ is a VLAN stacking technology that marks users with stacked VLAN tags to expand VLAN resources. You can add, strip, or exchange VLAN tags depending on the scenario.
- Configure Ethernet link aggregation groups (LAGs) that can be divided into intra-board LAGs and inter-board LAGs, including:

- Creating and deleting a LAG.
- Adding and deleting ports to a LAG.
- Querying ports in a LAG and the aggregation status.
- Configure the quality of service (QoS), including:
 - Flow
 - Committed access rate (CAR)
 - Class of service (CoS)
 - Flow shaping
 - Port shaping
 - Port policy of the differentiated service (DiffServ) domain
 - CAR policy
 - Weighted random early detection (WRED) policy of ports
 - V-UNI ingress policy
 - V-UNI egress policy
 - PW policy
 - WRED congestion and discarding policy of services
 - QinQ policy
 - Weighted fair queuing (WFQ) scheduling policy
 - WRR scheduling policy
 - CoS mapping
- Check frame receiving and transmitting on Ethernet boards.
- Query information about the peer NE of a data service.
- Provide a QoS template to simplify the QoS configuration for Ethernet services on a per-NE basis.
- Automatically report RMON performance events on Ethernet boards.
- Dump historical RMON performance events on Ethernet boards.
- Perform protocol diagnoses.
- Enable alarms in the event of no traffic at Ethernet ports.
- Configure Ethernet port mirroring and flow mirroring. In this manner, the product does not resolve or process the captured data.
- Set and query the MAC address of a data board.
- Collect traffic statistics for a port.
- Monitor Ethernet port traffic and generate reports.
- Enable the board to respond to ping commands.
- Create flows in batches.
- Manage multi-protocol label switching Label Switching (MPLS) tunnels. The MSTP equipment sets up a label switched path (LSP) to a PE router, identifies LSP labels and service priorities, and encapsulates LSPs into virtual concatenation groups (VCGs) for transmission.
- Configure the control plane, including static routes and address resolution.
- Manage VPLS services.

RPR Management

You can perform the following operations on the U2000:

- Change the node information for a resilient packet ring (RPR).
- Set or query the node information about an NE in an RPR.
- Set the RPR link information for an NE.
- Query the topology information about the RPR to which an NE belongs.
- Query the protection status, switching status, and switching nodes of the RPR that an NE belongs to.
- Configure switching for the RPR to which an NE belongs, including:
 - Forced switching
 - Manual switching
 - Clearing switching

Ethernet OAM

You can perform the following operations on the U2000 for configuring the 802.1ag Ethernet OAM:

- Create and configure maintenance nodes.
- Perform a CC check.
- Perform a loopback (LB) check.
- Perform a link trace (LT) check.
- Perform performance detection.

You can perform the following operations on the U2000 for configuring the 802.3ah Ethernet OAM:

- Enable OAM automatic discovery.
- Query the peer OAM parameters.
- Notify link events.
- Set link monitoring parameters for detecting frame error events, frame error periods, and frame error seconds.
- Implement remote loopback.
- Implement the reporting of Ethernet OAM loopback events.

Clock Configuration

You can perform the following operations on the U2000:

- Configuration of physical clocks
 - Query the clock synchronization status.
 - Set clock source priority, including:
 - Priority table for system clock sources
 - Priority table for phase-locked sources of the first external clock output
 - Priority table for phase-locked sources of the second external clock output
 - Set clock source switching, including:

- Clock source restoration parameters
- Clock source switching conditions
- Performing clock source switching
- Configure clock subnets, including:
 - Clock subnet
 - Clock quality
 - Synchronization status message (SSM) output control
 - Enable status of clock IDs
- Set phase-locked sources of external clock output, including:
 - Phase-locked sources of external clock output
 - Attributes of 2M phase-locked sources of external clocks
- Configuration of IEEE 1588 clocks
 - Set the selection mode of frequency sources.
 - Set the PTP clock source.
 - Set the quality level of PTP clock sources.
 - Set the priority table of PTP clock sources.
 - Configure a PTP clock service.
 - Configure the clock interface.
 - Set the external clock interface output.
- Configuration of CES ACR clocks

The CES adaptive clock recover (ACR) function, based on CES services, uses the adaptive mode to recover the source clock at the sink. Specifically, the sink equipment can recover the TDM clock (in FIFO mode) according to changes in the buffer for CES services (the buffer changes when receiving packets from the network side). In this manner, clock synchronization can be maintained for services at the sink.
- Unified configuration of clock domains

Network Health Check

- View check reports.
- Run immediately.
- Suspend.
- Timely suspend.
- Timely resume.

Configuration of Hybrid MSTP Service Interfaces

You can configure the general, Layer 2, or Layer 3 attributes for an interface to specify the working mode and application scenario of the interface.

General attributes are physical attributes of the interface. Layer 2 attributes are data link layer attributes of the interface, such as ATM attribute, VLAN attribute, and QinQ attribute. Layer 3 attributes are network layer attributes of the interface, such as the IP attribute.

Table 8-1 lists the Hybrid MSTP service interface types that the U2000 supports.

Table 8-1 Types of Hybrid MSTP service interfaces

Service Interface	Supported Port Mode/ Encapsulation Type	Port Type	Function
SDH interface	General attributes	Physical port	To set general attributes for an SDH interface.
	Advanced attributes	Physical port	To set advanced attributes for an SDH interface.
PDH interface	General attributes	Physical port	To set general attributes for a PDH interface. The PDH interface configured with general attributes can be used to carry TDM services.
	Layer 3 attributes	Physical port	To make a PPP-enabled PDH interface act as a member in a Multilink PPP (MP) group after Layer 3 attributes have been set for the interface.
	Advanced attributes	Physical port	To set advanced attributes for a PDH interface.
Ethernet interface	General attributes	Physical port	To set general attributes for an Ethernet interface.
	Layer 2 attributes	Physical port	To set Layer 2 attributes for an Ethernet interface. The Ethernet interface configured with Layer 2 attributes can be used to carry user-side or network-side Ethernet services.

Service Interface	Supported Port Mode/ Encapsulation Type	Port Type	Function
	Layer 3 attributes	Physical port	To set Layer 3 attributes for an Ethernet interface. The Ethernet interface configured with Layer 3 attributes can be used to carry tunnels.
	Advanced attributes	Physical port	To set advanced attributes for an Ethernet interface.
	Flow Control	Physical port	Indicates the flow control method used by an Ethernet interface in Non-Autonegotiation Flow Control Mode or Autonegotiation Flow Control Mode . Autonegotiation enables information exchange between two connected NEs, fully exerting their capabilities.
Serial interface	General attributes	N/A	To set general attributes for a serial interface.
	Layer 3 attributes	Logical port	To make a PPP-enabled serial interface act as a member in an MP group after Layer 3 attributes have been set for the interface.

Synchronization Protocol Configuration

In the application scenario of dual-homing, the status of the peer equipment needs to be obtained for the MC LAG. Meanwhile, the actions on both sides need to be negotiated based on different fault cases. With the method of adding information of the peer end, a channel is established for control status synchronization with the peer end. In this manner, the control

packets can be transmitted and received through the channel and link fault detection can be performed.

LAG/MC LAG Configuration

A LAG aggregates multiple Ethernet physical links to form a logical link of faster rate for transmitting data. This function improves the link availability and increases link capacity.

The MC LAG supports the ability to share load between aggregation group equipment.

The U2000 supports the ability to set the following LAG/MC LAG attributes:

- Load sharing type, including sharing and non-sharing
- LAG type, including manual and static
- Load sharing hash algorithm of the LAG
- Port priority and system priority of the LAG

LMSP Configuration

Linear MSP protection contains 1+1 linear MSP and 1:N linear MSP. They use the protection channel to protect services that are transmitted on the working channel. When the working channel fails, services are switched to the protection channel. The linear MSP applies to the POS interface and structured STM interface.

The U2000 supports the following functions of LMSP configuration:

- Creates a linear MSP.
- Checks the linear MSP switching status.
- Performs linear MSP switching.

MSTP Configuration

The multiple spanning tree protocol (MSTP) can be used to clear loops on a network. Using an algorithm, the MSTP blocks redundant trails so that the loop network can be trimmed as a non-loop tree network. In this case, broadcast storms caused by the proliferation and endless cycling of packets on the loop network do not occur. Different from the STP and RSTP that use only one spanning tree to correspond to all VLANs, the MSTP introduces the mapping between VLANs and multiple spanning trees, and therefore can forward data according to VLAN packets and achieve load balance of VLAN data.

You can perform the following operations on the U2000:

- Configure parameters of port groups and network bridges.
- Configure CIST and MSTI parameters.
- Query CIST status and MSTI status.

IGMP Snooping Configuration

The Internet group management protocol snooping (IGMP snooping) is a scheme of multicast constraints on Layer 2 equipment, and is used to manage and control multicast groups.

The U2000 supports the configuration of IGMP snooping for E-LAN services, and provides the following operations:

- Configure IGMP Snooping protocol parameters.
- Configure quick leaving ports.
- Manage routes.
- Configure route member ports.
- Query statistics of IGMP protocol packets.

LPT Configuration

LPT is used to return the remote-end link status to the near end. The near-end equipment performs operations depending on the remote-end link status. When the intermediate transmission network of the services becomes faulty, the LPT informs the access equipment at both ends of the transmission network to enable the backup network. This ensures the normal transmission of the important data.

The Hybrid MSTP NEs support configuring point-to-point LPT and point-to-multipoint LPT.

QoS Configuration

QoS indicates the performance of the data flow that travels through a network. The QoS is used to ensure end-to-end service quality. The QoS cannot increase the bandwidth, but it can minimize the delay and jitter in the network by appropriately allocating and monitoring network resources. In this way, the quality of important services is ensured.

The DiffServ (DS) domain consists of a group of network nodes that enable the DiffServ function, that is, DS nodes. In a DS domain, all DS nodes use the same service provision policy to realize the same per-hop behavior (PHB). The DS nodes are classified into edge DS nodes and internal DS nodes. The edge DS nodes usually perform complex flow classification on the traffic that enters the DS domain. Traffic of different types is marked with different PHB service types. For internal DS nodes, you need to perform only simple flow classification based on PHB service type.

The U2000 supports the following QoS functions:

- Configures QoS profiles.
- Configures DiffServ domains.
- Configures ATM CoS mapping.
- Configures simple flow classification and complex flow classification.
- Configures CAR and Shaping.
- Configures the WFQ scheduling policy.
- Configures the port WRED policy.
- Configures the service WRED policy.
- Configures WRR scheduling policy.
- To simplify the operation and share some common QoS configuration parameters, the U2000 supports creating QoS function point policies as follows: port policy, ATM policy, V-UNI ingress policy, V-UNI egress policy, PW policy and QinQ policy. By using these function point policies, you can bind the CAR configuration attribute, shaping configuration attribute, flow classification configuration attributes, WFQ Schedule policy, WRED policy and WRR scheduling policy.
- Configure CoS queue mapping.

- Supports the application of the QoS policy to multiple NEs by configuring QoS profile.

MPLS Tunnel Configuration

MPLS is a type of transmission technology used to transparently transmit data packets between users. The MPLS tunnel is the tunnel defined in the MPLS protocol. Independent from the service, the MPLS tunnel realizes end-to-end transmission and carries the PWs related to the service.

The U2000 supports configuring the following functions of the MPLS tunnel on a per-NE basis:

- Configures general attributes of the MPLS.
- Configures static unicast MPLS tunnels.
- Creates forward and backward MPLS tunnels at the same time.
- Creates static and bidirectional MPLS tunnels.
- Manages PWs.
- Manages tunnel labels and PW labels.

Configuration of the MPLS Tunnel Protection Group

You can perform the following operations on the U2000:

- Create and configure an MPLS tunnel 1+1 protection group and MPLS tunnel 1:1 protection group, including the switching mode, revertive mode, WTR time, and hold-off time.
- Perform MPLS tunnel protection switching.
- Query the switching status of MPLS tunnel protection.

MS-PW Configuration

By creating multi-segment pseudo wires (MS-PWs) to transmit services, you can transmit services over different networks while saving tunnel resources.

PW APS Configuration

As a network protection mechanism, PW automatic protection switching (APS) is intended to protect the services on the working PW with a protection PW. That is, when the working PW is faulty, the services on the working PW are switched to the protection PW. In this manner, the services on the working PW are protected.

You can perform the following PW APS operations on a per-NE basis:

- Create a protection group.
- Bind the master and slave protection pairs.

CES Configuration

CES configuration is mainly used for transparent transmission of TDM circuit switching data on the PSN network.

You can perform the following operations on the U2000:

- Create PWs for a CES service.
- Create UNI-UNI and UNI-NNI CES services.
- Create CES services with the following two modes:
 - Structure-aware TDM circuit emulation service over packet switched network (CESoPSN)
 - Structure-agnostic TDM over packet (SAToP)
- Configure QoS for CES services.
- Configure transparent transmission for CES service alarms.
- Create CES services using either of the following transparent transmission modes: common or SOH.
- Change the tunnel where PWs are carried in in-service mode.

ATM Service Configuration

ATM emulation service is mainly used to transparently transmit ATM services in the PTN.

The U2000 provides the following configuration functions for ATM service creation:

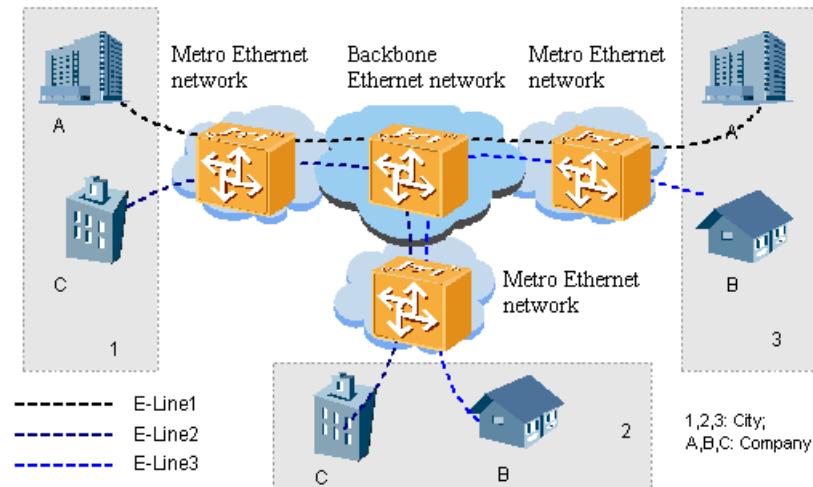
- Create an ATM service with multiple ATM connections.
- Creates UNI-UNI and UNIs-NNI ATM services.
- Create ATM services using one of the following connection types: PVP, PVC, or port transparent.
- Creates PWs for an ATM service.
- Configures IMA groups.
- Configures QoS for ATM services.
- Configures CoS mapping.
- Selects the tunnel that carries PWs without interrupting services.

E-Line Service Configuration

The E-line service is a point-to-point Ethernet service. The equipment transmits user packets from the user side to the network side based on Port or Port+VLAN. In this way, service data can be transparently transmitted in a point-to-point manner.

See [Figure 8-1](#). Company A has branches in City 1 and City 3. Company C has branches in City 1 and City 2. Branches of Company A or Company C that are in different cities have data communication requirements. The Hybrid MSTP equipment can provide E-line services for Company A and Company C, to meet their communication requirements. In addition, the service data can be completely isolated.

Figure 8-1 E-Line Service



The U2000 supports the following functions of configuring E-line services on a per-NE basis:

- Creates UNI-UNI E-Line services.
- Creates UNI-NNI E-Line services that are carried on ports.
- Creates UNI-NNI E-Line services that are carried on PWs.
- Creates UNI-NNI E-Line services that are carried on QinQ links.
- Configures QoS for the PWs of an E-Line service.
- Configures V-UNI groups.
- Selects the tunnel that carries PWs without interrupting services.

E-AGGR Service Configuration

E-AGGR services are multipoint-to-point Ethernet services. The equipment uses several ports to access services from the V-UNI side, and converges the services into one PW at the network side for transmission. In this way, service data from multiple points can be converged into one point.

See [Figure 8-2](#) and [Figure 8-3](#). One carrier wants to construct a 3G network. Services of each Node B are converged and transported to the RNC. The data between each Node B and RNC is regarded as one service. At the convergence point, the QoS parameters such as the overall bandwidth are specified.

Figure 8-2 E-AGGR service scenario 1

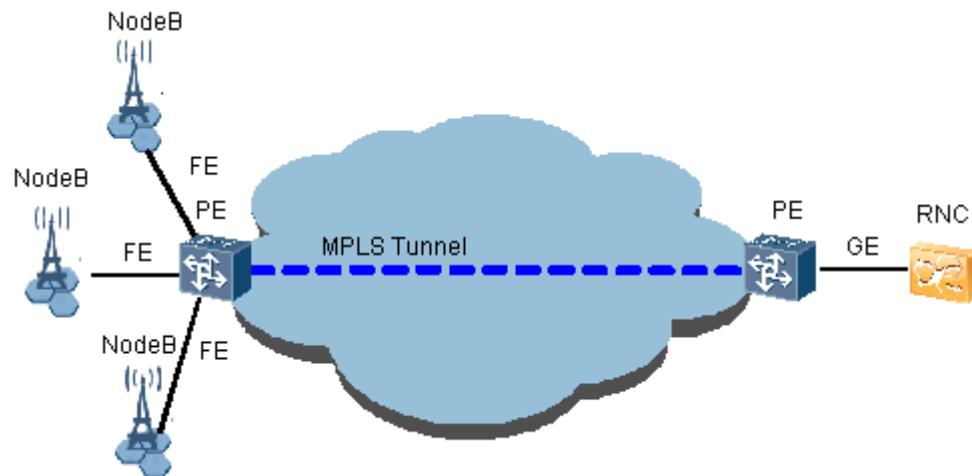
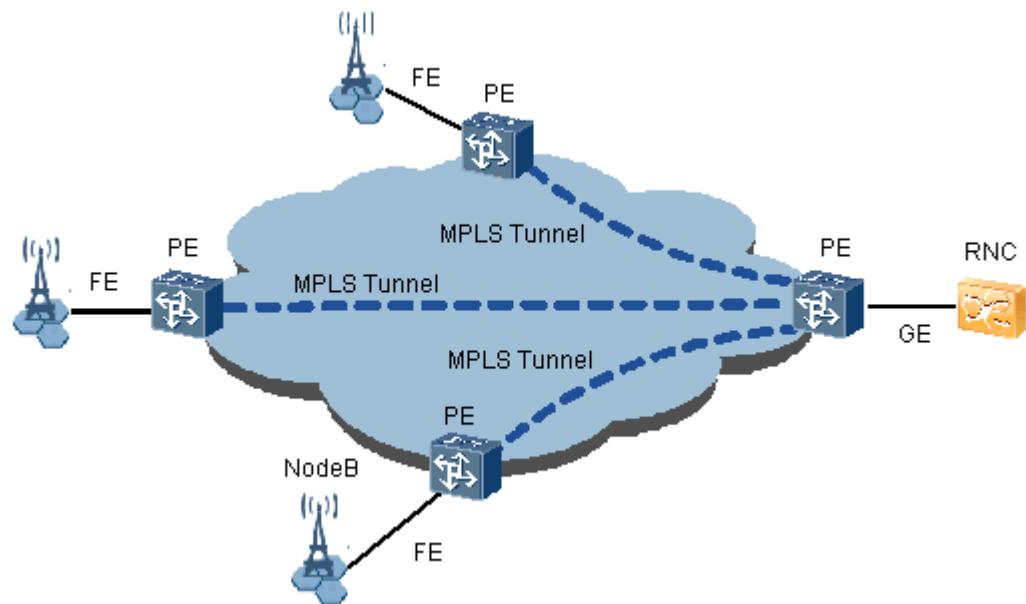


Figure 8-3 E-AGGR service scenario 2



The U2000 supports the following functions of configuring E-AGGR services on a per-NE basis:

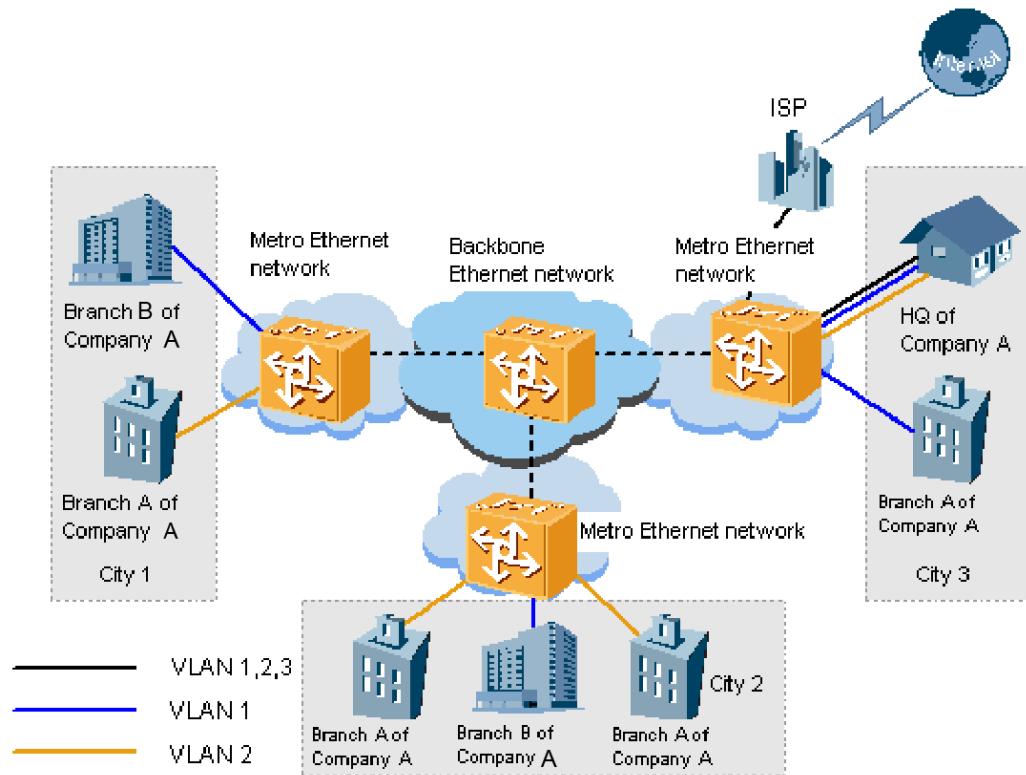
- Configures the VLAN forwarding table items of an E-AGGR service.
- Configures QoS for the PWs for an E-AGGR service.
- Configures V-UNI groups.
- Selects the tunnel that carries PWs without interrupting services.

E-LAN Service Configuration

The E-LAN is a multipoint-to-multipoint Ethernet service. It connects to multiple V-UNI and NNI access points. It realizes packet forwarding and interconnection by using the MAC address self-learning scheme of layer 2.

See **Figure 8-4**. The HQ of Company A is in City 3. Company A has Branch A in City 1, City 2, and City 3, and has Branch B in City 1 and City 2. Branch A and Branch B do not have business with each other. The data should be isolated between the two branches. The HQ has requirements of communicating with each branch and accessing the Internet.

Figure 8-4 E-LAN service



Different VLANs are used to identify service data of different branches by using the E-LAN service. In this way, data is shared within a branch and is isolated from other branches. The Internet data of the HQ is also isolated from the internal service data by using the VLAN.

The U2000 supports the following functions of configuring E-LAN services on a per-NE basis:

- Creates E-LAN services that are carried on port.
- Creates E-LAN services that are carried on QinQ links.
- Creates E-LAN services that are carried on PW.
- Configures QoS for the PWs for an E-LAN service.
- Configures V-UNI and NNI interfaces for an E-LAN service.
- Configures the split horizon group of an E-LAN service.

- Configures V-UNI groups.
- Configures MAC address learning parameters.
- Configures the unknown frame processing mode.
- Configures the static MAC address.
- Configures the disabled MAC address.
- Configures the self-learning MAC address.

MPLS OAM Configuration

MPLS OAM refers to a group of OAM functions that can check the quality of LSPs in an MPLS network. The MPLS OAM scheme can effectively detect, report, and handle a defect inside the network at the MPLS layer in addition to triggering protection switching when a malfunction occurs.

The U2000 provides the following functions of configuring MPLS OAM:

- Configures MPLS OAM parameters of a tunnel.
- Performs tunnel CV/FFD check.
- Performs tunnel ping check.
- Performs tunnel traceroute check.
- Performs PW ping check.
- Performs PW traceroute check.
- Enables or disables the FDI.

ATM OAM Configuration

ATM OAM refers to a group of end-to-end OAM functions that can check the quality of ATM links that pass through multiple NEs. The ATM OAM functions check an ATM link by inserting some OAM cells of the standard cell structure to the user cell flow.

The U2000 provides the following functions of configuring ATM OAM:

- Sets segment end attributes.
- Performs a CC activation test.
- Performs remote loopback.
- Sets LLID.
- Configures ATM alarm transmission

MPLS-TP OAM Configuration

Complying with MPLS-TP standards, MPLS-TP OAM provides the following OAM functions for MPLS-TP networks:

- Checking, discovering, and locating a defect inside the network at the MPLS layer.
- Reporting and handling the defect.
- Triggering protection switching when a fault occurs.

This feature provides the following functions:

- Setting MEP parameters.

- Performing a CC check.
- Performing ping tests.
- Performing traceroute tests.
- Performing LB tests.
- Performing LT tests.
- Checking packet loss ratios and delay.
- Performing LCK and TST tests.
- Setting MIP parameters.

MPLS OAM Switching

This feature provides the following functions:

- Switching OAM recommendations.
- Switching to the OAM dual-stack mode.

Setting SNMP NMS Parameters

When the OSS obtains alarm and performance data from NE over SNMP, you need to configure IP address and permission control parameters of OSS on the U2000.

Query the Core Routing Table

To quickly check whether the communication between the created NE and the gateway NE is normal during deployment in the scenario where hybrid MSTP NEs use in-band DCN protocol for communication.

Setting PCM Interfaces

The SDH equipment on a transport network integrates some pulse code modulation (PCM) interfaces, including FXO and FXS ports and 2-wire/4-wire AF EM interfaces. The main service scenarios are as follows:

- Z interface extension service: FXO and FXS ports work in pairs to implement transparent telephone transmission. Common telephones can connect directly to a private branch exchange (PBX) which extends to NEs with the FXO and FXS ports. Each telephone port occupies a 64 kbit/s E1 channel.
- Hotline service: FXO and FXS ports work in pairs to implement E-Line telephone services. It mainly completes the end-to-end voice communication between stations. Users can communicate with each other by just picking up the phone, that is, no dialing is required.
- 2-wire/4-wire AF EM regeneration: The PBXs are connected to transport NEs through the 2-wire/4-wire + EM interfaces. The EM interfaces transmit signaling and the 2-wire/4-wire ports transmit voice data. The transport NEs act as the regenerators of signaling and voice data.
- End-to-end control signal transmission: EM ports are used independently to transmit connection and disconnection signals through only one channel. In this manner, switch signals are transmitted remotely to implement remote control.

MPLS Ring Protection Management

This feature adds an independent ring layer, which does not affect services. The MPLS ring protection, similar to SDH ring protection, provides reliable protection capabilities to withstand multi-node failures. This feature provides the following functions:

- To discover MPLS rings automatically.
- To view the topology of MPLS rings.
- To refresh and query the protection switching status of MPLS rings.
- To create MPLS protection ring protection.
- To manage MPLS ring protection.
- To delete MPLS ring protection.
- To bind a tunnel to or unbind a tunnel from a protected MPLS ring.
- To unbind multiple tunnels from a protected MPLS ring at a time.
- To diagnose faults on protected MPLS rings.
- To display alarms for protected MPLS rings.
- To configure or delete the intersecting nodes of protected MPLS rings.

Maintaining and Troubleshooting

- IP Ping: In mobile backhaul scenarios, to diagnose a fault, engineers usually must find out on which network the fault occurred. IP ping enable you to preliminarily locate the fault on the transport or wireless network.
- Data Service Performance Test: E-Line service indicators such as the throughput and latency can be tested on the U2000 to avoid costly and inefficient meter tests.

8.1.2 MSTP Protection Subnet Management

A protection subnet is a network structure with comprehensive self-protection. For the U2000, the protection subnet is a generalized concept that covers not only the network structure with comprehensive self-protection, such as multiplex section protection (MSP) rings and path protection (PP) rings, but also the network structure without self-protection, such as unprotected rings and chains.

NOTE

A license is required to perform protection subnet management on the U2000.

The U2000 supports the following operations:

- Create protection subnets of different types, including:
 - Linear MSP such as 1+1 protection and M:N protection
 - MSP rings such as two-fiber bidirectional MS shared protection rings, two-fiber unidirectional MS dedicated protection rings, and four-fiber bidirectional MS shared protection rings
 - PP rings such as two-fiber unidirectional PP rings and two-fiber bidirectional PP rings
 - Dual node interconnection (DNI) protection
 - Unprotected rings and chains
 - SNCTP (Subnetwork Connection Tunnel Protection)

- IF_1+1 protection subnet, IF_N+1 protection subnet
- Search for protection subnets based on NE information and cable/fiber information, to form complete protection subnets.
- Convert the unprotected chain to 1+1 linear MSP without interrupting services.
- Enable or disable the MSP protocol of an MSP protection subnet, including:
 - Enabling or disabling the MSP protocol network-wide.
 - Enabling or disabling the MSP protocol for a single node.
- Automatically generate protection services for a service configured with 1+1 linear MSP.
- Adjust the bandwidth of MSP dynamically without interrupting services based on the actual bandwidth usage and service requirements to use the network bandwidths. For example, if the MSP of an STM-16 covers 8 x VC4 but only 6 x VC4 need protection, in-service bandwidth adjustment can be performed to save 2 x VC4 for services without MSP.
- Expand the capacity of an MSP ring or a linear MSP chain by replacing the line boards on both sides of the ring or chain without interrupting active services. For example, you can smoothly expand the capacity from STM-16 to STM-64 for an MSP ring.
- Modify the revertive mode of linear MSP without re-enabling the protocol.
- Add nodes to protection subnets of the following types: MSP, SNCP, PP, unprotected ring, unprotected chain, and hybrid type.
- Delete or replace nodes within an MSP protection subnet.
- Query the names, types and status of all protection subnets.
- Query or set the switching status, switching mode, wait-to-restore (WTR) time, and trigger condition of a protection subnet.
- Query all the isolated nodes and delete useless nodes.
- Set and view SDH NNIs (Only for release 4.0 NEs, version 4.bb.cc.dd).
- Query trails in a protection subnet. For an SNCTP protection subnet, you cannot query the VC4 server trails that function as working or protection trails in the subnet; only the lower order trails of the working trail can be queried.
- Manage the entire RPR ring network, including:
 - Creating, deleting, or searching for an RPR network.
 - Managing protection parameters of the RPR network.
 - Managing link parameters of the RPR network.
 - Displaying the RPR network in a topology view.
- Generate MSTP protection subnet reports to facilitate statistics collection and maintenance of protection subnets.

8.1.3 MSTP End-to-End Management

End-to-end (E2E) network management is also referred to as trail management. Trail-based configuration can be performed by searching for NE-layer data on the U2000 or by configuring the network-layer data on the U2000; then the configuration is applied to all associated NEs. Trail-based configuration is easier than configuring NE data on a per-NE basis.



A license is required to perform E2E network management on the U2000.

SDH Trail Management

Create the SDH trails, including:

 **NOTE**

For release 4.0 NEs (version 4.bb.cc.dd), a protection subnet and SDH network-to-network interface (NNI) must be created.

- Searching the SDH trails:
 - Performing trail search to generate E2E trails based on the NE configuration data at the NE layer, and the fiber connection data and protection subnet information at the network layer.
 - Switching to the trail management window to query and modify trail details.
 - Retaining the attributes of the existing SDH trails during the search for SDH trails.
- Creating SDH trails, the service levels include VC12, VC3, VC4, Link server trail, VC4 server trail, VC4-4C, VC4-8C, VC4-16C, and VC4-64C.
- Creating unterminated VC4 server trails.
- Creating SNCTP VC4 server trails.
- Creating SDH trails based on the MS-OTN feature.
- Specifying the timeslot and select the protection priority policy and the resource usage policy.
- Using timeslots with the minimum ID for route calculation.
- Setting subnet connection protection (SNCP) attributes such as the revertive mode and signal degrade (SD) trigger condition during SNCP trail creation.
- Creating manually a mono nodal trail and a single-source dual-sink trail whose source and sink are on the same NE.
- Automatically generating the protection service of a dual-fed SDH service configured with 1+1 linear MS protection (MSP).
- Duplicating SDH trails to create SDH trails in batches. Trail names can be changed during the duplication.
- Duplicating SDH trails configured with dual node interconnection (DNI) protection so that SDH trails can be created in batches.

Manage discrete SDH services, including querying discrete services and reverse discrete services, analyzing discrete services, and viewing the source, sink, and cross-connection loss flags of discrete services.

Maintain the SDH Trails, including:

- Filter trails in the following three ways:
 - Filter all: Filter all trails and display only those that meet the criteria.
 - Secondary filter: Filter the displayed trails according to new criteria and display the results.
 - Incremental filter: Filter all trails and display those that meet the criteria together with the trails that are currently displayed.
- Modifying the SDH Trails:
 - Modifying the add and drop ports on a trail and the timeslot occupied by the trail in in-service and manual mode.
 - Adjusting the original route in manual and in-service mode: Change the NE, board or timeslot that the trail passes through.

- Modifying the route for concatenated services in in-service mode.
- Modifying trails in batches that have the same source, sink and service layer trail as the trail being modified.
- Exchanging the source and sink of the trail.
- Upgrading an SDH trail to an ASON trail.
- Downgrading an ASON trail to a traditional SDH trail.
- Converting SDH discrete cross-connections to a mono nodal trail.
- Managing the SDH Trails:
 - Name trails automatically.
 - Activating or deactivating, and locking or unlocking SDH trails.
 - Joining or splitting, and enabling or disabling a VC4 server trail.
 - Querying the service status of SDH trails on a per-NE basis.
 - Managing optical power: Query the input power, output power, and power thresholds on boards of SDH NEs.
 - Setting and querying the overhead bytes on a trail, such as the trace byte, in a unified manner.
 - Prompting users to configure trace bytes when timeslots of a multiplex section (MS) are out of sequence.
 - Querying the status of a lower-order service.
 - Setting overhead pass-through or termination for all NEs on a trail.
 - Inserting alarms into VC4 trails, such as the alarm indication signal (AIS) and remote defect indication (RDI).
 - Setting loopback on any nodes of a trail, including VC4 loopback, tributary loopback, optical(electrical) interface loopback, and cross-connection loopback. The nodes of a trail can be viewed in the signal flow diagram.
 - Implementing the pseudo-random binary sequence (PRBS) on a trail.
 - Deleting SDH trails, VC4 server WorkRouter and ProtectRouter.
 - Setting subnet connection protection (SNCP) switching for a trail.
 - Modifying SNCP services in in-service mode. Delete the working or protection route of a service.
 - Displaying the usage of each VC12 or VC3 trail corresponding to a VC4 server trail in graphical format, and other information about the VC12 or VC3 trails.
 - Browsing the relevant fibers of the SDH trail.
 - Creating platinum service groups and displaying a routing diagram for both services in a platinum service group.
 - Collecting and maintaining SDH trail information statistics in an SDH trail information report.
 - Returning to the primary filter results after a secondary filter.
 - Exporting VC4 server trail information in SDH trail configuration reports.
 - Displaying information about VC3 and VC12 trails carried by VC4 server trails.
 - Analyzing the connectivity of SDH trails and locating faults to SDH trails.
 - Deleting the working route and the protection route of the SNCP-protected VC4 server trail.

- Displaying routes on the Main Topology for an SDH trail.
- Filtering the SDH trails by Protection Status in the Manage SDH Trail window.

Manage alarms and performance events of SDH trails, including:

- Configuring alarm suppression or alarm reversion for the entire trail, configuring the lower order alarm monitoring.
- Querying the following information about an SDH trail: current alarms, historical alarms, current performance data, historical performance data, unavailable time (UAT), and performance threshold-crossing records.
- Switching from an SDH performance event to the SDH trail management window.
- Setting performance parameters of SDH trails.
- Querying the affected SDH trails and customer information of an alarm.
- Displaying R_LOS alarms in the **Transmission Media Layer Route** view.
- Querying the affected SDH trails of a section layer alarm.
- Analyzing the same VC4 timeslots that are used by multiple alarm-affected SDH trails.
- Enabling user-defined trail alarm correlation rules.
- Monitoring SDH trails connectivity in real time.

Ethernet Trail Management

You can perform the following operations on the U2000:

- Create and maintain Ethernet trails.
- Create trunk links at VC12, VC3, VC4, VC4-4C, VC4-8C and VC4-16C levels.
- Create unterminated trunk links.
- Create Ethernet trails of the following types: Ethernet private line (EPL), Ethernet virtual private line (EVPL), unterminated EPL, Ethernet private LAN (EPLAN), EVPL based on QinQ, EVPL based on resilient packet ring (RPR), and Ethernet virtual LAN (EVPLAN) based on RPR.
- Create a protection Ethernet trail that has one source and dual sinks.
- Create an Ethernet trail that traverses multiple VLANs.

NOTE

For release 4.0 NEs (version 4.bb.cc.dd), the SDH NNI must be created on the Ethernet service processing board.

- Activate or deactivate Ethernet trails.
- Retain the attributes of the existing Ethernet trails during the search for Ethernet trails.
- Manage discrete Ethernet services, such as querying and analyzing the discrete services.
- Search for Ethernet trails.
- Filter trails in the following three ways:
 - Filter all: Filter all trails and display only those that meet the criteria.
 - Secondary filter: Filter the displayed trails according to new criteria and display the results.
 - Incremental filter: Filter all trails and display those that meet the criteria together with the trails that are currently displayed.
- Manage alarms and performance events of Ethernet trails, including:

- Querying the affected Ethernet trails and customer information of an alarm.
- Querying current and historical alarms of Ethernet trails.
- Implementing the RMON performance function for Ethernet trails.
- Monitoring Ethernet trails connectivity in real time.

ATM Trail Management

You can perform the following operations on the U2000:

- Create and maintain asynchronous transfer mode (ATM) trails, including:
 - Creating ATM trunk links.
 - Creating ATM trails.
 - Activating or deactivating ATM trails.
 - Managing ATM discrete services, such as querying and analyzing the discrete services.
 - Searching for ATM trails.
- Manage alarms and performance events of ATM trails, including:
 - Querying the affected ATM trails and customer information of an alarm.
 - Querying current and historical alarms of ATM trails.
- Filter trails in the following three ways:
 - Filter all: Filter all trails and display only those that meet the criteria.
 - Secondary filter: Filter the displayed trails according to new criteria and display the results.
 - Incremental filter: Filter all trails and display those that meet the criteria together with the trails that are currently displayed.

Packet Service Management

You can perform the following operations on the U2000:

- Service Trail View Management
 - Queries Layer 2 protocol configuration and status.
 - Performs loopback tests on E-LAN networks.
 - Creates performance monitoring tasks and queries historical and real-time performance data.
- Manage tunnels, including:
 - Creating tunnels based on the static CR protocol.
 - Pre-deploying tunnels.
 - Automatically discovering tunnels.
 - Modifying or deleting tunnels, and filtering tunnels to view the desired tunnels.
 - Viewing the topology in the tunnel management window that displays working routes and protection routes.
 - Viewing the tunnel alarms.
 - Viewing the performance of tunnels.
 - Testing and checking tunnels.

- Diagnosing tunnels.
 - Managing discrete tunnels.
 - Creating, modifying, deleting, and automatically discovering 1+1 or 1:1 tunnel protection groups.
 - Performing protection switching in 1+1 or 1:1 tunnel protection groups manually.
 - Viewing the topology in the window for tunnel protection groups (1+1 or 1:1 protection).
 - Creating a tunnel and its protection tunnel at the same time.
 - Setting and viewing the status of port loopback of tunnels.
 - Configuring OAM.
 - Viewing tunnel names in the global LSP view.
 - Managing bidirectional tunnels.
 - Duplicating static CR tunnels.
 - Viewing lower-layer (Layer 2 link) tunnel alarms.
 - Bulk changing the switching status of tunnels in the tunnel management window.
 - Collecting statistics on the port bandwidth usage.
 - Filtering tunnels by subnet.
 - Viewing actual routing information of static tunnels in the topology view of protection groups.
 - Viewing the correlated services of tunnels.
 - Adjusting the route of a tunnel.
 - Creating static tunnels by means of cloning.
 - Monitoring tunnels.
 - Switching the protection status of tunnels in batches in the tunnel management window.
 - Export tunnel service data from the U2000 to .xls files and import the .xls files containing tunnel service data to the U2000.
- Manage PWE3 services, including:
 - Creating multiple types of PWE3 services such as ATM, CES and Ethernet.
 - Pre-deploying PWE3 services.
 - Automatically discovering PWE3 services.
 - Modifying, deleting, and filtering PWE3 services to view the desired services.
 - Managing multi-hop PWE3 services.
 - Managing PWE3 service protection.
 - Viewing the topology in the PWE3 service management window.
 - Viewing the alarms of PWE3 services.
 - Viewing the performance events of PWE3 services.
 - Testing and checking PWE3 services.
 - Managing discrete PWE3 services.
 - Creating PWE3 services by duplication.
 - Managing PWE3 service templates.

- Automatically generating Ethernet OAM for Ethernet PWE3 services.
- Implementing the loopback function.
- Importing PWE3 service data from and export PWE3 service data to .xls files.
- Performing the one-click continuity check on ATM and CES services.
- Performing the intelligent ETH PWES service fault diagnosis.
- Setting VC12 loopback for CES services.
- Viewing lower-layer (tunnel, Layer 2 link) alarms of PWE3 services.
- Filtering PWE3 services by subnet.
- Migrating PWE3 services.
- Viewing the relative tunnel.
- Monitoring PWE3 services.
- Performing batch protection switchover.
- Implementing bandwidth CAC control.
- Migrating Ethernet PWE3 services based on ports.
- Manage MPLS protection ring, including:
 - Creates/deletes a single protection ring or intersecting rings.
 - Bind/unbind a tunnel to one or multiple MPLS protection rings.
 - Select one or more tunnels and bound the tunnels to rings in batches
 - Views MPLS protection ring alarms.
 - Deletes MPLS protection rings from the network side.
 - Performs MPLS protection ring switchovers.
- Manage linear multiplex section protection (LMSP), including:
 - Discovering LMSP services automatically.
 - Starting or stops the APS protocol.
 - Modifying LMSP information.
 - Performing LMSP switchovers.
 - Deleting LMSP services.
- Manage virtual private LAN services (VPLSs), including:
 - Creating VPLS services.
 - Pre-deploying VPLS services.
 - Automatically discovering VPLS services.
 - Modifying or deleting VPLS services, and filtering VPLS services to view the desired services.
 - Viewing the topology in the VPLS service management window.
 - Viewing the alarms of VPLS services.
 - Viewing the performance of VPLS services.
 - Testing and checking VPLS services.
 - Diagnosing VPLS services intelligently.
 - Managing virtual switch interface (VSI) resources.
 - Managing VPLS service templates.

- Automatically generating Ethernet OAM for VPLS services.
- Setting and viewing the status of port loopback of VPLS services.
- Displaying lower-layer (tunnel, Layer 2 link) alarms for VPLS services.
- Migrating VPLS services.
- Implementing scheduled automatic discovery of VPLS services.
- Manage E-AGGR service, including:
 - Creating E-AGGR services.
 - Pre-deploying E-AGGR services.
 - Automatically discovering E-AGGR services.
 - Modifying or deleting E-AGGR services, and filtering E-AGGR services to view the desired services.
 - Viewing the topology in the E-AGGR service management window.
 - Viewing the alarms of E-AGGR services.
 - Viewing the performance of E-AGGR services.
 - Managing discrete E-AGGR services.
 - Managing E-AGGR service templates.
 - Automatically generating Ethernet OAM for E-AGGR services.
 - Implementing the loopback function.
- Manage composite services, including:
 - Creating composite services:
 - H-VPLS.
 - EPL+L3VPN: This type of composite service is valid only when terminated EPL services use the Hybrid MSTP series NEs, and L3VPN services use routers.
 - EPL+PWE3, PWE3+PWE3.
 - PWE3+E-AGGR.
 - SDH+PWE3: This type of composite service is valid only when SDH services use the Hybrid MSTP series NEs and PWE3 services use PTN NEs.
 - Modifying or deleting composite services, and filtering composite services to view the desired services.
 - Automatically discovering composite services.
 - Viewing the topology in the composite service management window that displays internal connections between composite services.
 - Viewing the status of composite services.
 - Supported jumping to view the service components from composite services.

Native Ethernet Service Management

A license is required to manage end-to-end native Ethernet services on the U2000.

- Create and maintain native Ethernet services, including:
 - Automatically discovering E-Line, E-LAN, and E-Line_E-LAN services.
 - Creating native Ethernet services.

- Managing native Ethernet services.
- Querying E-Line discrete services.
- Converting E-Line discrete services to mono nodal trails.
- Modifying native Ethernet services.
- Performing LM/DM Test on native Ethernet services.
- Querying MAC address learning results of E-LAN services and identifying the MAC address being diagnosed in the topology view.
- Diagnosing E-Line service faults.
- Configuring CEs during native Ethernet service creation and management.
- Verifying VLAN IDs for native Ethernet services, and displaying the service that is occupying the VLAN ID if detecting a VLAN ID conflict.
- Manage native Ethernet service alarms, including:
 - Querying current and historical alarms of native Ethernet services.
 - Querying native Ethernet services affected by an alarm.
 - Displaying alarm status and details for topological nodes in the topology view.
- Filter trails.

Filter all: Filter all trails and display only those that meet the criteria.
- Configure Ethernet OAM.
- Create and maintain the ERPS.
 - Creating ERPS rings.
 - Searching for ERPS rings.
 - Managing ERPS rings.
 - Managing discrete ERPS nodes.

8.1.4 SDH ASON Network Management

An automatically switched optical network (ASON) is a new-generation optical network that integrates switching and transport functions. After a user initiates a service request, the ASON network automatically selects a route. The network then dynamically establishes and removes connections through signaling control. An SDH ASON NE refers to the equipment that has both SDH and ASON features. The U2000 combines ASON and SDH features to perform SDH ASON network management.

You can perform the following operations on the U2000:

ASON Topology Management

- Implement automatic discovery of the ASON network topology and resources.
- Synchronize NEs in the ASON domain: The U2000 can obtain the topology of the ASON domain from an active NE.
- Set NE users and passwords, and implement automatic NE data loading after NEs are added.
- Set active and standby NEs.
- Synchronize cross-connections for NEs.
- Manage domains (including creating and deleting domains and changing domain names).

- Query the ASON NE software version.
- Search for ASON discrete signaling.
- Manage the ASON NE IDs.
- Manage the optical virtual private network (OVPN) status of ASON NEs.
- Query the share risk group (SRG) of an ASON NE.
- Manage the preempt priority status of ASON NEs.
- Manage the large-scale mode of ASON NEs.
- Manage OSPF IP addresses.
- Configure the Global ASON Parameters.

Control Link Management

- Synchronize network-wide control links.
- Filter control links by domain, interface type or source/sink information.
- View control links.
- Query current alarms and historical alarms of control links.
- Set alarm suppression for control links.
- Display color-code alarms in the **SDH Control Link Management** window.
- Print or save control link reports.

Component Link Management

- Synchronize network-wide component links.
- Filter component links by source/sink information.
- View component links.
- Add component links.
- Delete component links.
- Configure ASON resource reservation.
- Query the usage status of VC4 timeslots.
- Query link timeslot segmentation.
- Print or save component link reports.

TE Link Management

- Synchronize network-wide traffic engineering (TE) links by domain and link status.
- Filter TE links by domain, source/sink information, or extended attributes.
- View TE links.
- Create virtual TE links.
- Delete virtual TE links.
- Create fibers.
- Set the length of TE links.
- Set the risk link group number.
- Generate link resource reports.
- View resource usage.

- Allocate TE links to OVPN customers.
- Query alarms of TE links.
- Set alarm suppression for TE links.
- Query the performance of TE links.
- View broken TE links.
- Query SRGs of TE links.
- Set the costs of customizing TE links.
- Query the affected TE links according to control plane alarms.
- Synchronize the fiber length to the TE link distance.
- Query the relevant links, SRGs and ASON trails of the link in the topology view.

ASON Trail Management

- Filter SDH ASON services by domain, name, creator, source, sink, actual route, OVPN customer, original route, shared mesh restoration trail, preset restoration trail, create time, plan time, type, activation status, managed identifier, class, original route is active, ASON trail lock status or remarks.
- Synchronize SDH ASON trails by domain or basic attributes(basic information, working state, SLA-compliant, rerouting properties and associated services).
- View SDH ASON trails.
- View the details of SDH ASON trails.
- Create diamond, gold, silver, or copper SDH ASON server trails.
- Create diamond, gold, silver, copper, or iron SDH ASON trails.
- Set the OVPN customer of an SDH ASON trail.
- Activate or deactivate SDH ASON trails and SDH ASON server trails.
- Delete inactive SDH ASON trails and inactive SDH ASON server trails.
- Delete SDH ASON trails and SDH ASON server trails on the NMS side.
- Duplicate SDH ASON trails.
- Optimize SDH ASON trails.
- Pre-Calculate or optimize the route of SDH ASON trails.
- Set routing attributes of ASON trails, including the rerouting lockout status, revertive lockout status, rerouting priority, revertive mode for rerouting, WTR time, scheduled revertive time, route selection policy, trigger condition, number of crankbacks, rerouting triggered by B3 bit errors, SNCP switching upon SD, maximum hops, longest distance and restore original selective receiving.
- Query the rerouting reversion status of a revertive SDH ASON trail.
- Create associated trails with the same source node or different source nodes.
- Set associations for SDH ASON trails.
- Cancel associations for SDH ASON trails.
- Set the association source for SDH ASON trails.
- Query associated trail.
- Query the associated trails of an SDH ASON trail.
- Set a preset restoration trail for an ASON trail.

- Downgrade an ASON trail to an SDH trail.
- Convert the level of an ASON trail when it is in in-service mode.
- View the actual route, original route, or associated routes of an ASON trail.
- View the preset restoration trail or shared mesh restoration trail of an ASON trail.
- Support reverting ASON trails manually and forcibly.
- Manually switch services on the working trail of a diamond ASON trail to the protection trail and vice versa.
- View alarms of ASON trails.
- Set alarm suppression for ASON trails.
- View the 15 minutes and 24 hours current performance of the trails.
- View the 15 minutes and 24 hours historical performance of the trails.
- View the control plane performance of ASON trails.
- View and set the control plane performance parameters of ASON trails.
- Generate routing tables for ASON trails.
- Refresh the original route, actual route, or associated routes of an ASON trail.
- Refresh the preset restoration trail or shared MESH restoration trail of an ASON trail.
- Set the current route as the original route.
- Restore ASON trails to the original routes in batches.
- Use naming rules and name ASON trails in batches.
- Query the service level agreement (SLA) of ASON trails.
- Display the actual routes of gold services after MSP switching.
- Save settings in the window for creating ASON services after a service is successfully created.
- Restore the default settings of ASON services in the window for creating ASON services.
- Set SNCP access to ASON trails.
- Manage creators of SDH ASON trails.
- Reroute the preset SDH ASON restoration trail that malfunctions.
- Implement automatic route refreshing after the protection switching of diamond trails.
- Set attributes for associated routes of associated ASON trails.
- Create, delete, duplicate, synchronize, activate, and deactivate differentially protected ASON trails. The U2000 cannot associate such trails or convert them without interrupting services.
- Set the maximum unidirectional delay and hold-off time for differentially protected ASON trails.
- Lock or unlock ASON trails.
- Configure FlexP&R protection, including the maximum switching events and maximum rerouting events.
- Query the SDH rerouting history.

ASON Lower-order E2E Service Management

- Back up the lower-order E2E services that use an ASON trail as the server trail.

- Analyze the backup data and current data on U2000, then list the fault lower-order service.
- Recover the lower-order service by backup data.

ASON Clock Subnet Management

- Create an ASON clock subnet.
- Create a preconfigured ASON clock subnet.
- Convert a preconfigured ASON clock subnet to an ASON clock subnet.
- Convert an SDH clock subnet to an ASON clock subnet.
- Manage a hybrid network comprised of ASON clock subnets and SDH clock subnets.
- Manage the start time for ASON clock recovery.

SRG Management

- Create, delete, or modify SRGs.
- Manage the SRGs of pipes, fibers/cables, NEs, sites, or custom SRGs.

Management of One-End Terminated ASON Server Trails

- Create or delete one-end terminated ASON server trails.
- Activate or deactivate one-end terminated ASON server trails.
- Set associations for one-end terminated ASON server trails.
- Create or delete ASON-SDH trails that contain a section of one-end terminated ASON server trail.
- Activate or deactivate an ASON-SDH trail that contains a section of one-end terminated ASON server trail.
- Search for an ASON-SDH trail that contains a section of one-end terminated ASON server trail.
- Set association between the ASON trails that have different sources and sinks.

Combination of SDH and ASON Trails

- Specify a route section for the ASON trail when creating an ASON-SDH trail. The ASON-SDH trail is a combination of SDH trails and ASON trails.
- View SDH and ASON trails in the **Manage SDH Trail** window.
- Manage overhead bytes, alarms, and performance of ASON-SDH trails in a unified manner.
- Query the ASON trails from the related SDH trails.
- Query the SDH trails from the related ASON trails.
- Downgrade an ASON trail to an SDH trail.
- Upgrade an SDH trail to an ASON trail.
- Set revertive attributes when upgrading an SDH trail to an ASON trail.
- Create dual-fed and selectively received VC4 ASON server trails.
- Calculate the working and protection routes using the SPC first policy.
- Collect statistics on alarms of ASON-SDH trails, including alarms on the ASON trails.

- Configure FlexP&R protection when creating ASON-SDH trails.
- Provide FlexP&R protection when upgrading SDH trails to ASON trails.
- Upgrade SDH trails to differentially protected ASON trails.
- Convert traditional trails to ASON trails or ASON trails to traditional trails with the original trail names retained.

Export and Import of Simulated Network Planning

- Export files of and information about simulated network planning to a script, including the network-wide configuration file, NE configuration file, network-layer information file, ASON information file, TE link information, associated ASON service information, route calculation policy for ASON services, component link information, ASON resource reservation information, WTR time information, preset restoration trails, and route calculation policy for nodes.
- Import the script that contains information and files required for simulated network planning.

ASON NE Recovery

If the dual SCC boards of an NE become faulty, or the NE is in the installation status, or the database of the NE is lost, you can restore the data on the NE in the ASON NE recovery wizard.

Quick Single-NE Downgrade

You can quickly downgrade the ASON feature or control plane status of an ASON NE, and all the ASON trails related to the NE.

SDH ASON Management on a Per-NE Basis

- Manage the ASON features of an NE.
- Manage auxiliary ASON function.
- Manage node ID of an ASON NE.
- Manage the ASON features of boards.
- Manage the control plane status of an NE.
- Manage control plane parameters, including the bandwidth usage (%), bandwidth weight, distance weight, hop weight, and custom cost weight. The route selection policy is supported.
- Manage control channels.
- Query LMP component links.
- Query LMP TE links.
- Set the LMP auto discovery mode.
- Manage fiber resource thresholds.
- Query OSPF control links.
- Query OSPF SDH TE links.
- Query OSPF component links.
- Manage OSPF IP addresses.

- Manage OSPF TE link flood thresholds.
- Manage OSPF protocol authentication.
- Manage ASON trail groups.
- Query ASON trails.
- Maintain SDH ASON signaling.
- Maintain SDH ASON switch controllers.
- Maintain ASON shared mesh switch controllers.
- Manage the auto-reporting status of control plane alarms.
- Manage the severities and suppression status of control plane alarms.
- Manage control plane performance parameters.
- Query control plane performance.
- Manage resource reservation.
- Manage the usage status of VC4 timeslots.
- Manage the virtual interfaces of ASON links.
- Manage the inactive PPPoE interfaces.

8.2 WDM/OTN Network Feature Management

This topic describes the functions and features of WDM NE management and network management.

8.2.1 WDM/OTN NE Management

Network element (NE) management consists of attributes, communications, services, protections, and clock configurations of each NE. The configuration data is stored in the database of the U2000 and the database of the corresponding NE.

Basic NE Configurations

You can perform the following operations on the U2000:

- Synchronize NE time: Specify the interval or exact time to automatically align the time of all NEs with the system time of the U2000 server, NTP server, or standard NTP server. You can also set the time and period for automatic NE time synchronization.
 - If you use the scheme of synchronizing with the U2000 server, all NEs use the U2000 server time as the standard time. The NE time can be synchronized with the U2000 server time manually or automatically. The U2000 server time refers to the system time of the workstation or computer where the U2000 server is located. This scheme features easy operation, and is applicable in networks that require a low accuracy with regard to time.
 - If you use the scheme of synchronizing with the NTP server or synchronizing with the standard NTP server, the NE time and the U2000 time are synchronized with the NTP server time or the standard NTP server time automatically. The NTP server can be the U2000 server or a special time server. This scheme enables the U2000 and NEs to have a time accuracy of one nanosecond in theory, and applies to a network with high requirement for time accuracy.

- Query physical inventories, including:
 - Telecommunications rooms
 - NEs
 - Rack
 - Boards
 - Ports
 - Optical module
 - Occupied slot statistics
 - Slot usage status
- Display boards in plug-and-play (PnP) mode: After being inserted into slots, boards along with their information are automatically displayed in the NE Panel.
- Inform users of board replacement by blinking an indicator on the control board.
- If you set **Automatic Disabling of NE Function**, service-affecting operations, such as loopback and ALS, will be automatically disabled after the specified period. When the time for performing a service-affecting operation exceeds a certain period, the operation is disabled automatically.
- Modify the following NE attributes:
 - NE name
 - NE ID
 - NE extended ID
 - Remarks
 - Preconfiguration attributes

 **NOTE**

Long-distance and WDM Metro NEs can be pre-configured. For pre-configured NEs, all configurations on the U2000 are performed in off-line mode. Such configurations bring no impact on services. The configuration data is stored in the database of the U2000 only, not applied to the NEs. The preconfiguration attribute is generally used either in training or when the involved NEs are not in place.

- Modify the following attributes of an optical NE:
 - NE name
 - Remarks
 - Resource allocation
- Set the PMU interface and NE fan speed and monitor the temperature and voltage.
- Set relevant information about network operators, including the international identifier, domestic identifier, and user-defined identifier.
- Search for and create NEs by automatically discovering NE IP addresses.
- When a faulty board is replaced, related indicators on the U2000 will blink.
- View board legends and the meanings of different colors in the NE panel.
- Create the virtual WDM NE to simulate the network NE during the network planning.

NE License Authorization

In the **NE License Authorization** window provided by the U2000, you can control the basic functions, enhanced functions, and service access licenses of the TP Assistant, which greatly increases device O&M efficiency.

Orderwire Configuration

You can perform the following operations on the U2000:

- Set a board as an orderwire board and query the orderwire board information.
- Set and query the orderwire phone numbers, call waiting time, dialing mode, and orderwire phone port availability.
- Set and query network-wide conference call numbers.
- Set and query the length of subnet numbers and the related subnet of an optical interface.
- Set and query the NNI orderwire phone numbers.
- Set and query the F1 data port.
- Set and query the broadcast data port.
- Set E1 cross-connections.

Optical Layer Configuration

- Schedule and manage wavelengths based on ITU-T recommendations.
- Schedule and manage wavelengths based on Flex Grid.
- Configure automatic commissioning at the optical layer for OptiX OSN 1800: The commissioning aims to establish data communication network (DCN) communication between the U2000 and OptiX OSN 1800s, discover the adjacent nodes of each OptiX OSN 1800, and maintain high optical performance of main optical routes.

WDM Board Configuration

You can perform the following operations on the U2000:

- Configure optical transponder units.
- Configure optical multiplexer and demultiplexer boards.
- Configure optical amplifier boards.
- Configure protection boards.
- Configure optical tributary and line boards.
- Configure PID boards.
- Configure spectrum analysis boards.
- Configure optical supervisory channel boards.
- Configure optical add/drop multiplexer boards.
- Configure variable optical attenuation boards.
- Configure automatic optical fiber monitoring boards.
- Configure optical equalization boards.
- Configure dispersion compensation boards.
- Configure wavelength management boards.

Dynamically manage ports.

Query the line rate of the optical transport network (OTN).

You can set channels in batches, including customer information.

Each wavelength channel name supports a maximum of 127 characters, 84 of which can be Japanese characters. (Verification is required.)

Overhead Configuration

You can perform the following operations on the U2000:

Configure OTN overheads.

- Configure and query section monitoring (SM) overheads.
- Configure and query optical transmission section (OTS) overheads.
- Configure and query path monitoring (PM) overheads.
- Configure and query tandem connection monitoring (TCM) overheads.
- Query optical channel payload unit (OPU) overheads.
- Configure and query fault type and fault location reporting channel (FTFL) overheads.
- Configure and query multiframe structure identifier (MSI) overheads.
- Configure and query reserved for future international standardisation (RES) overheads.

Configure WDM overheads.

- Configure optical channel (OCh) overheads at SDH interfaces.
- Configure optical transponder unit (OTU) overheads at OTN interfaces.
- Configure optical demultiplexer unit (ODU) overheads at OTN interfaces.
- Query OPU overheads at OTN interfaces.
- Configure OTS overheads at OTN interfaces.

Configure SDH overheads for the OptiX OSN 8800 series.

- Configure regenerator section overheads (J0).
- Configure lower-order path overheads (V5 and J2).
- Configure VC4 higher-order path overheads (J1 and C2) and pass-through or termination.
- Configure VC3 higher-order path overheads (J1 and C2).

Ethernet Interface and Service Configuration

You can perform the following operations on the U2000:

- Configure the mirroring of Ethernet ports to facilitate packet listening, routine maintenance, and in-service commissioning. In this manner, the product does not resolve or process the captured data.
- Configure internal Ethernet interfaces, including:
 - Basic attributes
 - Flow control
 - Tag attributes
 - Network attributes
 - Bound paths
 - Advanced attributes
 - LCAS

- Configure external Ethernet interfaces, including:
 - Basic attributes
 - Flow control
 - Tag attributes
 - Network attributes
 - Advanced attributes
- Configure E-Line services, such as Ethernet private line (EPL) services, Ethernet virtual private line (EVPL) services (QinQ), and VLAN subnet connection protection (SNCP) services.

 **NOTE**

- QinQ is a VLAN stacking technology that marks users with stacked VLAN tags to expand VLAN resources. Currently, the U2000 can add, split, and exchange VLAN tags.
- A VLAN SNCP service is a VLAN-based E-Line service that is configured with SNCP protection. You can create VLAN SNCP and QinQ VLAN SNCP services, and perform conversion between VLAN SNCP services and common Ethernet services.
- Configure Ethernet private LAN (EPLAN) services: You can create a virtual bridge (VB) and set parameters including service mounting, VLAN filtering, VLAN unicast, MAC address disabling, bound path, and self-learning MAC address.
- Set the quality of service (QoS), including:
 - Flow
 - Committed access rate (CAR)
 - Class of service (CoS)
 - Flow shaping
 - Port shaping
- Configure the link capacity adjustment scheme (LCAS): LCAS can dynamically adjust the number of virtual containers required for service mapping to satisfy bandwidth requirements of different services. In this manner, bandwidth usage and robustness of virtual concatenation are improved.
- Configure OAM for Ethernet services.
- Configure OAM for Ethernet ports.
- Implement the intra-board LAG function.
- Implement the inter-board LAG function.
- Implement the MC-LAG function.
- Implement the VLAN group function.
- Filter port MAC addresses.
- Test frame receiving and transmitting on Ethernet boards.
- Perform protocol diagnoses.
- Configure QinQ type domains.
- Configure Ethernet Layer 2 switching, including:
 - Aging time
 - Spanning tree
 - IGMP snooping protocol

- Configure the multiple spanning tree protocol (MSTP): MSTP is compatible with STP and RSTP and addresses the defects of STP and RSTP. MSTP supports fast convergence. In addition, MSTP provides multiple trails for data forwarding to achieve load balance.
- Configure MPLS tunnels: On a PSN network, an MPLS tunnel carries pseudo wires (PWs) where various services are encapsulated. In this manner, data packets can be transparently transmitted between NEs. You can dynamically adjust the number of virtual containers required for service mapping to satisfy bandwidth requirements of different services. In this manner, bandwidth usage and robustness of virtual concatenation are improved.
- Configure link-state pass through (LPT): LPT is used to return the remote-end link status to the local end so that operations on the local equipment can vary with the remote-end link status. The Ethernet board periodically monitors the network to learn the network condition. When the connection to Ethernet ports changes due to a link failure, the LPT function helps switch services quickly from the working route to the protection route between the two ends; this feature helps ensure that the transmission of important data is maintained.
- Configure Ethernet ring protection switching (ERPS): Based on the conventional Ethernet mechanism, ERPS uses the Ethernet OAM function and the ring automatic protection switching (R-APS) protocol to achieve fast protection switching on Ethernet ring networks.
- Configure ELPS: protection for VLAN-based Ethernet private line services.
- Automatically report RMON performance events on Ethernet boards.
- Dump historical RMON performance data of Ethernet boards.

WDM Service Configuration

You can perform the following operations on the U2000:

Configure ADM for GE/FC services at an optical add/drop multiplexer (OADM) station by using the OTU board.

- Configure several WDM service boards in specified slots to form a cross-connect board group.
- Enable the add/drop, pass-through, and loopback functions for GE/FC services in each cross-connect board group.
- Configure wavelength cross-connection protection (WXCP) with working and protection cross-connections configured on the sink NE.

Configure electrical cross-connections.

- Configure electrical cross-connections, which allows you to control service flow at the electrical layer, and to dynamically groom, converge, or split sub-wavelength services. In this manner, the networking capability and network survivability are greatly enhanced.
- Implement unified grooming based on GE, ODU0, ODU1, ODU2, ODU3, ODU4 and ODUflex services through the XCS board.
- Implement distributed grooming based on GE services, ODU0, ODU1, ODU2, ODU3 and ODU4 services, and Any services.
- Configure unidirectional and bidirectional SNCP at the ODU3, ODU2, ODU1, ODU0, ODUflex and ODU4 level.

Configure optical cross-connections.

- Dynamically create optical cross-connections.
- Manage optical cross-connections on boards and NEs including creating, activating, deactivating, deleting and querying such boards and NEs.
- Create, query, or delete edge ports.
- Configure NE-level optical broadcast services.

Implement transparent transmission for 100GE services.

Manage services.

- Lock WDM trails and display the lock status.
- Display client trails and server trails of a service.
- Query client trails and server trails of a service.

Manage service packages for the OptiX OSN 1800, OSN 6800 and OSN 8800 series. The service package module can complete typical service configurations, which frees engineers from having to perform onsite commissioning and also reduces the costs involved with deployment commissioning and maintenance. In addition, one-click configuration is supported.

Manage licenses controlling the service types and cross-connect capacity for the OptiX OSN 8800 series and OSN 9800 series.

ROADM Configuration

By using the reconfigurable optical add/drop multiplexer (ROADM) function, you can perform add/drop and pass-through configurations for optical channels. The WDM equipment can use the DWC and wave selective switch (WSS) to implement the ROADM function.

- Configure ROADM based on the DWC: Groom wavelengths by using the DWC boards. This mode applies to common nodes on chain and ring networks.
- Configure ROADM based on the WSS, including the WSSD + WSSM and WSS + RMU/ROAM networks. This mode applies to cross-connect nodes on a ring.
- Configure ROADM based on multiplexer and demultiplexer boards: Wavelengths cannot be groomed dynamically. This mode applies to common nodes on chain networks.

Clock Configuration

You can perform the following operations on the U2000:

- Configure a clock source for a board.
- Configure transparent transmission for an external clock.
- Configure a clock for the SCC board, including:
 - Configuring clocks for optical supervisory channel boards
 - Specifying the clock source that the SCC board traces
 - Defining clock source priorities

PTP Clock (IEEE 1588v2 Clock) Configuration

You can perform the following operations on the U2000:

- Configure the frequency source mode.

- Configure PTP clock synchronization attributes.
- Query the clock source received at a port.
- Configure a PTP clock subnet.
- Configure PTP packet attributes.
- Configure an external time interface.

Physical Clock Configuration

You can perform the following operations on the U2000:

- Configure the input attributes of external clock sources.
- Configure the priority table for system clock sources.
- Configure clock source protection and clock source switching.
- Configure phase-locked sources of external clock output.
- Configure the quality of clock sources.

WDM Protection Configuration

You can perform the following operations on the U2000:

- Configure optical line protection.
- Configure extended OLP protection.
- Configure an optical wavelength protection group.
- Configure port protection.
- Configure 1:N ($N \leq 8$) optical channel protection.
- Configure 1+N ($N \leq 48$) optical channel protection.
- Configure protection for clock transparent transmission.
- Configure optical wavelength share protection (OWSP) for the Metro WDM equipment and the NG WDM equipment.
- Configure WXCP protection for GE/FC services, including:
 - Configuring a WXCP protection group for the sink NE
 - Configuring and query WXCP protection
 - Querying the switching status of WXCP protection
 - Querying services with WXCP protection
 - Performing working/protection switching
- Configure a TPS protection group.
- Configure a DPPS protection group.
- Configure board 1+1 protection, including:
 - Configuring 1+1 protection for SCC boards
 - Configuring 1+1 protection for cross-connect and synchronous timing (XCS) boards
 - Performing working/protection switching
 - Querying the switching status
- Configure Client 1+1 Protection.

- Configure SNCP protection, including:
 - Configuring sub-wavelength (SW) SNCP protection for OTU boards with GE services or Any services
 - Configuring SNCP protection for ODUk services
 - Configuring MS SNCP protection
 - Configuring VLAN SNCP protection for Ethernet boards
 - Performing working/protection switching
 - Querying the switching status
- Configure board protection switching (BPS).
- Configure a distribute board protect system (DBPS). The DBPS protects the 10 gigabit Ethernet (10GE) and GE ports on TBE boards. The cross-connection granularity is GE service.
- Configure ODUk SRPing base on ODU1, ODU2, ODU3 and ODU4.
- Query data backup status between the active and standby SCC boards that are configured with 1+1 protection.

Optical Power Adjustment

You can perform the following operations on the U2000:

- Manage the optical power: Query the input power, output power, and power thresholds of each WDM board.
- Perform intelligent power adjustment (IPA): In the event of a fiber cut, the optical amplifier board detects signal loss at the local station. The local station reports an event to the U2000. After the event is confirmed, the optical amplifier boards at the upstream and downstream stations reduce their output power to a safe level to protect fiber maintenance engineers from being injured by the laser emitted from the cut fiber. After the fiber is reconnected, the optical signals are restored and the optical power of each optical amplifier board automatically returns to normal levels.
- Perform automatic level control (ALC): The U2000 supports three adjustment modes, including wavelength count detection, power detection, and link attenuation (gain mode). In wavelength count detection mode and power detection mode, you can manually enable or disable the ALC function.
 - The wavelength count detection mode is applicable to a transmission link where no service is added or dropped or where the number of add wavelengths and drop wavelengths are the same at an OADM station. When the spectrum analyzer unit detects that the total optical power of wavelengths greatly differs from the standard power corresponding to the wavelength count, an event is reported to the U2000. After confirming the event, you need to manually issue a command to adjust the attenuation at each station on the link.
 - The power detection mode is applicable to a transmission link where the number of add wavelengths differs from the number of drop wavelengths at an OADM station. When the optical amplifier board detects that the output power is out of range, the station a command is automatically issued to adjust the attenuation at each station on the link. This mode does not involve a spectrum analyzer unit and is therefore cost-effective.
 - The link attenuation adjustment mode is also applicable to a transmission link where the number of add wavelengths differs from the number of drop wavelengths at an OADM station. When the attenuated optical power reaches the detection

threshold, a command is automatically issued to adjust the attenuation at each station on the link.

 **NOTE**

The link attenuation adjustment mode is also referred to as gain mode, which compares line attenuation with amplifier gain and adopts node gain offset compensation. In this mode, either the nominal gain of the optical amplifier unit or the attenuation of the attenuation adjustment unit is adjusted so that the two values are equal to each other, which maintains the power budget of the entire link.

- Perform automatic power equilibrium (APE). If the optical power of the channels detected by the MCA board at the receive end is abnormal, an event is reported to the U2000. After the event is confirmed, a command is issued to the optical attenuation adjustment board at the upstream station to adjust the optical power of the corresponding channels. In this manner, the optical signal noise ratio (OSNR) of each channel at the receive end is equalized.
- Perform ROADM optical power equalization. After ROADM is enabled to dynamically configure WDM services, the WDM equipment outputs multiplexed wavelengths. The optical power between each channel, however, may be significantly different, especially for new add wavelengths. To avoid negative impacts on transmission performance, the ROADM optical power equalization mechanism is provided. This mechanism first determines whether the wavelengths are pass-through wavelengths or add wavelengths. Then, optical power adjustment starts. The DWC/WSS adjusts the optical power of pass-through wavelengths, while the optical attenuation adjustment board adjusts the optical power of add wavelengths based on wavelength labels.
- Configure pre-alerts for optical power at ports.

Dispersion Compensation

You can perform the following operations on the U2000:

- Perform dispersion compensation with DCM board configured on optical NEs for each band to achieve dispersion equalization.
- Use the tunable dispersion compensator (TDC) to adjust dispersion precisely.
- In the submarine system, use a separate dispersion compensation board, such as the TDC1 or TDC2, to perform dispersion compensation for signals on the line side of an OTU board.

Wavelength Monitoring

On the U2000, you can perform wavelength monitoring for the OptiX BWS 1600G, OptiX OSN 6800, the OptiX OSN 1800 series and the OptiX OSN 8800 series.

WDM PRBS

On the U2000, you can perform pseudo-random binary sequence (PRBS) tests on boards to check the path quality. You can also verify that the WDM link is functioning properly before service provisioning.

SDH Board Configuration

The OptiX OSN 8800 series support SDH line boards. You can perform the following operations on the U2000:

- Configure SDH ports dynamically.

- Adjust the rates of optical ports on SDH boards.
- Query port status.

SDH Service and Protection Configuration

You can perform the following operations on the U2000:

- Configure SDH line boards, SDH services, and SDH service protection for the OptiX OSN 8800 series.
- Configure VC12, VC3, or VC4 services.
- Activate or deactivate SDH services.
- Configure SNCP services.
- Convert SNCP services into common services and vice versa.
- Query the capacities of higher order and lower-order cross-connections.
- Configure subnet connection tunnel protection (SNCTP). SNCTP provides protection channels at the VC4 level. When the working channel malfunctions, all services are switched to the protection channel.
- Configure linear multiplex section protection (MSP). On a chain network, the MSP protection uses bytes K1 and K2 in the SDH multiplex section overhead (MSOH) to transmit protocol information to control the transmit and receive paths of services.
- Configure an MSP ring, including two-fiber bidirectional MSP ring and four-fiber bidirectional MSP ring.
- Configure a transoceanic MSP ring. A transoceanic multiplex section (MS) is based on the transoceanic protocol and provides path protection for higher-order services on the MSP ring.

MPLS Tunnel Configuration

The Multi-Protocol Label Switch (MPLS) protocol allows service packets to transmit transparently. The MPLS tunnel is defined by the MPLS protocol. Independent of services, an MPLS tunnel enables E2E transmission and provides channels for service-related PWs.

You can perform the following operations on a per-NE basis on the U2000:

- Configure basic attributes of the MPLS.
- Configure static unicast MPLS tunnels.
- Create forward and backward MPLS tunnels at the same time.
- Manage PWs.
- Manage tunnel labels and PW labels.

MPLS Tunnel Protection Group Configuration

You can perform the following operations on the U2000:

- Create 1+1 MPLS tunnel protection groups and 1:1 MPLS tunnel protection groups that consist of the switching mode, revertive mode, wait-to-restore (WTR) time, and hold-off time.
- Perform MPLS tunnel protection switching.
- Query the protection switching status of an MPLS tunnel.

MS PW Configuration

By creating multi-segment pseudo wires (MS-PWs) to transmit services, you can save tunnel resources and transmit services over different networks.

PW APS/MC PW APS Configuration

As a network protection mechanism, PW automatic protection switching (APS) is intended to protect the services on the working PW. That is, when the working PW malfunctions, the services on the working PW are switched to the protection PW. In this manner, the services on the working PW are protected.

The following PW APS/MC PW APS functions can be performed on a per-NE basis:

- Create protection groups.
- Bind the master and slave protection pairs.

E-Line Service Configuration

E-Line services are a point-to-point Ethernet service. The equipment transmits user packets from the user side to the network side based on Port or Port+VLAN. Service data can be transparently transmitted in a point-to-point manner.

You can perform the following operations on a per-NE basis on the U2000:

- Create UNI-UNI E-Line services.
- Create UNI-NNI E-Line services through ports.
- Create UNI-NNI E-Line services that are carried on PWs.
- Create UNI-NNI E-Line services that are carried on QinQ links.

E-LAN Service Configuration

The E-LAN is a multipoint-to-multipoint Ethernet service. It connects to multiple V-UNI and NNI access points. It realizes packet forwarding and interconnection by using the MAC address self-learning scheme of layer 2.

Different VLANs are used to identify service data of different branches by using the E-LAN service. In this way, data is shared within a branch and is isolated from other branches. The Internet data of the HQ is also isolated from the internal service data by using the VLAN.

You can perform the following operations on a per-NE basis on the U2000:

- Create E-LAN services that are carried on port.
- Create E-LAN services that are carried on QinQ links.
- Configure V-UNI and NNI interfaces for an E-LAN service.
- Configure the split horizon group of an E-LAN service.
- Configure MAC address learning parameters.
- Configure the unknown frame processing mode.
- Configure the static MAC address.
- Configure the disabled MAC address.
- Configure the self-learning MAC address.
- Implement automatic loopback tests on Ethernet services.

- Enable Ethernet services.

QoS Configuration

Quality of service (QoS) refers to the performance of the data flow transmission in a network. The QoS is used to ensure end-to-end service quality. The QoS cannot enhance the bandwidth, but it can minimize the delay and jitter in a network by properly allocating and monitoring network resources. In this way, the service quality is ensured.

The DiffServ (DS) domain consists of a group of network nodes with the DiffServ function. Nodes of this type are also called DS nodes. In a DS domain, all DS nodes adopt the same service provisioning policy to achieve the same per-hop behavior (PHB). DS nodes are classified into edge DS nodes and internal DS nodes. Edge DS nodes usually perform complex flow classification on the traffic that enters the DS domain. Traffic of different types is marked with different PHB service types. Internal DS nodes only need to perform simple flow classification based on PHB service types.

You can perform the following operations on the U2000:

- Configure QoS templates.
- Configure Diffserv domains.
- Configure ATM CoS mapping.
- Configure simple flow classification and complex flow classification.
- Configure shaping.
- Configure port WRED policies.
- Configure port V-UNI ingress policies.
- Configure WRR scheduling policies.
- Apply QoS policies to multiple NEs by configuring QoS templates.

MPLS-TP OAM Configuration

Complying with MPLS-TP standards, MPLS-TP OAM provides the following OAM functions for MPLS-TP networks:

- Check, discover, and locate a defect inside the network at the MPLS layer.
- Report and handle the defect.
- Trigger protection switching when a fault occurs.

This feature provides the following tunnel and PW functions:

- Set MEP parameters.
- Perform a CC check.
- Perform ping tests.
- Perform traceroute tests.
- Perform LB tests.
- Perform LT tests.
- Check packet loss ratios and delay.
- Set MIP parameters

Energy Consumption Management

Managing NE energy consumption to conserve energy and protect the environment without affecting the proper operation of NEs:

- Query energy consumption of boards and NEs.
- Configure energy-saving functions for NEs. You can dynamically adjust NE energy consumption to conserve energy and protect the environment.
- View network-wide NE energy consumption reports.

Submarine Cable Line Management

Managing submarine cable line on the U2000:

- Create unidirectional or bidirectional submarine cable lines.
- Modify unidirectional or bidirectional submarine cable lines.
- Manage underwater devices.
- Activate unidirectional or bidirectional submarine cable lines.
- Delete unidirectional or bidirectional submarine cable lines.

Submarine Cable Line Monitoring

U2000 supports submarine line monitoring, you can monitor and test the status of fibers and repeaters, and analyze test data for status monitoring and fault locating in a submarine system. You can perform the following operations on the U2000:

- Monitor the status of submarine lines and repeaters without interrupting services.
- Locate faults quickly.
- Locate faults on submarine lines for interrupted services.
- Perform a variety of tests, including manual tests, comparison tests in single-test mode, and comparison tests in periodic mode.
- Synchronize, query, and analyze test data.
- Refresh monitoring information in real time.
- Query the gain report and event report.
- Monitor forward and reverse submarine cable lines at the same time.
- Query the testing status of local and peer NEs.
- Query the submarine cable line diagram.

Submarine Line Terminal Equipment Management

- Support configuring NE basic attributes:
 - Search for and create NEs by automatically discovering NE IP addresses.
 - Synchronize NE time.
 - Implement automatic disabling of NE functions.
 - Query physical inventories.
 - Modify NE attributes.
- Support extended C-band and 25 GHz channel spacing (at the rate of 10 Gbit/s).
- Support alarm cascading and signal control in the same rack.

- Support configuring orderwire.
- Support configuring WDM Services: implement unified grooming based on SDH service, Ethernet services, ODUk services.
- Support configuring overheads:
 - Configure WDM overheads: including OCh overheads, OTU overheads, ODU overheads, OPU overheads.
 - Configure OTN overheads: including PM overheads, TCM overheads, FTTL overheads, SM overheads, OPU overheads.
- Support configuring WDM protection:
 - Configure optical line protection.
 - Configure extended OLP protection.
 - Configure inter-board wavelength protection.
 - Configure inter-shelf 1+1 optical channel protection.
 - Configure 1+1 wavelength protection on the client.
 - Configure 1:N optical channel protection.
 - Configure 1+N optical channel protection.
 - Configure ODUk SNCP.
- Support configuring IPA.
- Support configuring APE.
- Support configuring LPT.
- Support configuring PRBS test.

Submarine Network View Management

You can manage the following resources in the submarine network view:

- Sites
- Repeaters
- Cable terminal box (CTBs)
- BUs
- Submarine cables
- Submarine cable lines
- Cables
- Power supply devices

You can import locations of nodes and submarine devices into the U2000 in the form of a project document.

You can diagnose submarine faults quickly.

BU Management

You can perform the following operations on the U2000:

- Create BUs.
- Maintain BUs.

- Switch power supply over BUSs.
- Delete BUSs.

FC Service Test

You can perform FC service tests on the U2000 with the 12LOM board, instead of the FC test instrument (such as the SmartBits). By performing such tests, you can determine whether FC service lines and the devices under test are working properly.

OSN 9800s service management enhanced

- MPLS-TP section OAM is supported.
- Help information is clear and easy to obtain. The meanings and value ranges of parameters are directly displayed in GUIs.
- Functions included in NE software packages are directly loaded to the U2000, eliminating the need for adaptation to new functions and realizing plug-and-play (PnP).
- The names, probable causes, and handling suggestions of alarms are directly displayed in GUIs.
- power sourcing equipment (PSE) can be managed.
- The light-weight and space-saving Web-based client is available.
- Through a combination of trees and tables, users can add objects quickly without switching a lot. Scenario-specific configurations are provided to centralize function operations in one GUI.
- Supports auxiliary alarm.
- Supports alarm performance templates.
- Supports board-level service encryption.
- Supports SNCP bidirectional switching.

OTN Board Replacement

The wizard helps you securely and quickly adjust or add boards.

- **Adjusting boards:** You only need to select the board to be replaced and specify the type and slot of the replacement board. The U2000 automatically modifies and configures related data (on itself and on NEs). The replacement board must provide more ports and larger capacity than the replaced board or must be located in a different slot.
- **Adding boards:** You can add optical-layer boards to NG WDM NEs to expand the NE capacity. You only need to specify the type and slot of the board to be added. The U2000 automatically modifies and configures related data (on itself and on NEs).

8.2.2 WDM/OTN NE (NA) Management

NE management consists of the attributes, communications, services, protections, and clock configurations of each NE. The configuration data is stored at the NE layer on the U2000 and in the database of the corresponding NE.

Basic NE Configurations

The U2000 supports the following operations:

- Synchronize NE time: Specify the interval or exact time to automatically align the time of all NEs with the system time on the U2000 or NTP server.
- Query physical resources, including:
 - NEs
 - Board manufacturer information
 - Boards
 - Subracks
 - Telecommunications rooms
- Display boards in plug-and-play (PnP) mode: After being inserted into slots, boards along with their information are automatically displayed in the NE Panel.
- Automatically disable NE functions: NE functions that affect services, such as loopback and automatic laser shutdown (ALS), are disabled at the schedule time.
- Modify NE attributes, including:
 - Setting NE name
 - Entering remarks
 - Enabling or disabling automatic board installation
 - Enabling or disabling LAN port access control
 - Setting start time for 24-hour performance monitoring
 - Enabling or disabling the daylight saving time (DST)
 - Modifying the IP address and subnet mask of an NE
 - Enabling or disabling the address resolution protocol (ARP) proxy
 - Enabling or disabling the open system interconnection (OSI) protocol
 - Modifying subrack names
 - Modifying the remarks of subracks
 - Setting the time zone and DST
 - Cold resetting or warm resetting an NE
 - Resetting an NE in the DBERASE mode, with the NE database erased
 - Resetting an NE in the SWDL mode after the NE software is downloaded
 - Enabling or disabling performance reporting
 - Enabling or disabling alarm reporting
 - Enabling or disabling database changed (DBCHG) reporting
 - Clearing audible and visual alarm indicators on an NE rack
 - Setting NE alarm delay, including the delay for alarm-start events and the delay for alarm-end events
 - Setting the longitude and latitude of an NE
 - Setting gateway IP addresses
 - Setting gateway ports
 - Setting the state model of an NE
 - Setting the country code and national segment code of an NE
 - Enabling or disabling the buzzer of an NE
- Modify attributes of optical NEs, including:

- Type
- Name
- Remarks
- Vendor
- Resources allocated to optical NEs
- Query and modify parameters in the window of board attributes, including:
 - Setting the status to active or standby
 - Querying the logical and physical boards of an NE
 - Querying the PCB version, software version, FPGA version, and BIOS version
 - Querying the CLEI code, vendor ID, part number, serial number, manufacturer information, and board description
 - Querying the backup power and rated power voltage
 - Setting the upper and lower temperature thresholds and the current temperature
 - Setting the fan speed, working mode, and LED state
 - Cold resetting a board
 - Warm resetting a board
- Modify environmental monitoring information. You can set the NE fan speed mode and speed level.
- Manage fibers and cables, including:
 - Viewing fiber and cable information
 - Adding or deleting a fiber or cable
 - Generating a fiber/cable report
- Dynamically add, delete, or modify a port: You can dynamically add, delete, or modify an SFP/XFP client-side colored port and then perform operations related to fiber connections, optical cross-connections, and client-side 1+1 protection.
- Search for and create NEs by discovering their IP addresses automatically.

Orderwire Configuration

You can perform the following operations on the U2000:

- Set and query orderwire phone numbers, and call waiting time.
- Set and query network-wide conference call numbers.
- Set and query the length of subnet numbers.

Board Attribute Management

You can perform the following operations on the U2000:

- Set the status to active or standby as presented in the form of PST-PSTQ and SST.
- Query the logical and physical boards of an NE.
- Query the PCB version, software version, FPGA version, and BIOS version.
- Query the CLEI code, vendor ID, part number, serial number, manufacturing data, and board description.
- Query the backup power and rated power voltage.

- Set the upper and lower temperature thresholds and the current temperature.
- Set the fan speed, working mode and LED state.
- Cold reset a board.
- Warm reset a board.

Ethernet Interface and Service Configuration

You can perform the following operations on the U2000:

- Configure Ethernet port mirroring. You can monitor packets, perform routine maintenance and in-service commissioning through a mirrored port. In this manner, the product does not resolve or process the captured data.
- Configure the internal ports of an Ethernet interface, including:
 - Basic attributes
 - TAG attributes
 - Network attributes
 - Advanced attributes
 - Flow control attributes
- Configure the external port of an Ethernet interface, including:
 - Basic attributes
 - Flow control attributes
 - TAG attributes
 - Network attributes
 - Advanced attributes
- Configure Ethernet private line (EPL) services, Ethernet virtual private line (EVPL) (QinQ) services, and VLAN subnet connection protection (SNCP) services.

NOTE

- QinQ is a VLAN stacking technology that marks users with stacked VLAN tags to expand VLAN resources. Currently, the U2000 supports only the function of adding VLAN tags.
- A VLAN SNCP service is a VLAN-based E-Line service that is configured with SNCP protection. You can create VLAN SNCP and QinQ VLAN SNCP services, and perform conversion between VLAN SNCP services and common Ethernet services.
- Configure Ethernet private LAN (EPLAN) services: You can create a virtual bridge (VB) and set parameters including service mounting, VLAN filtering, VLAN unicast, MAC address disabling, bound path, and self-learning MAC address.
- Configure QoS, including:
 - Flow
 - Committed access rate (CAR)
 - Class of service (CoS)
 - Port shaping
- Configure OAM for Ethernet services.
- Configure OAM for Ethernet ports.
- Implement the intra-board LAG function.
- Implement the DLAG function.

- Implement the VLAN group function.
- Filter port MAC addresses.
- Test frame receiving and transmitting on Ethernet boards.
- Perform protocol diagnoses.
- Configure QinQ type domains.
- Configure Ethernet Layer 2 switching, including:
 - Aging time
 - Spanning tree
 - IGMP snooping protocol
- Automatically report RMON performance events on Ethernet boards.
- Dump historical RMON performance data of Ethernet boards.

WDM Board Configuration

You can perform the following operations on the U2000:

- Configure optical transponder boards.
- Configure service multiplexer and demultiplexer boards.
- Configure tributary and line boards.
- Configure protection boards.
- Configure optical amplifier boards.
- Configure spectrum analysis boards.
- Configure optical supervisory channel boards.
- Configure optical add/drop multiplexer boards.
- Configure variable optical attenuation boards.
- Configure optical equalization boards.
- Configure wavelength monitoring boards.
- Configure optical equalization boards.

Overhead Configuration

You can perform the following operations on the U2000:

- Configure and query section monitoring (SM) overheads.
- Configure and query path monitoring (PM) overheads.
- Configure and query tandem connection monitoring (TCM) overheads.
- Query optical channel payload unit (OPU) overheads.
- Configure and query fault type and fault location reporting channel (FTFL) overheads.
- Configure and query multiframe structure identifier (MSI) overheads.

You can perform the following operations on the U2000:

- Configure overheads at the OCh overhead management-SONET interface.
- Configure OTU overheads at the OCh overhead management-OTN interface.
- Configure ODU overheads at the OCh overhead management-OTN interface.

- Configure OPU overheads at the OCh overhead management-OTN interface.
- Configure TCM overheads at the OCh overhead management-OTN interface.
- Configure OTS overheads at the OCh overhead management-OTN interface.

WDM Service Configuration

At an optical add/drop multiplexer (OADM) station, you can configure ADM for GE/FC services by using the LQG, LOG, and other boards.

- Configure several WDM service boards in specified slots to form a cross-connect board group.
- Enable the add/drop, pass-through, and loopback functions for GE services in each cross-connect board group.
- Configure wavelength cross-connection protection (WXCP), with working and protection cross-connections configured on the sink NE.

Configure electrical cross-connections. The U2000 allows you to configure electrical cross-connections to control service flow at the electrical layer. In this manner, the networking capability and network survivability are greatly enhanced.

- Implement unified grooming based on GE, ODU0, ODU1, ODU2, ODU3, ODU4 and ODUflex services through the XCS board.
- Implement distributed grooming based on GE services, ODU0, ODU1, ODU2, ODU3 and ODU4 services, and Any services.

Deploy the ODUflex, ODU4, ODU3, ODU2, ODU1, ODU0, GE, and Any services and OTU1 cross-connections; configure unidirectional and bidirectional SNCP at the ODU0, ODU1, ODU2, ODU3, ODU4, and ODUflex levels.

Configure optical cross-connections.

- Dynamically create OCh cross-connections.
- Manage optical cross-connections on boards and NEs (including creating, activating, deactivating, deleting and querying such boards).
- Create edge ports.

Manage services.

- Lock WDM trails and display the lock status.
- View client and server trails of a service.
- Query client trails and server trails of a service.

ROADM Configuration

By using the reconfigurable optical add/drop multiplexer (ROADM) function, you can perform add/drop and pass-through configurations for optical channels. The WDM equipment uses the DWC and WSS to implement the ROADM function.

- Configure ROADM based on the DWC. This mode applies to common nodes on chain and ring networks.
- Configure ROADM based on the WSS. This mode applies to cross-connect nodes in a ring to groom multi-dimensional optical cross-connections. A maximum of eight dimensions are supported.

Optical cross-connection broadcast services: Support broadcasting optical cross-connections on a per-NE basis.

WDM Protection Configuration

You can perform the following operations on the U2000:

- Configure 1+1 optical channel protection.
- Configure 1:N optical channel protection.
- Configure inter-subrack protection.
- Configure port protection, including:
 - Configuring optical line protection
 - Configuring intra-board 1+1 protection: This function includes the intra-board 1+1 protection realized by the dual-fed OTU board and the intra-board 1+1 protection realized by the DCP or OLP board
 - Configuring client-side 1+1 protection
- Configure protection for clock transparent transmission.
- Configure OWSP protection.
- Configure WXCP protection for GE/OTU1 services, including:
 - Configuring the WXCP protection group for the sink NE
 - Configuring and querying the WXCP protection parameters
 - Querying the switching status of WXCP protection
 - Querying services configured with WXCP protection
 - Performing WXCP protection switching
- Configure board 1+1 protection, including:
 - Configuring 1+1 protection for SCC boards
 - Configuring 1+1 protection for cross-connect and synchronous timing (XCS) boards
 - Configuring AUX board 1+1 protection
 - Performing working/protection switching
 - Querying the switching status
- Configure SNCP protection, including:
 - Configuring sub-wavelength (SW) SNCP protection for OTU boards with GE services or Any services
 - Configuring SNCP protection for ODUk services
 - Configuring VLAN SNCP protection for Ethernet boards
 - Performing working/protection switching
 - Querying the switching status
- Configure board protection switching (BPS). The BPS protection involves two boards, a working board and a protection board. This function providing protection for all ports by performing board-level protection switching.
- If 1+1 protection is configured for SCC boards, you can query the data backup status between the active and standby SCC boards.

Optical Power Adjustment

You can perform the following operations on the U2000:

- Manage the optical power: Query the input power, output power, and power thresholds of each WDM board.
- Perform intelligent power adjustment (IPA): In the event of a fiber cut, the optical amplifier board detects signal loss at the local station. The local station reports an event to the U2000. After the event is confirmed, the optical amplifier boards at the upstream and downstream stations reduce their output power to a safe level to protect fiber maintenance engineers from being injured by the laser emitted from the cut fiber. After the fiber is reconnected, the optical signals are restored and the optical power of each optical amplifier board automatically returns to normal levels.
- Perform automatic level control (ALC): The U2000 link attenuation (gain mode) as the adjustment mode. The link attenuation adjustment mode applies to the transmission link where the number of added wavelengths and dropped wavelengths are the same at an OADM station. When the optical power is attenuated to the detection threshold, a command is automatically issued to adjust the attenuation at each station on the link.

NOTE

The link attenuation adjustment mode is also referred to as gain mode, which compares line attenuation with amplifier gain and adopts node gain offset compensation. In this mode, either the nominal gain of the optical amplifier unit or the attenuation of the attenuation adjustment unit is adjusted so that the two values are equal to each other, which maintains the power budget of the entire link.

- Perform automatic power equilibrium (APE). If the optical power of the channels detected by the MCA board at the receive end is abnormal, an event is reported to the U2000. After the event is confirmed, a command is issued to the optical attenuation adjustment board at the upstream station to adjust the optical power of the corresponding channels. In this manner, the optical signal noise ratio (OSNR) of each channel at the receive end is equalized.
- Perform ROADM optical power equalization. After ROADM is enabled to dynamically configure WDM services, the WDM equipment outputs multiplexed wavelengths. The optical power between each channel, however, may be significantly different, especially for newly added wavelengths. To avoid negative impacts on transmission performance, the ROADM optical power equalization mechanism is provided. This mechanism first determines whether the wavelengths are pass-through wavelengths or add wavelengths. Then, optical power adjustment starts. The DWC/WSS adjusts the optical power of pass-through wavelengths, while the optical attenuation adjustment board adjusts the optical power of add wavelengths based on wavelength labels.
- Configure pre-alerts for optical power at ports.

Dispersion Compensation

- The G.652 and G.655 fibers have positive dispersion coefficients and positive dispersion slopes in 1550 nm window. After an optical signal is transmitted over a certain distance, the accumulation of positive dispersion broadens the optical signal pulse and seriously affects the transmission performance. To minimize this effect, a negative DCM is used on networks. It uses negative dispersion to compensate for the positive dispersion of fibers, so as to maintain the original signal pulse.
- The OEQ NE can apply dispersion compensation to each band to reach dispersion equalization.
- This function supports 40 Gbit/s dispersion compensation configuration. It uses the TDC to precisely adjust the dispersion.

Wavelength Monitoring

Wavelength monitoring uses the wavelength supervisory unit to monitor the wavelengths that are transmitted from the WDM-side optical interface of the OTU board (including the service convergence unit) and to control the wavelength drift. This function ensures stable wavelengths.

WDM PRBS

You can perform PRBS on a board to check the path quality. You can also verify that the WDM link is functioning properly before provisioning a service.

Housekeeping Configuration

You can perform the following operations on the U2000:

- Set and query the environmental alarm attributes, including:
 - Adding environmental alarm attributes
 - Setting the normal state of environmental attributes
 - Querying environmental alarm attributes
 - Modifying environmental alarm attributes
 - Deleting environmental alarm attributes
- Set and query external control attributes, including:
 - Adding external control attributes
 - Querying external control attributes
 - Modifying external control attributes
 - Deleting external control attributes
 - Setting the control time of the external control relay

Query of AO Buffer Records

You can perform the following operations on the U2000:

- Query the records in the automatic output (AO) buffer, including:
 - Generation time of a record
 - Auto report tag (ATAG) of a record
 - Record type
 - Remarks
- Filter records in the AO buffer.
- Save records in the AO buffer to a file.
- Export records in the AO buffer to the browser of the operating system for printing.

EAPE Management

Enhanced automatic power equalization (EAPE) management can reduce the bit error rate (BER) of a service. You can query the EAPE function for an OCh trail.

Energy Consumption Management

You can perform the following operations on the U2000:

- Manage NE energy consumption to conserve energy and protect the environment without affecting the proper operation of NEs.
- Query energy consumption of boards and NEs.
- Configure energy-saving functions for NEs. You can dynamically adjust NE power consumption to conserve energy and protect the environment.
- View the network-wide NE energy consumption reports.

ASON Management

Topology Management

You can perform the following operations on the U2000:

- Implement automatic discovery of ASON topologies and resources.
- Synchronize NEs in a domain. The U2000 can obtain the topology of the network through an active NE.
- Set the active and standby NEs.
- Manage domains, including creating or deleting domains, and changing domain names.
- Query the ASON NE software version.
- Manage node IDs on ASON NEs.
- Query the enable status of the ASON NE software.
- Enable or disable the ASON feature of an ASON NE.

TE Link Management

You can perform the following operations on the U2000:

- Synchronize network-wide links by domain or payload type.
- Filter links by domain, link signal type, payload type, or source/sink information.
- View TE links.
- Create fibers.
- Manage TE links with OCh-type payloads.
- Set the length of a TE link.
- Generate link resource reports.

8.2.3 WDM/OTN Protection Subnet Management

A protection subnet is a network structure with comprehensive self-protection. For the U2000, the protection subnet is a generalized concept that covers not only the network structure with comprehensive self-protection, such as multiplex section protection (MSP) rings and path protection (PP) rings, but also the network structure without self-protection, such as unprotected rings and unprotected chains.

NOTE

A license is required to perform protection subnet management on the U2000.

You can perform the following operations on the U2000:

- Create WDM protection subnets by searching for them, including:
 - 1:N WDM protection subnet
 - ODUk SPRings at ODU1, ODU2, ODU3 and ODU4 levels
- Manage WDM protection subnets, including:
 - Setting parameters of a 1:N WDM protection subnet.
 - Performing protection switching in a 1:N WDM protection subnet and verifying the switching.
 - Setting parameters of an ODUk SPRing.
 - Performing protection switching in an ODUk SPRing and verifying the switching.
 - Querying or deleting a protection subnet.
 - Querying or deleting an isolated node.
 - Querying protection subnet resources.

8.2.4 WDM/OTN E2E Network Management

End-to-end (E2E) network management is also referred to as trail management. Trail-based configuration can be performed by searching for NE-layer data on the U2000 or by configuring the network-layer data on the U2000; then the configuration is applied to all associated NEs. Trail-based configuration is easier than configuring NE data on a per-NE basis.

Management of WDM Services



A license is required to perform E2E network management on the U2000.

The U2000 supports the following operations:

- Search for trails, including:
 - Generating the network-layer information about E2E trails based on the NE configuration data and fiber connection data at the NE layer. The trails include OTS trails, OCh client trails, OCh trails, optical multiplex section (OMS) trails, optical supervisory channel (OSC) trails, ODUk trails, and optical channel transport unit (OTUk) trails.
 - Combining trails automatically during trail search.
 - Retaining user-defined trail information during WDM trail search.
 - Searching for 10 Gbit/s and 40 Gbit/s inverse multiplexing trails.
 - Searching for trails that adopt both DWDM and CWDM technologies.
 - Combining two unidirectional trails (meeting the following requirements: at the OMS or higher layers, between the same NEs, and in opposite directions) into a bidirectional trail automatically after trail search.
 - Searching for trails on the network consisting of NG WDM NEs and conventional NEs.
 - Searching for Ethernet trails that carried on WDM trails.
 - Switching to the trail management window to query and modify trail details.
- Create trails, including:
 - Automatically generating an OTS trail after two boards are connected by a fiber.

- Selecting an NE in the topology view and browsing relevant alarms during trail creation.
- Identifying causes for failing to compute a route at the optical or electrical layer during trail creation.
- Creating OCh trails: Create OCh cross-connections by using the trail management function.
- Creating ODU0, ODU1, ODU2, ODU3, ODU4 or ODUflex trails: Create ODU0, ODU1, ODU2, ODU3, ODU4 or ODUflex cross-connections by using the trail management function.
- Creating and managing third-party WDM trails (OCh trails).
- Viewing detailed routing information during WDM trail creation.
- Creating Client trails: Create services at GE, FC, and FE rates based on OCh, OTUk, or ODUk trails by using the trail management function.
- Creating SNCP- or WXCP-protected trails by using the trail management function.
- Selecting the source and sink nodes by double-clicking NEs to create a WDM trail.
- Selecting the explicit route for protection when creating a WDM trail.
- Creating multi-layer WDM trails: Create Client and ODUk cross-connections by using the trail management function.
- Creating multiple trails by duplicating a trail and generating Client and ODUk cross-connections in batches by using the trail management function.
- Creating WDM trails where fiber jumpers are connected inside a station.
- Setting port attributes and channel status.
- Displaying new cross-connections.
- Creating Client trails that connect to client-side ports with fibers.
- Creating bidirectional WDM trails.
- Performing a consistency check between the discrete cross-connection type at the source and sink and the user-defined service type before route calculation, including the discrete cross-connections and services to be created at the source and sink ports, and the existing services on NEs.
- Defining the levels of pass-through cross-connections for transit nodes on a route when specifying the route constraints.
- Selecting wavelengths for the source and sink boards in the NE Panel when creating OCh trails.
- Setting port working modes in the NE Panel of the source and sink NEs when creating WDM trails.
- Setting the service types automatically for the source and sink ports when creating trails.
- Configuring port attributes manually.
- Enabling the non-intrusive monitoring of the PM overhead automatically when creating ODUk trails with the SNCP/N protection.
- Generating SNCP-protected ODUk trails automatically when the protection is configured for a Client trail.
- Creating Ethernet trails that carried on WDM trails.
- Managing virtual OTN NEs.

- Analyzing the causes of route calculation failures to facilitate fault troubleshooting.
- Automatically setting service types during ODUflex trail creation.
- Setting SNCP parameters, including Revertive Mode, WTR Time, Working Channel Hold-Off Time, Protection Channel Hold-Off Time, and SD Switching, during WDM trail creation.
- Manage customer information, including:
 - Creating customers and customer groups.
 - Viewing and modify customer information.
 - Viewing the trails related to a customer.
 - Viewing current and historical alarms of customer services.
 - Deleting customers.
 - Granting a customer to an NMS user for management.
- Query trail information, including:
 - Filter trails in the following three ways:
 - Filter all: Filter all trails and display only those that meet the criteria.
 - Secondary filter: Filter the displayed trails according to new criteria and display the results.
 - Incremental filter: Filter all trails and display those that meet the criteria together with the trails that are currently displayed.
 - Combining trails at the same level.
 - Splitting trail groups.
 - Querying routing information of a trail.
 - Viewing the signal flow diagram.
 - Querying the transmission-media layer of a trail.
 - Querying the client trail of a trail.
 - Querying the server trail of a trail.
 - Querying detailed information about a trail, including attributes and channel allocation.
 - Querying the optical power of a WDM trail, including the input and output optical power at the source and sink nodes of the trail.
 - Querying dual path protection switching (DPPS) of a trail.
 - Querying reachable routes for WDM trails configured with protection.
 - Querying the associated working and protection trails of OCh trails.
 - Displaying intra-station fibers in solid lines and inter-station fibers in dotted lines in the signal flow diagram of a trail.
 - Displaying the working and protection routes in different colors in the signal flow diagram of a trail.
 - Querying alarms from the signal flow diagram of a trail.
 - Displaying the detailed information about a trail group (such as the direction, name, trail status, source and sink nodes, wavelengths of the source and sink nodes, bearer rate, rate, and service type).
 - Switching between the window for viewing WDM trails and the window for viewing the associated SDH trails.

- Querying ALC links of OMS trails.
- Displaying trails of different levels except for the OTS, OMS/OSC and OTUk trails.
- Returning to the primary filter results after a secondary filter.
- Switching from Client and ODU2 trails to IP E2E trails to view tunnel details.
- Viewing the single route specifics of a trail.
- Allowing users to browse the client trails of a WDM trail by trail level.
- Displaying routes on the Main Topology for a WDM trail.
- Manage alarms and performance data, including:
 - Querying current alarms of a trail.
 - Querying historical alarms of a trail.
 - Querying current performance data of a trail.
 - Querying historical performance data of a trail.
 - Querying unavailable time (UAT) of a trail.
 - Querying performance threshold-crossing records of a trail.
 - Setting performance parameters and performance thresholds of a trail.
 - Querying Ethernet performance of an OCh client trail that carries services.
 - Managing network-wide WDM trails with triggered alarms in real time.
 - Monitoring WDM trails connectivity in real time.
 - Indicating fiber-cut alarms in the signal flow diagram by displaying the fiber in red.
 - Setting the alarm threshold of a trail.
 - Querying alarms (displayed in a table) on Client trails and their server trails.
 - Supporting dynamic and static correlation analysis of trail alarms. (This function requires a license.)
 - Suppressing alarms.
 - Enabling user-defined trail alarm correlation rules.
 - Switching from a WDM performance event to the WDM trail management window.
 - Analyzing OTN alarm correlation across multiple OMS trails.
 - Displaying the OSNR view of an OCh trail, and the port OSNR. (This function requires a license.)
- Query resource statistics, including:
 - Statistics on WDM client-side port resources.
 - Statistics on WDM inter-station wavelength resources.
 - Statistics on WDM link resources.
 - Statistics on WDM wavelength resources.
 - Statistics on WDM wavelength resource utilization.
 - Statistics on WDM bandwidth resources.
 - Statistics on subrack NE resources of optical NEs.
- Manage trails.
 - Querying 1+1 protection of optical-layer trails and performing 1+1 protection switching for the optical-layer trails.

- Querying trails with WXCP or SNCP protection, and performing protection switching for the trails.
- Using the TTI byte to check the fiber connection over an OCh trail.
- Automatically naming WDM trails or bulk changing their names according to naming rules.
- Modifying the source and sink nodes of ODUk ($k = 0, 1, 2, 3, 4$) trails and Client trails.
- Managing ODUk trails in an E2E manner.
- Searching for and performing E2E management over ODUk-based GE trails.
- Managing optical-layer alarms and configuring optical-layer overheads at the trail level.
- Analyzing the connectivity of a WDM trail and identifying a fault on a WDM trail.
- Adding or deleting WXCP or SNCP protection for an ODUk trail or a Client trail.
- Setting the optical power mode in an E2E manner.
- Implementing the Save As and Print functions for channel allocation of a WDM trail.
- Saving the signal flow diagram of a WDM trail.
- Managing WDM trails based on rights and domains.
- Managing WDM discrete services.
- Managing WDM platinum services and displaying the routes of the working and protection services in a platinum service group in the signal flow diagram.
- Configuring WDM trails on eight clients at the same time.
- Viewing relevant fibers of trails.
- Viewing the wavelength and frequency occupied by a configured OCh trail in the signal flow diagram.
- Adding a column in the **WDM Trail Management** window to indicate whether protection is configured.
- Identifying whether an OCh trail is used by a Client trail.
- Setting port loopbacks on any nodes of a trail.
- Managing trails that adopt both DWDM and CWDM technologies.
- Maintaining WDM trails.
- Creating ALC links of OMS trails
- Querying the current and reference attenuation of the ALC links on OMS trails.
- Configuring alarm thresholds and reference attenuation of ALC links on OMS trails.
- Managing bidirectional WDM trails.
- Setting and querying port attributes and channel status.
- Enabling or disabling service alarms of a trail.
- Locking and unlocking WDM trails.
- Selecting multiple protected services on a fiber for bulk protection switching.
- Setting TCM and PM overheads for service based on ODUk trails.
- Performing PRBS tests on WDM trails except OCS, OTS, and OMS trails.

- Displaying the ODUk trails that are free of cross-connections in the Manage WDM Trail window based on users' selection.
- Setting the maintenance and commissioning status of OCh trails.
- Displaying and setting the descriptions of protection groups in the WDM Trail Protection dialog box.
- Managing NEs (NA) and mainstream NEs at the same time.
- Exporting channel diagrams.
- Automatically setting main channel and flatness parameters in subnet policies.
- Changing the reversion mode for ODU SNCP protection.
- Retaining the names of traditional WDM trails after the trails are upgraded to ASON trails.
- Performing batch protection switchover.
- Smart Optical Management (SOM) based on OMS trails: The U2000 provides accurate optical power and online OSNR monitoring based on OMS trails and supports automatic and visible optical-layer commissioning and maintenance.
- Delete trails (except OTS trails) from the NE layer and network layer of the U2000.
- Support enhanced automatic power equilibrium (EAPE) based on OCh trails. The EAPE function automatically adjusts the optical power at the transmit end of each channel based on the signal quality of each channel detected by the optical transponder unit (OTU) at the receive end. Such adjustment ensures satisfactory signal quality at the receive end of each channel and service availability.
- Measuring the ODUk trail delay.

Management of Packet Services

- Service Trail View Management
 - Queries Layer 2 protocol configuration and status.
 - Performs loopback tests on E-LAN networks.
 - Creates performance monitoring tasks and queries historical and real-time performance data.
- PWE3 Service Management
 - Create multiple types of PWE3 services such as ATM, CES, ETH, and IP over PW.
 - Predeploy PWE3 services.
 - Automatically discover PWE3 services.
 - Modify, delete, and filter PWE3 services to view the desired services.
 - Manage multi-hop PWE3 services.
 - Manage PWE3 service protection.
 - View the topology of PWE3 services.
 - View the alarms of PWE3 services.
 - Manage performance of PWE3 services.
 - Test and check PWE3 services.
 - Diagnosing PWE3 services
 - Manage discrete PWE3 services.
 - Managing PWE3 services based on rights and domains.

- Clone PWE3 services.
- Manage PWE3 service templates.
- Automatically generate Ethernet OAM for Ethernet services.
- Set and view the status of port loopback of PWE3 services.
- Import PWE3 service data from or export PWE3 service data to .xls files.
- Perform one-key connectivity tests on ATM and CES services.
- Set the VC12 loopback for CES services.
- Display lower-layer (tunnel, Layer 2 link) alarms for PWE3 services.
- Filter PWE3 services by subnet.
- View the relative tunnel.
- Monitor the PWE3 services.
- Manage the PWE3 services protection switching.
- Convert a discrete service to an unterminated service.
- Support bandwidth connection admission control (CAC).
- Implement the MPLS-TP OAM configuration, MPLS-TP OAM tests, MPLS-TP performance monitoring and alarm association.
- Tunnel Management
 - Create static CR tunnels.
 - Duplicate static CR tunnels.
 - Predeploy tunnels.
 - Automatically discover tunnels.
 - Modify, delete, filter, and view tunnels.
 - View the topology of tunnels, including the working and protection routes.
 - View tunnel alarms.
 - Manage the performance of tunnels.
 - Test and check tunnels.
 - Diagnose tunnels.
 - Manage discrete tunnels.
 - Create, modify, delete, and automatically discover 1+1 or 1:1 tunnel protection groups.
 - Switch services in a 1+1 or 1:1 tunnel protection group manually.
 - Display the topology of 1+1 or 1:1 tunnel protection groups.
 - Create a tunnel and its protection tunnel at the same time.
 - Set and view the port loopback status of tunnels.
 - Display the name of a tunnel in the global LSP view.
 - Manage bidirectional static tunnels.
 - Display lower-layer (Layer 2 link) tunnel alarms.
 - Bulk change the switching status of tunnels in the tunnel management window.
 - Collect statistics on port bandwidth usage.
 - Filter tunnels by subnet.
 - Display the actual routing information of a static tunnel in the topology view of a protection group.

- View the correlated services of tunnels.
- Adjust the route of a tunnel.
- Monitor the tunnel.
- Export tunnel service data from the U2000 to .xls files and import the .xls files containing tunnel service data to the U2000.
- Implement the MPLS-TP OAM configuration, MPLS-TP OAM tests, MPLS-TP performance monitoring and alarm association.
- VPLS Service Management
 - Create VPLS services.
 - Predeploy VPLS services.
 - Automatically discover VPLS services.
 - Modify and delete VPLS services, and view VPLS services by using the filtering function.
 - View the topology of VPLS services.
 - View the alarms of VPLS services.
 - Manage the performance of VPLS services.
 - Test and check VPLS services.
 - Manage VSI Resource.
 - Manage VPLS services based on rights and domains.
 - Manage VPLS service templates.
 - Automatically generate Ethernet OAM for VPLS services.
 - Set and view the status of port loopback of VPLS services.
 - Display lower-layer (tunnel, Layer 2 link) alarms for VPLS services.
 - Migrate VPLS services.
 - Implement scheduled automatic discovery of VPLS services.
- Composite Service Management
 - Create H-VPLS services.
 - Modify and delete composite services, and view composite services by using the filtering function.
 - Automatically discover composite services.
 - View the topology of composite services, including the internal connections between the services.
 - Display the status of composite services.

8.2.5 WDM ASON Network Management

An automatically switched optical network (ASON) is a new-generation optical network that integrates switching and transport functions. After a user initiates a service request, the ASON network automatically selects a route. The network then automatically establishes and removes connections through signaling control. A WDM ASON NE refers to a device that has both WDM and ASON features. The U2000 combines ASON and WDM features to perform WDM ASON network management.

You can perform the following operations on the U2000:

Topology Management

- Automatically discover the ASON network topology and resources.
- Synchronize NEs in the ASON domain: The U2000 can obtain the topology of the ASON domain from an active NE.
- Set the active and standby NEs.
- Manage domains (including creating and deleting domains and changing domain names).
- Manage ASON NE IDs.
- Query the ASON NE software versions.
- Manage the ASON feature at the electrical and optical layer.
- Manage OSPF IP addresses.
- Manage global ASON.
- Set and query the upgrade state of ASON NEs.

Control Link Management

- Synchronize network-wide control links.
- Filter control links by domain, interface type or source/sink information.
- View control links.
- Query current and historical alarms on control links.
- Set alarm suppression for control links.

TE Link Management

- Manage TE links with the following payload types: OCh, ODUk ($k = 0, 1, 2, 3, 4, \text{flex}$), ODU1_ODU2, ODU0_ODU1_ODU2, ODU0_ODU1_ODU2_ODU3, ODU0_ODU1_ODU2_ODU3_ODU4_ODUFlex, ODU0_ODU1_ODU2_ODUFlex or ODU0_ODU1_ODU2_ODU3_ODUFlex.
- View TE links.
- View resource usage.
- Query the status of TE links.
- Display wavelength performance status of TE links.
- Set the length of TE links.
- Set the risk link group number.
- Customize the costs of TE links.
- Set TE links to maintenance status.
- Set resource reservation of TE links.
- Query ASON trails of TE links.
- Query the WDM trails of TE links.
- Query the name of TE links from NEs.
- Query the SRG(Shared Risk Group) of TE links.
- Delete broken TE links.
- Synchronize network-wide TE links by domain, payload type or extended attributes.
- Filter TE links by domain, link signal type, payload type (optical layer or electrical layer), TE link name, Link status or source/sink information.

- Synchronize the fiber length to the TE link distance.
- Create virtual TE links.
- Delete virtual TE links.
- Create fibers for TE links with OCh-type payloads.
- Collect statistics on bandwidth resources of TE links.
- Manage optical parameter.
- Query current and historical alarms of TE links.
- Set alarm suppression for control plane alarms.
- Generate link resource reports.
- Query TE link resource occupation status.
- Query the affected TE links according to control plane alarms.
- Set refreshes the alarm status, interrupt status, and added TE links automatically.

ASON Trail Management

You can create the ASON Trails:

- Create diamond, silver, or copper WDM ASON trails.
- Create WDM ASON trails at the OCh, ODU0, ODU1, ODU2, ODU3, ODU4, ODUflex level.
- Create associated WDM ASON trails with the same source node or different source nodes.
- Pre-compute routes when creating or optimizing WDM ASON trails.
- Duplicate the WDM ASON trail.
- Apply planning data to an ASON trail.
- Set routing attributes, including rerouting lockout status, reversion lockout status, rerouting priority, revertive mode, WTR time, scheduled revertive time, rerouting policy, trigger condition, number of crankbacks, rerouting triggered by SD, SNCP switching upon SD, restore original selective receiving and rerouting hold-off time.
- For WDM ASON OCh trail, you can set the preset restoration trail that with different wavelength by optical regenerator.
- Save the attributes of a WDM ASON service after the service is created successfully.
- Support traditional WDM networks' access to WDM ASON networks in SNCP mode.
- Create dual-homed WDM ASON trails.
- Convert WDM ASON OCh trails with the same source and sink to dual-homed WDM ASON trails.
- Configure FlexP&R protection, including the maximum switching events and maximum rerouting events.

You can view the ASON Trails:

- Filter WDM ASON trails by domain, name, creator, source, sink, actual route, original route, preset restoration trail, creation time, planning time, activation status, protection type, service level, alarm severity, management status, ASON trail lock status, E2E lock status, whether the original route is active.
- Synchronize network-wide WDM ASON trails by domain, service level, or attributes (optional).

- View WDM ASON trails.
- View the details of WDM ASON trails.
- View optical power commissioning information of WDM ASON trails.
- Query server and client trails of WDM ASON trails.
- Query the associated trails of a WDM ASON trail.
- Refresh the actual route, original route, associated routes, or signal flow diagram of a WDM ASON trail.
- View the actual route, original route, or associated routes of a WDM ASON trail.
- View the preset restoration trail for a WDM ASON trail.
- View alarms of WDM ASON trails.
- View and set the control plane alarm suppression information about WDM ASON trails.
- View performance events of WDM ASON trails.
- Set the control plane performance parameters of WDM ASON trails, and view the control plane performance.
- Generate WDM ASON trail reports.
- Refresh routes automatically after diamond trail protection switching.
- Query the optical power of WDM ASON trails.
- Refresh wavelengths upon being notified of a wavelength change on a WDM ASON OCh trail.
- Convert a dual-homing access WDM ASON trail to an associated trail.
- Query E2E status for ASON trails.
- Set the display mode and view the legend for a signal flow diagram.
- Query link and board information in signal flow diagrams.

You can maintain the ASON Trails:

- Share wavelengths in the working and protection diamond ASON trails at the optical and electrical layers.
- Share wavelengths in associated trails at the optical and electrical layers.
- Activate or deactivate WDM ASON trails.
- Delete inactive WDM ASON trails.
- Delete WDM ASON trails from the NMS.
- Set the association source for WDM ASON trails.
- Set and cancel associations for WDM ASON trails.
- Downgrade WDM ASON trails to WDM trails.
- Convert a WDM ASON trail in in-service mode.
- Enable or disable optical parameters verify of WDM ASON OCh trails, such as PMD and dispersion.
- Revert a WDM ASON trail to the original route.
- Optimize WDM ASON trails.
- Optimize a WDM ASON trail to a preset restoration trail.
- Switch services in the working or protection diamond trail manually.
- Set the current route as the original route.

- Refresh preset restoration trail.
- Set one or two preset restoration trails for a WDM ASON trail.
- Delete the preset restoration trail for a WDM ASON trail.
- Revert trails to the original routes in batches.
- Set names for WDM ASON trails in batches according to the naming rules.
- Manage creators of WDM ASON trails.
- Set the route attributes of associated WDM ASON trails, including trigger conditions for rerouting and the sharing policy.
- Perform manual switching.
- Revert WDM ASON trails manually and forcibly.
- Lock or unlock ASON trails on NMS.
- Support trail maintenance.
- Set the original selective receiving routes of diamond services at the optical layer to the original protection or working route.

You can troubleshoot the ASON Trails:

- Query fault information about preset restoration trails.
- Query the historical rerouting information of ASON trails.
- Query the overlap between diamond and associated silver links to identify the causes of SLA degradation alarms.

SRG Management

- Create, delete, or modify SRGs.
- Manage SRGs of the pipe type or a custom type.

Quick Single-NE Downgrade

You can quickly downgrade control plane status of an ASON NE and all the ASON trails related to the NE.

Combination of ASON Trails and WDM Trails

- Create ASON-WDM trails at the OCh, ODUflex, ODU4, ODU3, ODU2, ODU1, or ODU0 level.
- Configure multi-layer services easily. When you create a client trail, its electrical-layer ASON-WDM server trails are automatically created.
- View WDM trails and managed ASON trails in the **Manage WDM Trail** window.
- Manage overhead bytes, alarms, and performance of ASON-WDM trails in a unified manner.
- Query the ASON trails from the related WDM trails.
- Query the WDM trails from the related ASON trails.
- Downgrade an ASON trail to a WDM trail.
- Upgrade a WDM trail to an ASON trail.
- Collect statistics on alarms of ASON-WDM trails, including alarms on the ASON trails.
- Manage, search for, upgrade, and downgrade ASON-WDM trails.

- Upgrade WDM trails to dual-homed WDM ASON trails.
- Configure FlexP&R protection when creating ASON-WDM trails.
- Provide FlexP&R protection when upgrading WDM trails to ASON trails.
- Lock or unlock ASON-WDM trails on NMS.
- Set the rate mode of ASON-WDM ODUk trails to the standard or speedup mode.
- Retain the original trail name after a traditional-to-ASON or ASON-to-traditional conversion if the source and sink ports of the trail are not changed during the conversion.

Export and Import of Scripts

- Export WDM ASON node information in scripts or import scripts containing WDM ASON node information.
- Export WDM TE link information in scripts or import scripts containing WDM TE link information.
- Export WDM ASON trail information in scripts or import scripts containing WDM ASON trail information.

ASON Management on a Per-NE Basis

- Enable or disable ASON features.
- Manage ASON NE IDs.
- Manage the control plane status.
- Manage optical layer control plane parameters and electrical layer control plane parameters, including the bandwidth usage (%), bandwidth weight, distance weight, hop weight, and custom cost weight.
- Manage LMP control channels.
- Manage LMP TE links.
- Implement LMP automatic discovery.
- Manage OSPF control links.
- Manage OSPF TE links.
- Manage OSPF IP addresses.
- Manage OSPF protocol authentication.
- Manage the RSVP protocol authentication.
- Manage WDM fiber resource thresholds.
- Manage WDM ASON trails.
- Maintain ASON signaling.
- Maintain the ASON switching controller.
- Manage the status of the LMP protocol.
- Manage the status of the OSPF protocol.
- Manage the auto-reporting status of control plane alarms.
- Manage the severities and suppression status of control plane alarms.
- Query the SCN control route.
- Manage control plane performance parameters.
- Query control plane performance.

- Manage resource reservation.
- Manage the resource usage status.
- Manage wavelength performance monitoring.
- Manage wavelength performance status.
- Manage OMS with abnormal line attenuation.

8.3 RTN Network Feature Management

This topic describes the functions and features of RTN NE management and network management.

8.3.1 RTN NE Management

NE management refers to the configurations of an NE in terms of attributes, communications, services, protections, and clocks. The configuration object is a single NE. The data is saved to the U2000 NE layer database and to the NE database.

Configuring Automatic NE Connection

During new deployment or network expansion, many NEs need to be created. Creating them manually will consume much time. In this scenario, the NE automatic discovery function comes into play. This function can discover NEs automatically and create them in batches.

Smart deployment of small-cell RTN sites

The offline RTN service design tool, Microwave Deployment Tool (MDT), and U2000 together help hardware installation engineers quickly configure massive small-cell RTN sites, thereby reducing site deployment costs and improving efficiency.

Basic NE Configurations

You can perform the following operations on the U2000:

- Manage the connections between back-to-back RTN NEs. In the Main Topology of the U2000, the connections between back-to-back RTN NEs indicate the relationships between the RTN NEs on the same station that are connected in a back-to-back manner through network interfaces.
- Modify NE attributes, including:
 - NE name
 - NE ID
 - Extended NE ID
 - Remarks
- Synchronize NE time: Specify the interval or exact time to automatically align the time of all NEs with the system time of the U2000 server, NTP server, or standard NTP server. You can also set the time and period for automatic NE time synchronization.
 - If you use the scheme of synchronizing with the U2000 server, all NEs use the U2000 server time as the standard time. The NE time can be synchronized with the U2000 server time manually or automatically. The U2000 server time refers to the

system time of the workstation or computer where the U2000 server is located. This scheme features easy operation, and is applicable in networks that require a low accuracy with regard to time.

- If you use the scheme of synchronizing with the NTP server or synchronizing with the standard NTP server, the NE time and the U2000 time are synchronized with the NTP server time or the standard NTP server time automatically. The NTP server can be the U2000 server or a special time server. This scheme enables the U2000 and NEs to have a time accuracy of one nanosecond in theory, and applies to a network with high requirement for time accuracy.
- Display boards in plug-and-play (PnP) mode: After being inserted into slots, boards along with their information are automatically displayed in the NE Panel.
- Implement automatic NE function disabling: NE functions that affect services, such as loopback and automatic laser shutdown (ALS), are disabled at the scheduled time.
- Set environment monitoring interfaces.
- Implement automatic creation of RTN NEs: Creating a USB-Connected NE, Creating an NE Connected by Wi-Fi, Creating an NE (Searching for the NE), Creating an NE Manually.
- Support the license management function for equipment.
- Support the press-to-install function for logical boards.
- Search for the opposite NE.
- Query the microwave performance events.
- Query physical bandwidth and bandwidth usage of the port.
- Perform IP Address-based Ping tests and traceroute tests.
- Manage outdoor racks.
- Test the fade margin.
- Support the database restoration from peer.
- Support RTN NEs fault auto recovery.
- Support align antenna.
- Support RTN NEs 1+1 Configuration Sync.
- Support XPD meter-free test.
- Support Wi-Fi security management.
- Support CPRI Mode Setting.
- Support Radio Interface Encryption.
- Support MIMO Configuration.
- Support test CPRI/OBSAI delay.

IF Cable Hardware Test

After hardware installation is complete, IF cables can be tested in a one-click manner to diagnose hardware faults.

NE License Authorization

In the **NE License Authorization** window provided by the U2000, you can control the basic functions, enhanced functions, and service access licenses of the TP Assistant, which greatly increases device O&M efficiency.

Orderwire Configuration

You can perform the following operations on the U2000:

- Set and query the order wire phone numbers, call waiting time, and orderwire phone port availability.
- Set and query the bytes occupied by orderwires.
- Set and query the F1 data interface.
- Set and query the broadcast data interface.

Equipment Protection Configuration

You can perform the following operations on the U2000:

- Configure 1+1 board protection.
- Configure 1+1 IF protection.

Interface Configuration

You can perform the following operations on the U2000:

- Set the parameters for an SDH interface.
- Set automatic laser shutdown.
- Set the parameters for a PDH interface.
- Set the parameters for an IF interface.
- Set the parameters for a digital interface.
- Set the parameters for an outdoor unit (ODU) interface.
- Set overhead interfaces, including:
 - Orderwire
 - Broadcast data interface
- Query and set the overhead bytes including:
 - Regenerator section overhead (J0).
 - Lower-order path overhead (V5, J2)
 - VC-4 higher-order path overhead (J1, C2) and its pass-through or termination.
 - VC-3 higher-order path overhead (J1, C2).
- Enable IEEE 1588 overhead bytes.
- Perform PRBS testing.
- Set the parameters for an Ethernet virtual interface.
- Set the parameters for a serial interface.
- The features of packet radio. You can configure a microwave interface in terms of basic and advanced attributes, IF attributes, and Layer 2 and Layer 3 attributes.
- Configure the long and short serial numbers for an MP group.
- Configure enhanced compression.

Configure microwave links based on hop

U2000 support configuring basic attributes for the local and remote NEs of a single-hop microwave link.

- Configure the NE and link attributes for both the local and remote NEs of a single-hop microwave link.
- Configure the IF attribute, RF attribute and IF protection for both the local and remote NEs of a single-hop microwave link.
- Configure the PLA, LAG, XPIC based on a single-hop microwave link.
- View the optical power of the microwave link in graph.
- View the radio link performance: Collect statistics on power and bit error rates (BERs) of the NEs at both ends of a radio link and view the statistics in a graph or table. You can also quickly query the current and historical performance of the two NEs, which improves routine maintenance efficiency.
- View the radio link alarm: Browse radio link alarms to obtain the important intermediate frequency information and alarm information of the NEs on both ends of a radio link.
- Configure loopback based on radio link: View or set the loopback status of the IF interface or ODU interface at the two ends of a radio link.
- View the microwave link frequency scan: Scan frequencies for IF 1+1 protection groups and XPIC groups in cascading and non-cascading scenarios at the two ends of a radio link.

Scanning ODU Frequency Interference

When channel interference occurs, the commonly-used method is using special instruments to check whether transmit frequencies are interfered with. However, using special instruments to scan frequencies is not cost-effective. You can use the automatic frequency scanning function provided by the U2000 instead.

NE Offline Configuration

During new deployment, NEs can be created in offline mode. The general process is as follows: create and configure an NE on the U2000 in offline mode, export the NE data to a script, import the script into the Web LCT, and apply configuration data in the script to the NE. Multiple NEs can be created in this manner at the same time, which significantly improves the NE configuration efficiency.

One-Click Microwave Link Acceptance Test for RTN NEs

The one-click microwave link acceptance test function for RTN NEs abandons the traditional item-by-item testing method. Test reports are generated after acceptance tests are complete. You can check these reports together. In this manner, the test and report generation efficiency is improved.

LLDP Configuration

LLDP is a link layer communication protocol. LLDP allows a piece of equipment attached to an Ethernet to advertise, to its adjacent equipment attached to the same Ethernet, information such as its major capability, management address, equipment identifier, and interface identifiers. The information distributed by this protocol is stored by its recipients in a standard

management information base (MIB), making it possible for the information to be accessed by a network management system (NMS).

RTN Service and Protection Configuration

You can perform the following operations on the U2000:

- Configure VC-12, VC-3, or VC-4 services.
- Switch between an SNCP service and an ordinary service.
- Modify attributes of SNCP services.
- Perform SNCP protection switching.
- Configure 1+1 linear MSP and 1:N linear MSP.
- Configure 1+1 IF and N+1 IF protection.
- Configure REG.
- Configure MSP rings.
- Configure the XPIC feature.
- Configure the hybrid radio and the AM features, carry E1 and Ethernet services, and enhance the availability of radio links.
- Query for the AM mode adjustment history.
- Configure Ethernet ring protection (support ERPS V1 and V2).

Ethernet Interface and Service Configuration

You can perform the following operations on the U2000:

- Configure internal Ethernet interfaces, including:
 - TAG attributes
 - Encapsulation/mapping
 - Network attributes
 - Link capacity adjustment scheme (LCAS)
 - Bound path
- Configure external Ethernet interfaces, including:
 - Basic attributes
 - Flow control
 - TAG attributes
 - Network attributes
 - Advanced attributes.
- Configure jumbo frames.
- Configure QinQ types.
- Configure Ethernet private line (EPL) services.
- Configure EVPL (QinQ) services.
- Configure Ethernet private LAN (EPLAN) services. You can create a new virtual bridge (VB) and configure the following: service mount, VLAN filtering, VLAN unicast, disable MAC address, bound path, self-learning MAC address, and VLAN MAC address table capacity.

- Test frame receiving and sending on Ethernet boards.
- Configure QoS, including:
 - Flow
 - CAR
 - CoS
 - Port shaping
 - Board shaping
- Configure Ethernet Layer 2 switching, including:
 - Aging time
 - Spanning tree
 - IGMP snooping management.
- Perform operations of diagnosing protocol faults and restoring protocols.
- Configure point-to-point LPT management and point-to-multipoint LPT management.
- Configure intra-board Ethernet LAGs.
- Configure the RMON performance functions such as browsing history groups of Ethernet ports, setting an alarm group of Ethernet ports, collecting performance statistics of a group, and setting a history control group.
- Manage VPLS services.
- Configure the mirroring of Ethernet ports to facilitate packet listening, routine maintenance, and in-service commissioning. In this manner, the product does not resolve or process the captured data.
- Support E-LAN LD test management.

Clock Configuration

You can perform the following operations on the U2000:

- Query the clock synchronization status.
- Set clock source priority, including:
 - Priority for system clock sources
 - Priority for phase-locked sources of the first external clock output
 - Priority for phase-locked sources of the second external clock output
- Set clock source switching, including:
 - Clock source restoration parameters
 - Clock source switching conditions
 - Clock source switching
- Configure clock subnets, including:
 - Clock subnets
 - Clock quality
 - Synchronization status message (SSM) output control
 - Clock ID status
- Set phase-locked sources of external clock output, including:
 - Phase-locked sources of external clock output

- Attributes of 2M phase-locked sources of external clocks.
- Support frequency selection mode.
- Support clock source group configuration.
- Support PTP profile Configuration: IEEE-1588v2, G.8275.1.

Ethernet OAM Management

You can perform the following operations on the U2000 to configure the 802.1 ag Ethernet OAM:

- Configure maintenance domains (MDs), maintenance associations (MAs), maintenance points (MPs), and Test ID.
- Perform continuity checks.
- Perform LB checks.
- Perform LT checks.
- Perform ping tests.
- Execute performance tests.

You can perform the following operations on the U2000 to configure the 802.3 ah Ethernet OAM:

- Enable OAM self-loop detection.
- Enable OAM automatic discovery.
- Notify link events and adjust the OAM error frame monitoring threshold.
- Perform remote loopbacks.

IS-IS Protocol Configuration

The U2000 uses the intermediate system-to-intermediate system (IS-IS) protocol for the network control plane, and provides the following functions:

- Configure IS-IS protocol instances.
- Enable the IS-IS protocol for a port.
- Import routes.
- Configure link TE information.

OSPF Protocol Configuration

The U2000 uses the open shortest path first (OSPF) protocol for the network control plane, and provides the following configuration functions:

- Configure OSPF protocol instances.
- Enable the OSPF protocol for a port.
- Import routes.
- Configure link TE information.
- Configure Multi-Area OSPF management.

MPLS Signaling Protocol Configuration

The U2000 supports the configuration of the following signaling protocols:

- RSVP-TE protocol: Resource reservation protocol-traffic engineering (RSVP-TE) is derived from the RSVP protocol. The RSVP protocol is a type of QoS protocol. The RSVP protocol reserves resources for specific services in a network to ensure service quality. With the developments in TE, the RSVP protocol has been further developed to support LSP deployments.
- LDP protocol: Label distribution protocol (LDP) is an MPLS control and signaling protocol.

RTN equipment supports dynamic LSP connections by means of the RSVP-TE protocol and PW connections by means of the LDP protocol.

Static Route Management Configuration

The U2000 supports the configuration of static route management.

Address Resolution Configuration

The U2000 supports the configuration of address resolution.

IEEE 1588 Packet Clock Configuration

You can perform the following operations on the U2000:

- Configure the frequency source selection mode.
- Set the PTP system time.
- Configure a PTP clock subnet.
- Configure a PTP clock service.
- Set the WTR time for a PTP clock source.
- Set the PTP clock source priority.

ACR Clock Configuration

You can configure the CES ACR or 1588 ACR clock or clock domain.

LAG Configuration

A link aggregation group (LAG) aggregates multiple Ethernet physical links to form a logical link with a faster data transmission rate. This configuration improves link availability and increases link capacity.

The U2000 supports the configuration of the following LAG attributes:

- Configure the load sharing type, including sharing and non-sharing.
- Configure the LAG type, including manual and static.
- Configure the service distribution algorithm of the LAG.
- Configure the port priority and system priority of the LAG.

BFD Configuration

The bidirectional forwarding detection (BFD) protocol can be used to check the Ethernet link.

BFD is a simple Hello protocol. It is similar to the neighbor detection of well-known protocols in many aspects. A pair of systems periodically sends detection packets on the

bidirectional channel where sessions between the two systems were created. If one system does not receive any detection packets from the other within a specified period, that system assumes that there is a failure on the bidirectional channel.

QoS Configuration

Quality of service (QoS) refers to the performance of the data flow transmission in a network. The QoS is used to ensure end-to-end service quality. The QoS cannot enhance the bandwidth, but it can minimize the delay and jitter in a network by properly allocating and monitoring network resources. In this way, the service quality is ensured.

The DiffServ (DS) domain consists of a group of network nodes with the DiffServ function. Nodes of this type are also called DS nodes. In a DS domain, all DS nodes adopt the same service provisioning policy to achieve the same per-hop behavior (PHB). DS nodes are classified into edge DS nodes and internal DS nodes. Edge DS nodes usually perform complex flow classification on the traffic that enters the DS domain. Traffic of different types is marked with different PHB service types. Internal DS nodes only need to perform simple flow classification based on PHB service types.

The U2000 supports the following QoS configurations:

- Configure QoS templates.
- Configure Diffserv domains.
- Configure ATM CoS mapping.
- Configure simple flow classification and complex flow classification.
- Configure CAR and shaping.
- Configure WFQ scheduling policies.
- Configure port WRED policies.
- Configure WRR scheduling policies.
- Simplify operations and share some common QoS configuration parameters. The U2000 enables users to create QoS function point policies. The function point policies consist of port policies, ATM policies, and V-UNI ingress policies. By using these function point policies, you can bind configurations for CAR attributes, shaping attributes, flow classification attributes, WFQ scheduling policies, WRED policies and WRR scheduling policies.
- Support the application of the QoS policy to multiple NEs by configuring QoS templates.

MS PW Configuration

By creating multi step (MS)-PW to transmit services, you can transmit services over different networks while saving tunnel resources.

PW Dual-Homing Protection Configuration

As a network protection mechanism, PW automatic protection switching (APS) is intended to protect the services on the working PW with a protection PW. That is, when the working PW is faulty, the services on the working PW are switched to the protection PW. In this manner, the services on the working PW are protected.

As a network protection mechanism, PW fast protection switching (FPS) is intended to protect the services on the working PW with a protection PW. That is , when the working PW,

core equipment or link between core equipment and RNC(Radio Network Controller) is faulty, the node core equipment switches services to the protection PW. In this manner, services are protected.

PWs with UDP Encapsulation

The U2000 supports PWs with UDP encapsulations that are carried in IP tunnels.

MPLS Tunnel Configuration

The Multi-Protocol Label Switch (MPLS) protocol allows service packets to transmit transparently. The MPLS tunnel is defined by the MPLS protocol. Independent of services, an MPLS tunnel enables E2E transmission and provides channels for service-related PWs.

The U2000 supports the following configurations and operations on MPLS tunnels on a per-NE basis:

- Configure basic attributes of the MPLS.
- Configure static unicast MPLS tunnels.
- Create forward and backward MPLS tunnels at the same time.
- Create the E-LSP.
- Manage PWs.
- Manage tunnel labels and PW labels.

MPLS Tunnel Protection Group Configuration

The U2000 supports the following operations for configuring an MPLS tunnel protection group:

- Create 1+1 MPLS tunnel protection groups and 1:1 MPLS tunnel protection groups that consist of the switching mode, revertive mode, wait-to-restore (WTR) time, and hold-off time.
- Perform MPLS tunnel protection switching.
- Query the protection switching status of an MPLS tunnel.

IP Tunnel and GRE Tunnel Configuration

If the equipment in the IP network does not support the MPLS tunnel, PWE3 services can be carried in the IP network by using IP tunnels or GRE tunnels.

IP tunnels and GRE tunnels mainly apply to the offload scenarios of mobile communication.

The U2000 supports the configuration of bidirectional IP tunnels and GRE tunnels on a per-NE basis.

The U2000 supports the offload protection between MPLS and IP or GRE tunnels.

RSVP Tunnel Configuration

RSVP tunnels are flexibly deployed dynamic tunnels. After the source and sink nodes are manually selected, the MPLS protocol automatically calculates tunnel routes. You can specify route restrictions to route the tunnel to the desired path. To keep services secure, you can configure hot backup protection for tunnels.

CES Service Configuration

CES is used for transparent transmission of switching data on TDM circuits in packet transport networks.

The U2000 supports the following operations and features when users create CES services:

- Create PWs for a CES service.
- Create UNI-UNI and UNI-NNI CES services.
- Create CES services in CESoPSN and SATop modes. CESoPSN is short for structure-aware TDM circuit emulation services over packet switched network and SAToP is short for structure-agnostic TDM over packet.
- Configure QoS for CES services.
- Configure the value for idle timeslot recovery.
- Create CES services using either of the following transparent transmission modes: common or SOH.
- Calculate CES.

ATM Service Configuration

ATM emulation service is mainly used to transparently transmit ATM services in packet transport networks.

The U2000 supports the following functions when users create ATM services:

- Create an ATM service with multiple ATM connections.
- Create UNI-UNI and UNI-NNI ATM services.
- Create ATM services using one of the following connection types: PVP, PVC, or port transparent.
- Create PWs for an ATM service.
- Configure IMA groups.
- Configure QoS for ATM services.
- Configure CoS mapping.

E-Line Service Configuration

E-line services are a point-to-point Ethernet service. The equipment transmits user packets from the user side to the network side based on Port or Port+VLAN. Service data can be transparently transmitted in a point-to-point manner.

The U2000 supports the following functions when users create E-line services on a per-NE basis:

- Create UNI-UNI E-Line services.
- Create UNI-NNI E-Line services through ports.
- Create UNI-NNI E-Line services that are carried on PWs.
- Create UNI-NNI E-Line services that are carried on QinQ links.
- Configure QoS for the PWs of an E-line service.
- Configure V-UNI groups.

E-LAN Service Configuration

The E-LAN is a multipoint-to-multipoint Ethernet service. It connects to multiple V-UNI and NNI access points. It realizes packet forwarding and interconnection by using the MAC address self-learning scheme of layer 2.

Different VLANs are used to identify service data of different branches by using the E-LAN service. In this way, data is shared within a branch and is isolated from other branches. The Internet data of the HQ is also isolated from the internal service data by using the VLAN.

The U2000 supports the following functions of configuring E-LAN services on a per-NE basis:

- Create E-LAN services that are carried on port.
- Create E-LAN services that are carried on QinQ links.
- Create E-LAN services that are carried on PW.
- Configure V-UNI and NNI interfaces for an E-LAN service.
- Configure the split horizon group of an E-LAN service.
- Configure V-UNI groups.
- Configure MAC address learning parameters.
- Configure the unknown frame processing mode.
- Configure the static MAC address.
- Configure the disabled MAC address.
- Configure the self-learning MAC address.
- Support the automatic loopback test for Ethernet services.
- Allow users to enable Ethernet services manually.

E-AGGR Service Configuration

E-AGGR services are a multipoint-to-point Ethernet service. The equipment uses several ports to access services from the V-UNI side and then converges the services into one PW at the network side for transmission. Service data from multiple points can be converged into one point.

The U2000 supports the following configurations for E-AGGR services on a per-NE basis:

- Configure VLAN forwarding table items of an E-AGGR service.
- Configure QoS for the PWs of an E-AGGR service.
- Configure V-UNI groups.

IGMP Snooping Configuration

The Internet group management protocol snooping (IGMP snooping) is a scheme of multicast constraints on Layer 2 equipment, and is used to manage and control multicast groups.

The U2000 supports the configuration of IGMP snooping for E-LAN services, and provides the following operations:

- Configure IGMP Snooping protocol parameters.
- Configure quick leaving ports.
- Manage routes.

- Configure route member ports.
- Query statistics of IGMP protocol packets.

MPLS OAM Configuration

MPLS OAM refers to a group of OAM functions that can check the quality of LSPs in an MPLS network. The MPLS OAM scheme can effectively detect, report, and handle a defect inside the network at the MPLS layer in addition to triggering protection switching when a malfunction occurs.

The U2000 provides the following configurations for MPLS OAM:

- Configure MPLS OAM parameters for tunnels.
- Perform tunnel CV/FFD checks for tunnels.
- Perform tunnel ping checks.
- Perform tunnel traceroute checks.
- Perform PW ping checks.
- Perform LSP/PW traceroute checks.
- Enables or disables the FDI.

ATM OAM Configuration

ATM OAM refers to a group of end-to-end OAM functions for ATM services that can check the quality of an ATM link with multiple NEs. The ATM OAM functions check an ATM link by inserting some OAM cells with standard cell structures into the user cell flow.

The U2000 provides the following configurations for ATM OAM:

- Set segment end attributes.
- Perform CC activation tests.
- Perform remote loopbacks.
- Set the LLID.
- Perform fault notification.

Setting SNMP NMS Parameters

When the OSS obtains alarm and performance data from NE over SNMP, you need to configure IP address and permission control parameters of OSS on the U2000.

Setting Control Plane DCN Packet Priority and Bandwidth

In a DCN that packets travels on the control plane, DCN and service packets share the same forward channels. Therefore, you need to set the control plane DCN packet priority and bandwidth.

Configuring Layer 2 DCN

In the Layer 2 data communication network (DCN) solution, the U2000 implements NE management through Layer 2 forwarding. DCN data is encapsulated into Ethernet frames and forwarded at Layer 2 between NEs.

Configuring PLA

Physical link aggregation (PLA) allows all Ethernet transmission paths in several Integrated IP radio links connected to the same equipment to be aggregated as a PLA. For MAC users, a PLA works as a single link.

MPLS-TP OAM Configuration

Complying with MPLS-TP standards, MPLS-TP OAM provides the following OAM functions for MPLS-TP networks:

- Checking, discovering, and locating a defect inside the network at the MPLS layer.
- Reporting and handling the defect.
- Triggering protection switching when a fault occurs.

This feature provides the following functions for tunnels and PWs:

- Switching OAM recommendations.
- Setting MEP parameters.
- Performing a CC check.
- Performing ping tests.
- Performing traceroute tests.
- Performing LB tests.
- Performing LT tests.
- Checking packet loss ratios and delay.
- Performing LCK and TST tests.
- Setting MIP parameters.

L3VPN management

- Manage IP Protocol.
- Manage Route.
- Manage Tunnel.
- Manage VPN.
- Manage Reliability.

NE Loop

You can loop back all ports and query loopback ports on an NE.

Data Service Performance Test

E-Line service indicators such as the throughput and latency can be tested on the U2000 to avoid costly and inefficient meter tests.

Simplifying the 1+1 hot standby(HSB) protection configuration

Creating 1+1 hot standby(HSB) protection is simplified to set parameters for four NEs in one window.

8.3.2 RTN Protection Subnet Management

A protection subnet is a network structure with comprehensive self-protection functions.

A license is required to perform protection subnet management.

You can perform the following operations on the U2000:

- Create an RTN protection subnet.
 - IF_1+1 protection subnet
 - IF_N+1 protection subnet
- Manage RTN protection subnets.
 - Set the parameters for a protection subnet.
 - Query the switching status of a protection subnet.
 - Query and delete a protection subnet.
 - Query protection subnet resources.

8.3.3 End-to-End RTN Management

End-to-end (E2E) network management is also referred to as trail management. Trail-based configuration can be performed by searching for NE-layer data on the U2000 or by configuring the network-layer data on the U2000 and the configuration is applied to all associated NEs. Trail-based configuration is easier than configuring NE data on a per-NE basis.

A license is required to perform end-to-end network management.

You can perform the following operations on the U2000:

- Create and maintain a microwave trail
 - Create a PDH microwave trail.
 - Generate a link server trail for the created PDH microwave trail automatically.
 - Create an SDH microwave trail.
 - Activate or deactivate a microwave trail.
 - Tributary Use timeslots with the minimum ID for route calculation.
- Manage the alarms and performance events related to a microwave trail.
 - Query current and historical alarms, current and historical performance data, UAT, and performance threshold-crossing records of a microwave trail.
 - Set the performance parameters for a microwave trail.
 - Query the microwave trails and customer information affected by an alarm.
- Filter trails in three ways
 - Filter all: Filter all trails and display only the qualified trails on a network
 - Secondary filter: Filter the displayed trails according to the filter criteria.
 - Incremental filter: Filter all trails and display the newly qualified trails together with the currently displayed ones.

Management of Packet Services

- Service Trail View Management

- Queries Layer 2 protocol configuration and status.
- Performs loopback tests on E-LAN networks.
- Creates performance monitoring tasks and queries historical and real-time performance data.
- PWE3 service management
 - Create multiple types of Eth PWE3 services.
 - Predeploy PWE3 services.
 - Automatically discover PWE3 services.
 - Modify, delete, filter, and view PWE3 services.
 - Manage multi-hop PWE3 services.
 - Manage PWE3 service protection.
 - View the topology of PWE3 services.
 - View the alarms of PWE3 services.
 - View performance events of PWE3 services.
 - Test and check PWE3 services.
 - Diagnosing PWE3 services.
 - Manage discrete PWE3 services.
 - Managing PWE3 services based on rights and domains.
 - Clone PWE3 services.
 - Manage PWE3 service templates.
 - Automatically generate Ethernet OAM for PWE3 services.
 - Set and view the status of port loopback of PWE3 services.
 - Import PWE3 service data from or export PWE3 service data to .xls files.
 - Perform one-key connectivity tests on CES services.
 - Set the VC12 loopback for CES services.
 - Display lower-layer (tunnel, Layer 2 link) alarms for PWE3 services.
 - Filter PWE3 services by subnet.
 - View the relative tunnel.
 - Monitor the PWE3 services.
 - Performing batch protection switchover.
- L3VPN management
 - Create an L3VPN service that supports the BGP/MPLS protocol.
 - Predeploy an L3VPN service.
 - Automatically discover L3VPN services.
 - Modify and delete L3VPN services, and view L3VPN services by using the filtering function.
 - View the topology of L3VPN services.
 - View the alarms of an L3VPN service.
 - Manage the performance of an L3VPN service.
 - Test and check L3VPN services.
 - Diagnose L3VPN services

- Manage discrete L3VPN services.
- Manage L3VPN services based on rights and domains.
- Manage L3VPN service templates.
- Configure the VRRP and BFD.
- Set and view the status of port loopback of L3VPN services.
- Display lower-layer (tunnel, Layer 2 link) alarms for L3VPN services.
- Automatically discover L3VPN services as scheduled.
- Tunnel management
 - Create static CR, RSVP, and IP tunnels.
 - Create static CR tunnel, RSVP tunnels in batches.
 - Predeploy tunnels.
 - Automatically discover tunnels.
 - Modify, delete, view, and filter tunnels.
 - View the topology of tunnels, including the working and protection routes.
 - View tunnel alarms.
 - View the performance events of a tunnel.
 - Test and check tunnels.
 - Diagnose tunnels.
 - Manage discrete tunnels.
 - Create, modify, delete, and automatically discover 1+1 or 1:1 tunnel protection groups.
 - Manually switch services in a 1+1 or 1:1 tunnel protection group.
 - Display the topology of 1+1 or 1:1 tunnel protection groups.
 - Create a tunnel and its protection tunnel at the same time.
 - Display the name of a tunnel in the global LSP view.
 - Set and view the status of port loopback of tunnels.
 - Configure OAM.
 - Copy static CR tunnels.
 - Display lower-layer (Layer 2 link) tunnel alarms.
 - Bulk change the switching status of tunnels in the tunnel management window.
 - Collect statistics on port bandwidth usage.
 - Filter tunnels by subnet.
 - Display the actual routing information of a static tunnel in the topology view of a protection group.
 - Filter dynamic tunnels by NE, board, or port.
 - View the correlated services of tunnels.
 - Adjust the route of a tunnel.
 - Re-optimize the RSVP TE tunnel.
 - Monitor the tunnel.
- VPLS Service Management
 - Create and discover the VPLS services, configure the Ethernet OAM.

- View the topology of the services, monitor the performance and alarm of the services.
- Modify and deleted the VPLS services.
- Diagnose the VPLS services fault by using the test suite.
- Composite service management
 - Manage VLAN+PWE3 composite services.
 - Query, modify, delete, and filter composite services.
 - View the topology of composite services, including viewing intra-service connections.
 - Display the status of composite services.

Native Ethernet Service Management

A license is required to manage end-to-end native Ethernet services on the U2000.

- Create and maintain native Ethernet services.
 - Automatically discover E-Line, E-LAN, E-Line_E-LAN services.
 - Create native Ethernet services.
 - Manage native Ethernet services.
 - Query E-Line discrete services.
 - Converting E-Line discrete services to mono nodal trails.
 - Modify native Ethernet services.
 - Perform LM/DM Test on native Ethernet services.
 - Query the MAC address learning results of E-LAN services and display each MAC address being diagnosed in the service topology.
 - Diagnose E-Line service faults.
 - Configuring CEs during native Ethernet service creation and management.
 - Verifying VLAN IDs for native Ethernet services, and displaying the service that is occupying the VLAN ID if detecting a VLAN ID conflict.
- Manage native Ethernet service alarms.
 - Query current and historical alarms of native Ethernet services.
 - Query native Ethernet services affected by an alarm.
 - Displaying alarm status and details for topological nodes in the topology view.
- Filter trails.
Filter all: Filter all trails and display only those that meet the criteria.
- Configuring Ethernet OAM.

E2E monitoring and troubleshooting for Layer 3 services on RTN+CX networks:

- Supports E2E discovery and display of services.
- Diagnoses service deterioration upon the reporting of IP Flow Performance Measurement (IP FPM) events.
- Diagnoses faults manually using the smart ping function.

8.4 PTN Network Feature Management

This topic describes the functions and features of PTN NE management and network management.

8.4.1 PTN NE Management

NE configuration includes the configuration of attributes, communications, services, protection schemes, and clocks on an NE.

Basic NE Configurations

The U2000 supports the following operations and features:

- Set the following NE attributes:
 - NE name
 - NE ID
 - Extended NE ID
 - Remarks
- Synchronize NE time: Specify the interval or exact time to automatically align the time of all NEs with the system time of the U2000 server.
- Display boards in plug-and-play (PnP) mode: After being inserted into slots, boards along with their information are automatically displayed in the NE Panel.
- Automatically disable NE functions: NE functions that affect services, such as loopback and automatic laser shutdown (ALS), are disabled at the schedule time.
- Set environmental monitoring information.
- Replace boards.
- Manage fans.

Configuration of Service Interface Types

The working mode and application scenarios of an interface are determined by the basic attributes, Layer 2 attributes, Layer 3 attributes and advanced attributes of the interface.

Basic attributes are the physical attributes of an interface. Layer 2 attributes are the data link layer attributes of an interface, such as ATM, VLAN, and QinQ. Layer 3 attributes are the network layer attributes of an interface, such as an IP attribute. Advanced attributes are the maintainability and service attributes of an interface.

Table 8-2 lists the types of PTN service interfaces supported by the U2000.

Table 8-2 Types of PTN service interfaces

Service Interface	Supported Port Mode/Encapsulation Type	Port Type	MP Group Supported or Not	Function
SDH interface	Basic attributes	Physical port	Not supported	Sets basic attributes for an SDH interface.
	Layer 2 attributes	Physical port	Not supported	Sets Layer 2 attributes for an SDH interface. The interface can then be used to carry ATM services.
	Layer 3 attributes	Physical port	Not supported	Sets Layer 3 attributes for an SDH interface. The interface can then be used to carry tunnels when the PPP protocol is enabled.
	Advanced attributes	Physical port	N/A	Sets advanced attributes for an SDH interface.
PDH interface	Basic attributes	Physical port	Not supported	Sets basic attributes for a PDH interface. The interface can then be used to carry TDM services.
	Layer 3 attributes	Physical port	Supported	Enables the PDH interface to act as a member in a Multilink PPP (MP) group after Layer 3 attributes are set for the interface and the PPP protocol is enabled.

Service Interface	Supported Port Mode/Encapsulation Type	Port Type	MP Group Supported or Not	Function
	Advanced attributes	Physical port	N/A	Sets advanced attributes for a PDH interface.
Ethernet interface	Basic attributes	Physical port	Not supported	Sets basic attributes for an Ethernet interface.
	Flow Control	Physical port	N/A	Sets flow control for an Ethernet interface.
	Layer 2 attributes	Physical port	Not supported	Sets Layer 2 attributes for an Ethernet interface. The interface can then be used to carry user-side or network-side Ethernet services.
	Layer 3 attributes	Physical port	Not supported	Sets Layer 3 attributes for an Ethernet interface. The interface can then be used to carry tunnels.
	Advanced attributes	Physical port	N/A	Sets advanced attributes for an Ethernet interface.
Ethernet virtual interface	Basic attributes	Logical port	Not supported	Sets basic attributes for an Ethernet virtual interface so that you can create VLAN subinterfaces, EOA virtual interfaces, or Layer 3 virtual interfaces.

Service Interface	Supported Port Mode/ Encapsulation Type	Port Type	MP Group Supported or Not	Function
	Layer 3 attributes	Logical port	Not supported	Sets Layer 3 attributes for a VLAN subinterface or an EOA virtual interface. After being configured with Layer 3 attributes, an EOA virtual interface can be used to carry IP or GRE tunnels, a VLAN subinterface can be used to carry L3VPN services or tunnels, and a Layer 3 virtual interface can be used to carry IP-Line services.

Service Interface	Supported Port Mode/ Encapsulation Type	Port Type	MP Group Supported or Not	Function
	Layer Mix	Logical port	Not supported	VE interface can be used in the line-free static L3VPN service interworking scenarios where layer 2 and layer 3 services interconnect with each other, the UNI interface of the layer 2 E-Line or E-LAN service is configured as an L2VE interface; a VLAN aggregation subinterface is created based on the L3VE interface; the UNI interface of the L3VPN service is configured as the VLAN aggregation subinterface. Then, layer 2 and layer 3 services are bound by using the bridging relationship between the VE interfaces. In this way, services can interconnect with each other without line connection

Service Interface	Supported Port Mode/ Encapsulation Type	Port Type	MP Group Supported or Not	Function
				between physical ports. VLAN aggregation subinterface is created based on the L3VE interface and used in the line-free static L3VPN service interworking scenarios where layer 2 and 3 services interconnect with each other.
	Advanced Attributes	Logical port	Not supported	The Password Encryption and Authentication parameters to the port can be set through setting the advanced attributes of Ethernet virtual interfaces.
ADSL interface	Basic attributes	Physical port	N/A	Sets basic attributes for an ADSL interface.
	DSLTRUNK attributes	Logical port	N/A	Sets DSLTRUNK attributes for an ADSL interface. The interface can then be used to carry ADSL signals.

Service Interface	Supported Port Mode/Encapsulation Type	Port Type	MP Group Supported or Not	Function
G.SHDSL interface	Basic attributes	Physical port	N/A	Sets basic attributes for a G.SHDSL interface.
	Binding mode	N/A	N/A	Sets the binding mode of a G.SHDSL interface to carry G.SHDSL signals.
	EFM binding group	Logical port	N/A	Configures an EFM binding group for a G.SHDSL interface.
	ATM binding group	Logical port	N/A	Configures an ATM binding group for a G.SHDSL interface.
	IMA binding group	Logical port	N/A	Configures an IMA binding group for a G.SHDSL interface to carry G.SHDSL signals.
Serial interface	Basic attributes	N/A	N/A	Sets basic attributes for a serial interface.
	Layer 3 attributes	Logical port	Supported	Makes a PPP-enabled serial interface act as a member in an MP group after Layer 3 attributes are set for the interface.
MP Group	Basic attributes	N/A	N/A	Sets basic attributes for an MP group.

Service Interface	Supported Port Mode/ Encapsulation Type	Port Type	MP Group Supported or Not	Function
	Layer 3 attributes	Logical port	N/A	Sets Layer 3 attributes for an MP group. The group can then be used to carry tunnels.

PTP ACR Unicast Interface

You can query the information about PTP ACR unicast interfaces, including IP addresses and IP masks.

IS-IS Protocol Configuration

The U2000 uses the intermediate system-to-intermediate system (IS-IS) protocol as a protocol of the network control plane, and supports the following operations:

- Configure node attributes.
- Configure port attributes.
- Import routes.
- Configure the link TE information.
- Configure GR sessions.
- Configure route aggregation.
- View route forwarding tables.

OSPF Protocol Configuration

The U2000 uses the open shortest path first (OSPF) protocol for the network control plane and provides the following configurations:

- Configure node attributes.
- Configure port attributes.
- Configure peer attributes.
- Import routes.
- Configure the link TE information.
- Configure route aggregation.
- Query peer information.
- View route forwarding tables.

MP-BGP Protocol Configuration

The U2000 uses the internal border gateway protocol (IBGP) to implement L3VPN functions, and supports the following operations:

- Configure IBGP instances.
- Configure IBGP peers.
- Configure route filtering policies.
- Configure and query the MP-BGP peer group parameters.

LDP Protocol Configuration

The U2000 uses the label distribution protocol (LDP) to create LSP connections and PW connections, and supports the following operations:

- Configure session attributes.
- Configure node attributes.
- Configure port attributes.
- Configure IP address filtering tables.
- Configure routing policies.
- Configure label policies.

RSVP Protocol Configuration

The U2000 uses the resource reserved protocol (RSVP) to create LSP connections, and supports the following operations:

- Configure node attributes.
- Configure port attributes.

Static Route Management Configuration

The U2000 supports the configuration of static route management.

Address Resolution Configuration

The U2000 supports the configuration of address resolution.

- Configure address parse.
- Configure ARP attributes.

Clock Configuration

The U2000 supports configurations of multiple clock modes:

- Configure clock domains in a unified manner.
- Query the status of clock synchronization.
- Configure the IEEE 1588 clock.
 - Configure clock services.
 - Configure clock synchronization attributes.
 - Configure the clock source priority tables.
 - Configure clock subnets.
 - Configure external time interfaces.
- Configure the ACR clocks

- Configure the CES ACR, 1588 ACR Multicast clocks and 1588 ACR Unicast clocks.
- Configure physical-layer clocks
 - Query the status of clock synchronization.
 - Set clock source priority tables, including
 - System clock source priority list
 - Priority for phase-locked sources of the first external clock output
 - Priority for phase-locked sources of the second external clock output
 - Set clock source switching parameters, including:
 - Clock source reversion parameters
 - Clock source switching conditions
 - Clock source switching control
 - Configure clock subnets, including:
 - Clock subnets
 - Clock quality
 - SSM output control
 - Clock ID status
 - Set phase-locked sources of external clock output, including:
 - Phase-locked sources of external clock output
 - Attributes of 2M phase-locked sources of external clocks
 - Set clock source status, including:
 - Clock Source
 - Direction
 - Output status
 - Mode
- Configure frequency selection mode.

Board-Level Protection Configuration

You can perform the following operations on the U2000:

- Configure TPS protection of a subboard.
- Configure board 1+1 protection for the SCC and cross-connect boards.
- Check the switching status.
- Perform protection switching.

Synchronization Protocol Configuration

In dual-homing application scenarios, both the MC LAG and the MC LMSP need to learn about the status of the opposite end and determine which actions to take based on the different types of failures that occur. With the configured information about the opposite end, a channel is established for control status synchronization between the two ends. In this manner, the sending and receiving of packets can be controlled and link fault detection can be performed.

LAG/MC LAG Configuration

A link aggregation group (LAG) aggregates multiple Ethernet physical links to form a logical link with a higher transmission rate. This function improves link availability and increases link capacity.

A multi-chassis (MC) LAG achieves load sharing between NEs.

The U2000 enables you to set the following LAG/MC LAG attributes:

- Load sharing type (sharing or non-sharing)
- LAG types (manual or static)
- Service distribution algorithm
- Port and system priorities

LMSP/MC LMSP Configuration

Linear MSP (LMSP) includes 1+1 linear MSP and 1:N linear MSP. The protection scheme uses the protection channel to protect services that are transmitted on the working channel. When the working channel fails, services are switched to the protection channel. Linear MSP is applicable to the POS interface and structured STM interface.

The multi-chassis (MC) LMSP can implement the LMSP between NEs.

The U2000 supports the following LMSP/MC LMSP configurations:

- Create LMSP groups.
- Check the status of LMSP groups.
- Perform LMSP switching.

MSTP Configuration

The multiple spanning tree protocol (MSTP) can be used to clear loops in a network. The MSTP uses a specific algorithm to block some redundant trails and change a loop network to a non-loop tree network. This function prevents packet increase in a loop network and generation of broadcast storms in an endless cycle. Unlike the STP and RSTP, the MSTP can forward data according to VLAN packets, achieving load balance of VLAN data.

The U2000 provides the following operations:

- Configure parameters of port groups and bridges.
- Configure CIST and MSTI parameters.
- Query CIST status and MSTI status.

IGMP Snooping Configuration

The Internet group management protocol snooping (IGMP Snooping) is a scheme of multicast constraints on Layer 2 equipment, and is used to manage and control multicast groups.

The U2000 supports the configuration of IGMP snooping for E-LAN services, and provides the following operations:

- Configure IGMP Snooping protocol parameters.
- Configure fast-leave ports.

- Manage routes.
- Configure route member ports.
- Query statistics of IGMP protocol packets.
- Manage Route Member Ports for V3.
- Configure SSM mapping.

BFD Configuration

The bidirectional forwarding detection (BFD) protocol can be used to check the Ethernet link status.

BFD is a simple Hello protocol. It is similar to the neighbor detection of well-known protocols in many aspects. A pair of systems periodically sends detection packets on the bidirectional channel where sessions between the two systems were created. If one system does not receive any detection packets from the other within a specific time, the system assumes that there is a failure on the bidirectional channel.

The U2000 supports BFD detection on IP and GRE tunnels, IGP, PWs, and static routes.

LPT Configuration

The link state pass through (LPT) protocol is used to return the remote-end link status to the near end. The near-end equipment performs operations according to the remote-end link status. When the intermediate transmission network is faulty, the LPT immediately informs the access equipment at both ends of the transmission network of the necessity to use the backup network. In this manner, the transmission of data, especially of important data, is ensured.

QoS Configuration

Quality of service (QoS) refers to the performance of the data flow transmission in a network. The QoS is used to ensure end-to-end service quality. The QoS cannot enhance the bandwidth, but it can minimize the delay and jitter in a network by properly allocating and monitoring network resources. In this way, the service quality is ensured.

The DiffServ (DS) domain consists of a group of network nodes with the DiffServ function. Nodes of this type are also called DS nodes. In a DS domain, all DS nodes adopt the same service provisioning policy to achieve the same per-hop behavior (PHB). DS nodes are classified into edge DS nodes and internal DS nodes. Edge DS nodes usually perform complex flow classification on the traffic that enters the DS domain. Traffic of different types is marked with different PHB service types. Internal DS nodes only need to perform simple flow classification based on PHB service types.

The U2000 supports the following QoS configurations:

- Configure QoS templates.
- Configure DiffServ domains.
- Configure ATM CoS mapping.
- Configure SVLAN DEI used flag.
- Configure simple flow classification and complex flow classification.
- Recognizes IPV6 ToS.

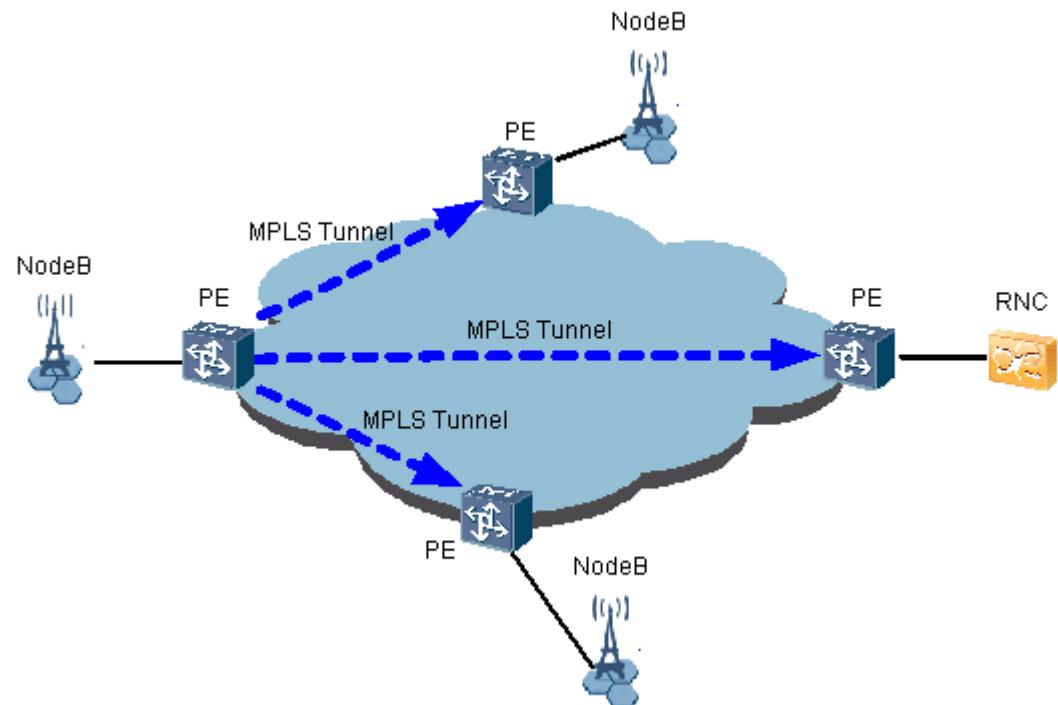
- Configure CAR and shaping.
- Configure color blindness modes.
- Configure WFQ schedule policies.
- Configure port WRED policies.
- Configure service WRED policies.
- Simplify operations and share some common QoS configuration parameters. The U2000 enables users to create QoS function point policies, including port policies, ATM policies, V-UNI ingress policies, V-UNI egress policies, PW policies, and QinQ policies. By using these function point policies, you can bind configurations for CAR attributes, shaping attributes, flow classification attributes, WFQ schedule policies, WRED policies, and color blindness modes.
- Configure CoS queue scheduling mapping.
- Configure QoS templates for applying the same QoS policies to multiple NEs.

MPLS Tunnel Configuration

The multi-protocol label switch (MPLS) protocol allows service packets to transmit transparently. The MPLS tunnel is defined by the MPLS protocol. Independent of services, an MPLS tunnel enables E2E transmission and provides channels for service-related PWs.

As shown in **Figure 8-5**, unicast MPLS tunnels are mainly used to transparently transmit point-to-point PWE3 services.

Figure 8-5 Unicast MPLS tunnels



The U2000 provides the following functions associated with MPLS tunnels on a per-NE basis:

- Configure MPLS basic attributes.
- Configure static unicast MPLS tunnels.
- Create forward and backward MPLS tunnels at the same time.
- Create static and bidirectional MPLS tunnels.
- Create the E-LSP.
- Manage PWs.
- Manage tunnel labels and PW labels.

MPLS Tunnel Protection Group Configuration

The U2000 provides the following functions associated with MPLS tunnel protection groups:

- Create MPLS tunnel 1+1 protection groups and MPLS tunnel 1:1 protection groups and configure the switching mode, revertive mode, wait-to-restore (WTR) time, and hold-off time for the groups.
- Perform MPLS tunnel protection switching.
- Query the status of an MPLS tunnel protection group.

MS PW Configuration

By creating multi-segment pseudo wires (MS-PWs) to transmit services, you can save tunnel resources and transmit services over different networks.

PW APS/MC PW APS Configuration

As a network protection mechanism, PW automatic protection switching (APS) is intended to protect the services on the working PW. That is, when the working PW malfunctions, the services on the working PW are switched to the protection PW. In this manner, the services on the working PW are protected.

The following PW APS/MC PW APS functions can be performed on a per-NE basis:

- Create protection groups.
- Bind the master and slave protection pairs.

IP Tunnel and GRE Tunnel Configuration

If the equipment at the two ends of an IP network does not support MPLS tunnels, PWE3 services can travel through the IP network by means of IP tunnels or GRE tunnels.

IP tunnels and GRE tunnels mainly apply to the offload scenarios of mobile communication.

The U2000 supports the configuration of bidirectional IP tunnels and GRE tunnels on a per-NE basis.

Supports Offload protection configuration between MPLS and IP/GRE tunnels.

Dual-Homing Protection Configuration

In dual-homing protection scenarios, two PE nodes (dual-homing nodes) are connected to one CE node through attachment circuit (AC) links so that the services received by the PE nodes at both ends of the bearer network can be protected.

The following types of dual-homing protection can be configured for ATM and CES services:

- 1:1 MC-PW APS and 1:1 MC-LMSP
- 1:1 MC-PW APS and 1+1 MC-LMSP
- 1:1 PW redundancy protection and 1:1 MC-LMSP
- 1:1 PW redundancy protection and 1+1 MC-LMSP

The following types of dual-homing protection can be configured for E-line services:

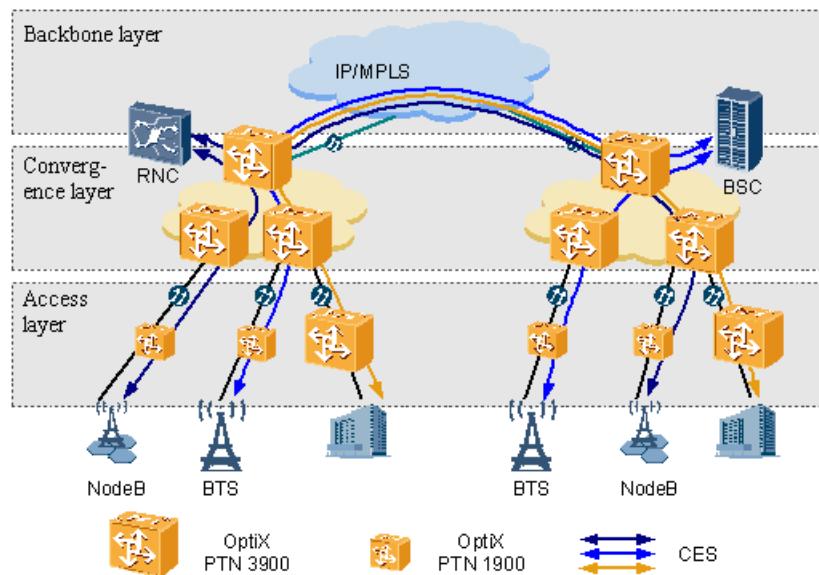
- 1:1 MC-PW APS and MC-LAG
- 1:1 PW redundancy protection and MC-LAG

CES Service Configuration

Circuit emulation services (CES services) achieve transparent transmission of TDM circuit switching data on the PSN.

As shown in **Figure 8-6**, the 2G/3G stations or enterprise private line accesses the PTN equipment by using the E1, T1, or channelized STM-1 line. The equipment divides the E1 and T1 signals into pieces and encapsulates the pieces on the Ethernet. Net, the E1 and T1 signals are transmitted to the opposite end by means of PWs.

Figure 8-6 CES service application model



The U2000 provides the following functions associated with CES services:

- Create CES services and corresponding PWs at the same time.
- Create UNI-UNI and UNI-NNI CES services.
- Create CES services in CESoPSN and SAToP modes. CESoPSN is short for structure-aware TDM circuit emulation services over packet switched network and SAToP is short for structure-agnostic TDM over packet.
- Configure QoS policies for CES services.
- Configure the value for idle timeslot recovery.

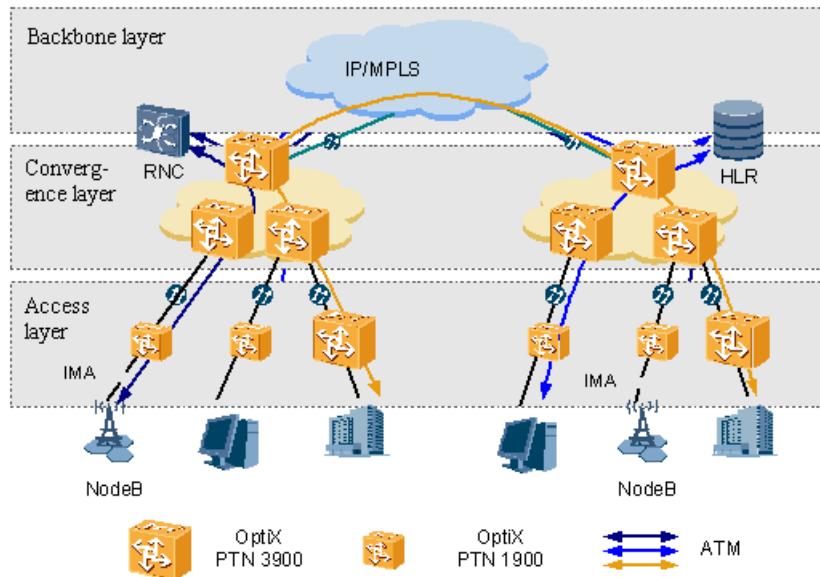
- Carry CES services over IP/GRE tunnels.
- Configure transparent transmission for CES service alarms.
- Modify the tunnel that carries PWs without interrupting services.

ATM Service Configuration

ATM emulation services achieve transparent transmission of ATM services on the PSN.

As shown in **Figure 8-7**, the 3G station accesses the PTN equipment by using the ATM IMA group. The equipment encapsulates the ATM cells into the Ethernet, and transmits the ATM cells to the opposite end by using the PW.

Figure 8-7 ATM service application model



The U2000 provides the following functions associated with ATM services:

- Create ATM services that contain multiple ATM connections.
- Create UNI-UNI and UNI-NNI ATM services.
- Create PVP and PVC ATM services.
- Create ATM services and corresponding PWs at the same time.
- Configure IMA groups.
- Configure QoS policies for ATM services.
- Configure CoS mapping.
- Modify the tunnel that carries PWs without interrupting services.

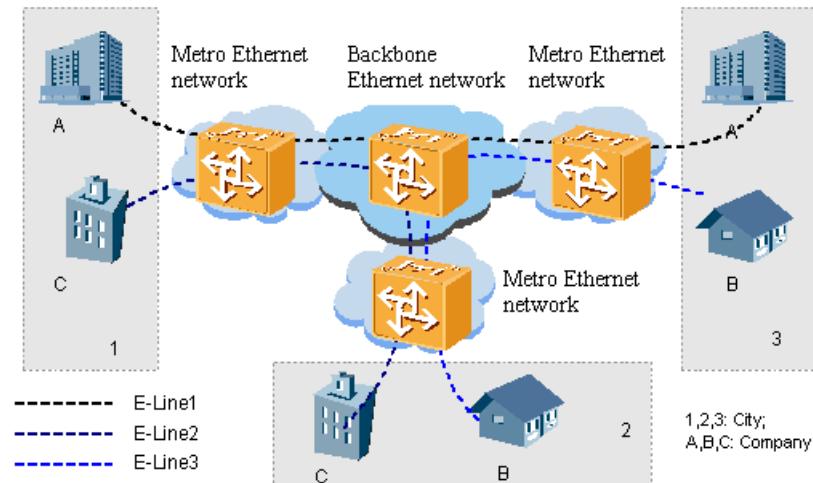
E-Line Service Configuration

E-line services achieve point-to-point transparent transmission of service data. The equipment transmits user packets from the user side to the network side based on Port or Port+VLAN.

As shown in **Figure 8-8**, company A has branches in City 1 and City 3. Company C has branches in City 1 and City 2. Branches of Company A or Company C that are in different

cities need data communication. The PTN equipment can provide E-line services for Company A and Company C, to meet their communication requirements. In addition, the service data can be completely isolated.

Figure 8-8 E-Line Service



The U2000 supports the following functions associated with E-Line services on a per-NE basis:

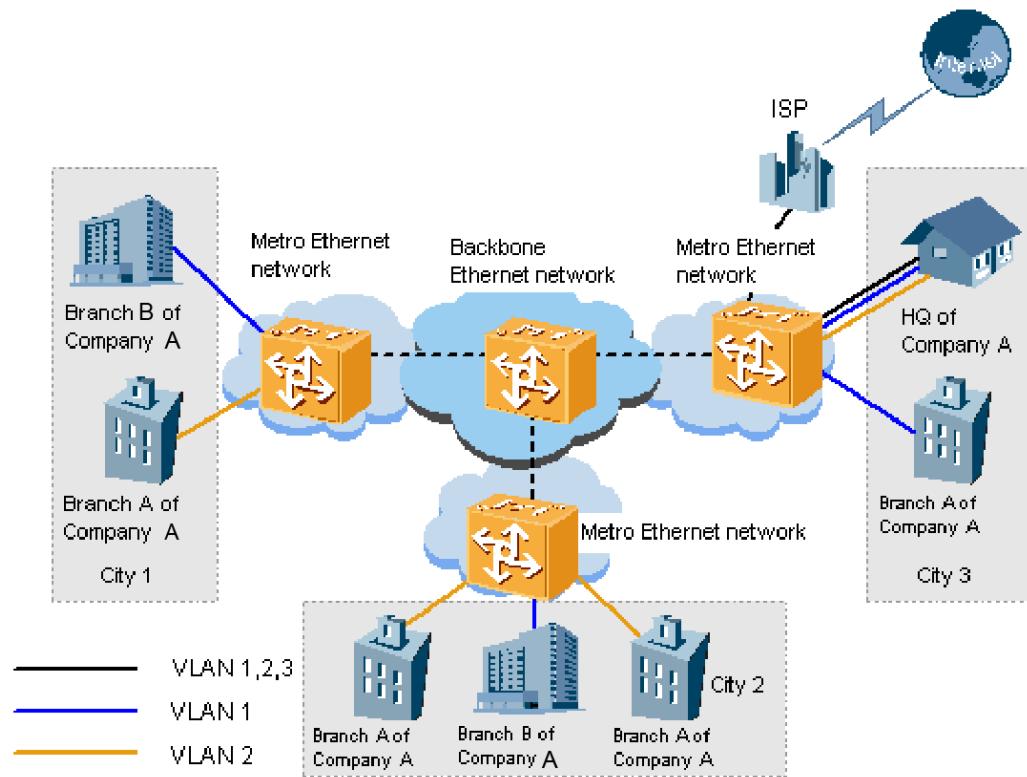
- Create UNI-UNI E-Line services.
- Create UNI-NNI E-Line services that are carried on ports.
- Create UNI-NNI E-Line services that are carried on PWs.
- Create UNI-NNI E-Line services that are carried on QinQ links.
- Configure QoS policies for L2VPN services and corresponding PWs during the creation of L2VPN services.
- Configure V-UNI groups.
- Modify the tunnel that carries PWs without interrupting services.

E-LAN Service Configuration

E-LAN service is multipoint-to-multipoint Ethernet service. Based on the self-learning of layer 2 MAC addresses, E-LAN services achieve packet forwarding between multiple V-UNI and NNI access points.

See **Figure 8-9**. The HQ of Company A is in City 3. Company A has Branch A in City 1, City 2, and City 3, and has Branch B in City 1 and City 2. Branch A and Branch B do not conduct any business with each other. The data should be isolated between the two branches. The HQ needs to communicate with each branch and access the Internet.

Figure 8-9 E-LAN Service



E-LAN services use different VLAN IDs to identify service data of different branches. In this way, data is shared within a branch and is isolated from the data for other branches. The Internet data of the HQ is also isolated from the internal service data by means of the VLAN.

The U2000 supports the following functions associated with E-LAN services on a per-NE basis:

- Create E-LAN services that are carried on ports.
- Create E-LAN services that are carried on QinQ links.
- Create E-LAN services that are carried on PWs.
- Configure the V-UNI and NNI interfaces of an E-LAN service.
- Configure the split horizon group of an E-LAN service.
- Configure V-UNI groups.
- Configure the MAC address learning parameters.
- Configure the unknown frame processing mode.
- Configure the static MAC address.
- Disable an MAC address.
- Configure the self-learning of MAC addresses.
- Modify the tunnel that carries PWs without interrupting services.

Service Mirroring Configuration

In service mirroring, all packets that enter a certain port are duplicated and then duplicated packets are transmitted through an observation port. In this manner, the service is scarcely

affected when packets of the mirrored service are analyzed. The product does not resolve or process the captured data.

You can configure local service mirroring.

MPLS OAM Configuration

MPLS OAM refers to a group of OAM functions that can check the quality of LSPs in an MPLS network. The MPLS OAM scheme can effectively detect, report, and handle a defect inside the network at the MPLS layer in addition to triggering protection switching when a malfunction occurs.

The U2000 provides the following MPLS OAM functions:

- Configure MPLS OAM parameters for tunnels.
- Perform CV/FFD checks.
- Perform LSP ping checks.
- Perform PW ping checks.
- Perform LSP traceroute checks.
- Perform PW traceroute checks.
- Enable and disable FDI.

Ethernet Service OAM Configuration

Ethernet service OAM refers to a group of end-to-end OAM functions that can check the quality of Ethernet links with multiple NEs. The Ethernet service OAM scheme can send OAM packets that are handled only at the MAC layer. As a low rate protocol, the OAM protocol occupies very low network bandwidth; therefore, it does not affect services carried on the link.

The U2000 provides the following Ethernet service OAM functions:

- Create maintenance domains (MDs), maintenance associations (MAs), maintenance end points (MEPs), and maintenance intermediate points (MIPs)
- Perform CC checks.
- Perform LB checks.
- Perform LT checks.

Ethernet Port OAM Configuration

Ethernet port OAM is mainly used to automatically check the connectivity and performance and locate faults on physical links under the MAC layer. It is used when the physical Ethernet ports are directly connected.

The U2000 provides the following Ethernet port OAM functions:

- Configure OAM parameters.
- Configure OAM error frame monitoring.

ATM OAM Configuration

ATM OAM refers to a group of end-to-end OAM functions that can check the quality of ATM links with multiple NEs. The ATM OAM functions check an ATM link by inserting some OAM cells with standard cell structures into the user cell flow.

The U2000 provides the following ATM OAM functions:

- Set segment end attributes.
- Perform CC activation tests.
- Perform remote loopbacks.
- Set the LLID.
- Insert OAM cell to ATM.

NMS Server Configuration

After the IP address of the NMS is configured on the gateway NE, all the managed non-gateway NEs can automatically go online after being powered on.

Power-Off Notification

The PTN equipment sends a power-off notification to the U2000 before it is totally powered off. According to this notification, the U2000 determines whether the failure to manage the equipment is caused by a power failure or a DCN fault such as a fiber cut.

Inter-Frame Gap Configuration

PTN equipment supports the adjustment of inter-frame gaps for ports, which can be used for the wire speed of ports.

Board Insertion and Removal Notification

When a faulty board is replaced, related indicators on the U2000 will blink.

Setting SNMP NMS Parameters

When the OSS obtains alarm and performance data from NE over SNMP, you need to configure IP address and permission control parameters of OSS on the U2000.

Setting Control Plane DCN Packet Priority and Bandwidth

In a DCN that packets travel on the control plane, DCN and service packets share the same forward channels. Therefore, you need to set the control plane DCN packet priority and bandwidth.

Adding 1+1 Protection for the AUX Board

AUX board 1+1 protection is added for PTN3900-8 equipment.

Performing a Network-Wide PRBS Test

Network-wide PRBS tests can determine network services function properly based on the bit error rate (BER) and the test results are displayed in a table or chart. The test results help maintenance engineers learn the QoS over the current service channel in time.

This feature provides the following functions:

- Viewing network-wide PRBS test status.
- Shifting from a record to the test result in the NE Explorer.
- Starting the test from a record.
- Stopping the test from a record.
- Querying the data from NE.
- Saving network-wide test results to files.
- Checking test-related CES services.

AIE Board Protection

This feature provides the following functions:

- Viewing protection status of AIE boards.
- Performing protection switching manually.

MPLS OAM Switching

This feature provides the following functions:

- Switching OAM recommendations.
- Switching to the OAM dual-stack mode.

Control Plane Configuration: VRF Cross-Connection Management

This feature provides the following functions:

- Binding public VRF tunnels automatically or manually.
- Querying VRF Cross-Connection Management.

MPLS-TP OAM Configuration

Complying with MPLS-TP standards, MPLS-TP OAM provides the following OAM functions for MPLS-TP networks:

- Checking, discovering, and locating a defect inside the network at the MPLS layer.
- Reporting and handling the defect.
- Triggering protection switching when a fault occurs.

This feature provides the following functions:

- Setting MEP parameters.
- Performing a CC check.
- Performing pings.

- Performing traceroutes.
- Performing LB tests.
- Performing LT tests.
- Performing TST tests.
- Checking packet loss ratios and delay.
- Performing Throughput tests.
- Configuring maintenance intermediate points (MIPs).

The 802.1X/Remote Authentication dial-in User Service (RADIUS) Management

To perform security authentication for base stations connected to ensure security of the bearer network, and to control access of PTN edge equipment based on authentication results.

MPLS Ring Protection Management

This feature adds an independent ring layer, which does not affect services. The MPLS ring protection, similar to SDH ring protection, provides reliable protection capabilities to withstand multi-node failures. This feature provides the following functions:

- To discover MPLS rings automatically.
- To view the topology of MPLS rings.
- To refresh and query the protection switching status of MPLS rings.
- To create MPLS protection ring protection.
- To manage MPLS ring protection.
- To delete MPLS ring protection.
- To bind a tunnel to or unbind a tunnel from a protected MPLS ring.
- To unbind multiple tunnels from a protected MPLS ring at a time.
- To diagnose faults on protected MPLS rings.
- To display alarms for protected MPLS rings.
- To configure or delete the intersecting nodes of protected MPLS rings.

Network Resource Statistics Report

The network resource statistics report is used to collect live-network statistics for planning customers' networks. This feature provides the function of collecting the numbers of the following items:

- Nodes
- IS-IS peers
- Data communication network (DCN) links
- DCN nodes
- Tunnels
- L2VPN PWs
- L2VPN T-LDP peers
- L3VPN VRFs
- L3VPN routes, including L3VPN routes at the local end

- L3VPN BGP peers

Association Between Channel Alarms on Relays and Channel Names

The U2000 separately displays alarms for different channels and allows users to define alarm names.

Plus Sign (+) in NE Names

The U2000 allows the plus sign (+) in NE names to meet NE naming requirements.

Link-based IP Ping

The U2000 adds Ping to the shortcut menu for fibers in the Main Topology. This feature facilitates link continuity checks.

PTN LAG Protection Group Configuration Export

This feature allows users to export PTN LAG protection groups to files using the Save As operation and view the configurations of the LAG protection groups. The file format can be XLS, CSV, HTML, and TXT.

Service Mapping Diagram

The service mapping diagram feature allows users to view port and channel usage, query services efficiently, and switch between windows. The U2000 supports the service mapping diagrams of Ethernet, E1, channelized STM-1, and POD41 boards.

Support PTN NE replacement

To replace PTN NEs if they are faulty and restore their data to new NEs, which improves the fault recovery efficiency.

Support the data communications channel (DCC) view

- To ascertain the network locations of PTN NEs quickly during new deployment by searching for them in the DCC view.
- To find data communication network (DCN) links between a PTN NE and its gateway NE by querying DCC link information in the DCC view during maintenance, which facilitates DCN fault diagnosis.
- To query the scale of a single DCN domain and export the scale data of network-wide DCN domains.

Support NE-level Performance Monitoring Templates for PTN NEs

To monitor the performance of one or multiple PTN NEs quickly, which improves the performance monitoring efficiency on PTN networks.

Support Checking PTN Network Health

Health check on PTN networks is performed on a graphical user interface (GUI) for centralized check and performance indicator monitoring, by which users can check the current

and historical running status of networks in routine maintenance. In this way, network risks are fixed in time to prevent network problems.

Support the Interconnection Between Layer 2 And Layer 3 Services Without Line Connection Between Physical Ports

In the line-free static L3VPN service interworking scenarios, you need to create a Virtual Ethernet (VE) group to connect the L2VE interface with the L3VE interface. In this manner, layer 2 services can be forwarded internally to layer 3 services, which avoids line connection between physical ports, saves port resources, and simplifies operations.

Test Suite Function Enhancement

- Supports creation of continuous ping test suites and definition of alarm thresholds.
- Supports creation of test cases through duplication.

TWAMP Check

- Allows PTN devices to support TWAMP (RFC 5347) tests in L3 PTN or edge access PTN scenarios.
- Supports performance task creation in the PMS module, allows the U2000 to collect performance indicators, and displays delay, packet loss, and jitter indicators in figures and tables.

Support the Syslog Feature

Allows logs to be backed up to the external Syslog server either manually or at a self-defined interval.

Support Obtaining of Packet Headers

Supports obtaining of packet headers and record them to files during PTN network fault locating, which helps analyze faults in detail. The U2000 does not parse or handle the obtained packet headers.

8.4.2 E2E PTN Management

End-to-end (E2E) network management is also referred to as trail management. Trail-based configuration can be performed by searching for NE-layer data on the U2000 or by configuring the network-layer data on the U2000; then the configuration is applied to all associated NEs. Trail-based configuration is easier than configuring NE data on a per-NE basis.



A license is required to perform E2E network management on the U2000.

PWE3 Service Management

- Create multiple types of PWE3 services such as ATM, CES, ETH, and IP over PW.
- Predeploy PWE3 services.
- Automatically discover PWE3 services.

- Modify, delete, and filter PWE3 services to view the desired services.
- Manage multi-hop PWE3 services.
- Manage PWE3 service protection.
- View the topology of PWE3 services.
- View the alarms of PWE3 services.
- Manage performance of PWE3 services.
- Test and check PWE3 services.
- Diagnosing PWE3 services
- Manage discrete PWE3 services.
- Managing PWE3 services based on rights and domains.
- Clone PWE3 services.
- Manage PWE3 service templates.
- Automatically generate Ethernet OAM for Ethernet services.
- Set and view the status of port loopback of PWE3 services.
- Import PWE3 service data from or export PWE3 service data to .xls files.
- Perform one-key connectivity tests on ATM and CES services.
- Set the VC12 loopback for CES services.
- Display lower-layer (tunnel, Layer 2 link) alarms for PWE3 services.
- Filter PWE3 services by subnet.
- Migrate PWE3 services.
- View the relative tunnel.
- Monitor the PWE3 services.
- Manage the PWE3 services protection switching.
- Convert a discrete service to an unterminated service.
- Performing batch protection switchover.
- Support bandwidth connection admission control (CAC).
- Implement the MPLS-TP OAM configuration, MPLS-TP OAM tests, MPLS-TP performance monitoring and alarm association.
- Support deployment and undeployment of discrete services.

VPLS Service Management

- Create VPLS services.
- Predeploy VPLS services.
- Automatically discover VPLS services.
- Modify and delete VPLS services, and view VPLS services by using the filtering function.
- View the topology of VPLS services.
- View the alarms of VPLS services.
- Manage the performance of VPLS services.
- Test and check VPLS services.
- Diagnose VPLS services

- Manage VSI Resource.
- Manage VPLS services based on rights and domains.
- Manage VPLS service templates.
- Automatically generate Ethernet OAM for VPLS services.
- Set and view the status of port loopback of VPLS services.
- Display lower-layer (tunnel, Layer 2 link) alarms for VPLS services.
- Migrate VPLS services.
- Implement scheduled automatic discovery of VPLS services.
- Migrate VPLS services of the Label Distribution Protocol (LDP) signaling based on ports.

L3VPN Service Management

- Create Full-Mesh and Customized static L3VPN services.
- Predeploy an L3VPN service.
- Automatically discover L3VPN services.
- Modify and delete L3VPN services, and view L3VPN services by using the filtering function.
- View the topology of L3VPN services.
- View the alarms of an L3VPN service.
- Manage the performance of an L3VPN service.
- Test and check L3VPN services.
- Diagnose L3VPN services
- Manage discrete L3VPN services.
- Manage L3VPN services based on rights and domains.
- Manage L3VPN service templates.
- Configure the VRRP and BFD.
- Set and view the status of port loopback of L3VPN services.
- Display lower-layer (tunnel, Layer 2 link) alarms for L3VPN services.
- Automatically discover L3VPN services as scheduled.
- Support deployment and undeployment of discrete services.

Tunnel Management

- Create static CR, RSVP, LDP, and IP tunnels.
- Create static CR, RSVP and LDP tunnels in batches.
- Predeploy tunnels.
- Automatically discover tunnels.
- Modify, delete, filter, and view tunnels.
- View the topology of tunnels, including the working and protection routes.
- View tunnel alarms.
- Manage the performance of tunnels.
- Test and check tunnels.

- Diagnose tunnels.
- Manage discrete tunnels.
- Create, modify, delete, and automatically discover 1+1 or 1:1 tunnel protection groups.
- Switch services in a 1+1 or 1:1 tunnel protection group manually.
- Display the topology of 1+1 or 1:1 tunnel protection groups.
- Create a tunnel and its protection tunnel at the same time.
- Display the name of a tunnel in the global LSP view.
- Manage bidirectional static tunnels.
- Set and view the port loopback status of tunnels.
- Duplicate static CR tunnels.
- Display lower-layer (Layer 2 link) tunnel alarms.
- Bulk change the switching status of tunnels in the tunnel management window.
- Collect statistics on port bandwidth usage.
- Filter tunnels by subnet.
- Display the actual routing information of a static tunnel in the topology view of a protection group.
- Filter dynamic tunnels by NE, board, or port.
- View the correlated services of tunnels.
- Adjust the route of a tunnel.
- Re-optimize the RSVP TE tunnel.
- Monitor the tunnel.
- Export tunnel service data from the U2000 to .xls files and import the .xls files containing tunnel service data to the U2000.
- Implement the MPLS-TP OAM configuration, MPLS-TP OAM test, MPLS-TP performance monitoring and alarm association.

MPLS Protection Ring Management

- Creates/deletes a single protection ring or intersecting rings.
- Bind/unbind a tunnel to one or multiple MPLS protection rings.
- Select one or more tunnels and bound the tunnels to rings in batches
- Views MPLS protection ring alarms.
- Deletes MPLS protection rings from the network side.
- Performs MPLS protection ring switchovers.
- Add NEs to an MPLS protection ring or Delete NEs from an MPLS protection ring for capacity expansion.
- Adjust NE interfaces about the MPLS protection ring.

LMSP Management

- Discovers LMSP services automatically.
- Starts or stops the APS protocol.
- Modifies LMSP information.

- Performs LMSP switchovers.
- Deletes LMSP services.

Composite Service Management

- Manage composite services: Composite services can be created in user-defined, H-VPLS, and PWE3 services in static L3VPN.
 - Custom: All types, such as PWE3+PWE3, PWE3+E-AGGR, PWE3+EPL, PWE3+E-Line, and PWE3+SDH types of composite services can be created by configuring basic attributes, service components, and connection points manually.
 - H-VPLS: Service components and connection points can be automatically created by configuring basic attributes and adding service nodes of composite services. The creation process is simplified but only H-VPLS composite services can be created.
 - In PWE3 in Static L3VPN N:1 mode, the U2000 automatically creates qualified PWE3+L3VPN services after the gateway IP address is set, the static L3VPN is selected, and PWE3 is added.
- Manage the performance of a composite service.
- Modify and delete composite services, and view composite services by using the filtering function.
- Automatically discover composite services.
- View the topology of composite services, including the internal connections between the services.
- Display the status of composite services.
- Automatically discover composite services as scheduled.
- Supported jumping to view the service components from composite services.
- Diagnose composite service:
 - Ethernet OAM detection
 - inter-service detection for a PWE3 service accesses a static L3VPN composite service
 - MPLS-TP OAM detection for H-VPLS composite service
 - PW fast diagnosis for H-VPLS composite service

Native Ethernet Service Management

A license is required to manage end-to-end native Ethernet services on the U2000.

- Create and maintain E-Line services.
 - Create E-Line services.
 - Manage E-Line services.
 - Query E-Line discrete services.
 - Automatically discover E-Line services.
 - Converting E-Line discrete services to mono nodal trails.
 - Modify E-Line services.
- Manage E-Line service alarms.
 - Query current and historical alarms of E-Line services.

- Query E-Line services affected by an alarm.
- Filter trails.
Filter all: Filter all trails and display only those that meet the criteria.

Layer 2 Multicast Service Management

- Creates Layer 2 multicast services, including the creation of a root ring and attachment of other rings.
- Predeploys Layer 2 multicast services.
- Automates the discovery of Layer 2 multicast services.
- Modifies, deletes, and filters out Layer 2 multicast services.
- Synchronizes Layer 2 multicast services.
- Views paths in the topology.
- Views Layer 2 multicast service alarms.
- Diagnose Layer 2 multicast services.
- Enables APS protection switchovers.
- Views switchover status.
- Views the tunnels carried on PWs.
- Provides management functions for E-Tree nodes, involving viewing, filtering out, deleting, deploying, and releasing E-Tree nodes.

Network Slice

- Creates channelized sub-interface.
- Configures network slice for interface or channelized sub-interface.
- Modifies and deletes the slice link.
- Views the topology of the slice link.
- Views MPLS protection ring/Tunnel/VPN service information of the slice link.
- Configures and modifies network slice for MPLS protection ring/Tunnel/VPLS/PWE3/L3VPN/Layer 2 Multicast services.

8.5 Router Feature and Switch Feature Management

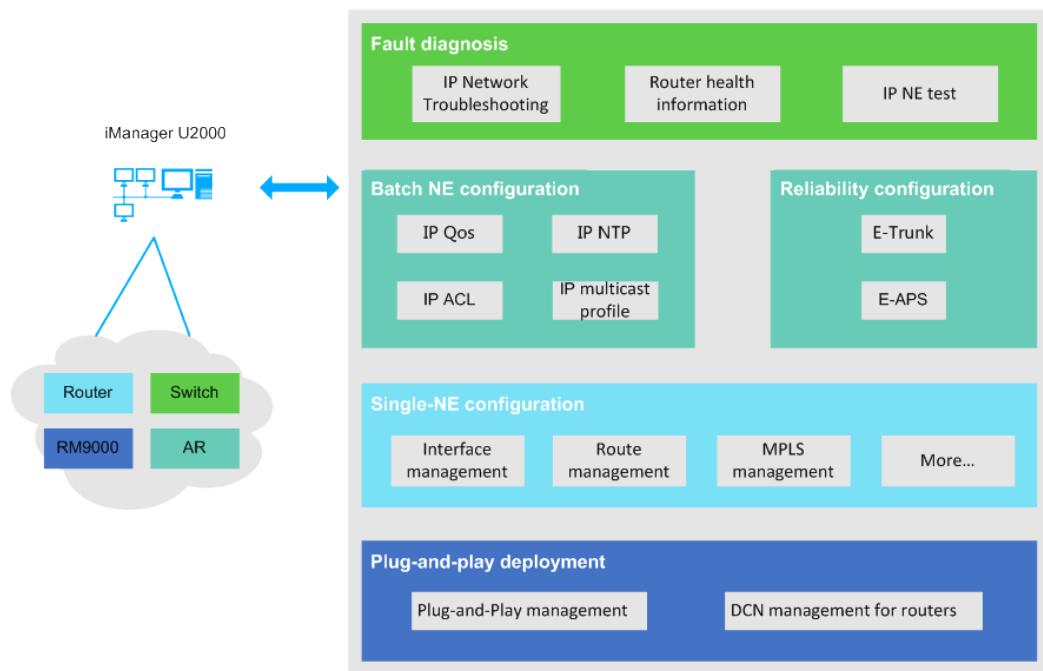
This topic describes router features and switch features.

8.5.1 Overview of Router and Switch Management

Panorama of Router and Switch Management

[Figure 8-10](#) shows the panorama of router and switch management.

Figure 8-10 Panorama of router and switch management



Version Mappings Between the U2000 and NEs

Version mappings between the U2000 and NEs are fixed. For details about the version mappings, see relevant chapters in the "Manageable Equipment Versions" part. If a manageable NE needs to be upgraded to a version that is not supported by the U2000, the U2000 must also be upgraded to a mapping version.

The U2000 can support old features without being upgraded, only can be compatible with the following items:

- New boards
- New NE versions
- New NE models of the same series

NOTE

For details about the compatibility between NEs and the U2000 of previous versions, see the chapter about version compatibility in the Release Notes released for the associated NE.

NOTICE

When using the U2000 of a compatible version to manage NEs, observe the following rules to ensure the proper running of services on the live network:

- Do not use new or extended command lines in the new NE version. For the list of the command lines, see relevant documents released for the associated NE.
- Do not manage NEs using both the U2000 and command lines.

NE Virtual System Management by the U2000

Virtual system (VS): The network administrator divides a physical device into multiple virtual devices that execute independent routing tasks. Different virtual devices share the same software and all public resources. That is, different VSs share the same control board and interface board. Each interface can belong to only one VS. A physical router is virtualized into multiple virtual routers. Services between virtual routers do not affect each other, and multiple routers are represented externally.

The U2000 manages VSs by independent NE. The NE types, consumed NE licenses, and equivalent coefficients are the same as those of physical NEs.

8.5.2 Network Deployment

8.5.2.1 IP Plug and Play

The IP Plug and Play can be used to complete remote commissioning and basic configuration for multiple NEs, freeing engineers from going to sites and improving the deployment efficiency greatly.

Deployment Scenario

The IP Plug and Play is used in the process of making scripts and configuring NEs during deployment, helping to implement graphical CLI. You need to set only a few of parameters for generating basic NE scripts. The DCN remote commissioning mode does not need any planning before NE power-on, and NEs can be automatically added to the U2000 for management.

During deployment, the IP Plug and Play is mainly used for remote commissioning and online for newly added NEs, allowing the U2000 to manage the NEs. The IP Plug and Play can be used to deploy basic configurations to NEs for different networking scenarios to complete batch NE deployment.

U2000 operators can use the IP Plug and Play or Unistar to perform network planning. The plug-and-play function can be implemented after the planning list is imported to the IP Plug and Play.

System-defined Template

Configuration templates are defined in the system for IPRAN scenarios. You can select a desired template and set a few parameters to generate a script.

Remote Commissioning

The plug-and-play management module supports two remote commissioning methods:

- Remote commissioning using DCN

An NE automatically negotiates a route using a routing protocol after it is powered on. The U2000 connects to the NE through the gateway NE by Telnet/STelnet and applies basic configurations to the NE.

- Remote commissioning using DHCP

The plug-and-play management module integrates with a DHCP server. After an NE is powered on, it exchanges DHCP packets with the plug-and-play management module

through the upstream NE and obtains an IP address. The plug-and-play management module applies basic configurations to the NE.

- Remote commissioning using HTTPS

After a VRouter is powered on, it sends an HTTPS packet that carries information such as management IP address and device name to the plug-and-play management module. A user logs in to the VRouter using STelnet to verify received information and configure commands.

Offline Script Verification

The plug-and-play management module allows you to modify scripts in offline mode. The plug-and-play management module automatically verifies generated scripts and displays verification results in different colors to ensure that all configurations are compliant with command line standards. This function supports only command syntax check, rather than service logic check.

Quick Template Generation

Scripts can be used to generate templates in one-click mode, facilitating the similar configuration in subsequent operations.

Interconnection to the Unistar

The .xls file generated by exporting the network information that network planning engineers plan in the Unistar can be imported to the plug-and-play management module to generate link planning and NE information.

VBNG Auto-Online Function

You can remotely commission and deliver basic configurations to VBNG using the plug-and-play management function, which requires no software commissioning engineers to visit sites during site deployment and therefore greatly improves efficiency.

8.5.2.2 Router Management

Router management allows you to configure and maintain routers by means of the graphical user interface (GUI).

 **NOTE**

- Routers include NE, CX, ATN, AR, R, and PTN6900 series NEs.
- Supported features may vary with NE versions. For details, contact Huawei technical engineers to obtain *Performance Event List & IP domain NE Feature List* in *Bidding Support Documents* of the mapping U2000.

Device Management

- Automatically identify device types and software versions to implement device-based management.
- Automatically obtain and refresh information about entities such as subracks, boards, power supply units, fans, and ports, and monitor status of these entities.
- Display the front panel view of an NE, including subracks, boards, power supply units, fans, and ports in the NE Panel.

- Display the running status and alarm status of boards and ports in the NE Panel by using alarm indicators and colored legends.
- Perform the following operations on the NE panel: view common information and alarms of NEs, boards, and ports; view real-time performance of boards and ports; reset boards and daughter boards; perform active/standby switchover for control boards and multi-subrack cluster NEs.
- Monitor link and NE status, collect monitoring data, and export the monitoring data to text files, which makes it convenient for users to summarize, analyze, and report the data.
- The wavelength and wave band management function is used to connect routers and WDM equipment and achieves fiber multiplexing between WDM equipment during service data transmission, thereby reducing fiber resources.
- Supports laser management, when an optical module is used, you can turn on the laser and specify the parameters of the laser.
- Supports Ethernet Power Supply function. In this case, using the router to directly supply power for the IP phone and wireless assess points, helps reduce NE deployment costs. If the NE is connected to an external power supply, PoE becomes a backup power supply solution to ensure that the NE can run more stably.

LLDP Management

The U2000 can discover Layer 2 links and display them if the Link Layer Discovery Protocol (LLDP) function is configured for NEs and interfaces.

You can perform the following operations on the U2000:

- Configure LLDP globally.
- Configure LLDP on interfaces.
- Synchronize LLDP neighbor information.

NE Channel Management

You can configure management channels on NEs. Detailed features are VTY configuration, File Transfer Protocol (FTP) service, local user management, log service, alarm service, and Secure Shell (SSH) service.

Clock Management

Routers must support clock/time synchronization to meet requirements of base stations on an IP radio access network (IP RAN).

The U2000 supports Precision Time Protocol (PTP) clock management, physical clock management, querying the clock tracking status, and view the switching records of the clock source for routers.

With the PTP clock management function, you can perform the following operations on the U2000:

- Configure global PTP information.
After global PTP is configured for all NEs on the clock synchronization network, PTP clock signals can be properly transmitted over the clock synchronization network.
- Configure a local or BITS clock source and port PTP attributes.

- Configure an adaptive clock.

With the physical clock management function, you can perform the following operations on the U2000:

- Configure global physical clock information.
- Configure a port clock source or another clock source.
 - A port clock source is configured on a router port. To configure a port clock source, you must select the desired port manually and set mandatory parameters such as clock enabling and SSM level.
 - Another clock source can be the BITS or PTP clock source of a router. On the U2000, such a clock source cannot be created and only its attributes can be queried or modified.

DCN Communication Management

Supports configuring DCN communication parameters on U2000 and gateway NEs to implement remote commissioning and automatic discovery of non-gateway NEs on the U2000.

Interface Management

You can configure a variety of media interfaces on the U2000, including physical and logical interfaces.

- Physical interfaces indicate the interfaces that physically exist on components such as boards. The U2000 supports configuration of Ethernet interfaces, packet over SDH/SONET (POS) interfaces, channelized POS (CPOS) interfaces, asynchronous transfer mode (ATM) interfaces, E1 interfaces, and other interfaces.
- Logical interfaces indicate the interfaces that do not exist physically but can exchange data. They are created through configuration. The U2000 supports configuration of subinterfaces, trunk interfaces, tunnel interfaces, virtual Ethernet (VE) interfaces, loopback interfaces, virtual template (VT) interfaces, virtual local area network (VLAN) interfaces, ATM-Bundle interfaces, inverse multiplexing over ATM (IMA)-group interfaces, and other interfaces.

The interface monitoring group manages access-side interface status based on network-side interface status to ensure that services are switched to the standby link if a fault occurs on the active link. This prevents traffic overloads and traffic forwarding failures.

Ethernet Feature Management

Ethernet is a main TCP/IP LAN and MAN technology that features fast data transmission, excellent compatibility, and low costs. You can perform the following operations on the U2000:

- Configure global VLANs, port VLANs, VLAN stacking, and VLAN mapping.
- Manage media access control (MAC) addresses.
Setting static MAC addresses, MAC address learning rules, and MAC address aging time, and querying dynamic MAC addresses.
- Manage VLAN switches.

ACL Management

An ACL defines a set of rules that determine what packets are permitted to pass through NEs.

You can perform the following operations on the U2000:

- Configure a time range in which ACL rules take effect. Absolute time range and periodic time range are available.
- Configure an ACL group to define the type, matching order, and step of ACL rules. One ACL group can contain one or multiple ACL rules.
- Configure ACL rules, namely, basic rules, advanced rules, interface rules, Ethernet frame header rules, Layer 2 rules, and simple rules.

ANCP Management

The Access Node Control Protocol (ANCP) facilitates the transmission of control messages between a BRAS and an access node, and implements neighbor configuration, access configuration, and OAM for access user ports.

The U2000 supports the following ANCP functions for routers:

- Global ANCP management
- Access management
- Neighbor management

Route Management

The U2000 supports IPv4 route configuration and maintenance for NEs. Route Management just supports managing IPv4 route.

You can perform the following operations on the U2000:

- View routing information.
- Configure global parameters for routes.
- Configure IP address prefixes.
- Configure routes, including static routes, Border Gateway Protocol (BGP) routes, Open Shortest Path First (OSPF) routes, and Intermediate System to Intermediate System (IS-IS) routes.
- Configure routing policies.
- View the running information about OSPF and IS-IS, the BGP peer, the BGP peer group, as well as the BGP peer and BGP peer group in a VPN instance address family.

Multicast Management

The multicast technology implements highly-efficient P2MP data transmission on an IP network. In multicast mode, a data flow is simultaneously sent to a group of users along the multicast distribution tree. Only one copy of the multicast data flow is available on every link. Compared with the unicast mode, the multicast mode reduces the server and CPU load, and the growth of users does not greatly increase the network load. The U2000 supports the following multicast management functions:

- Layer 2 multicast management

The U2000 supports VSI-based Layer 2 multicast features of routers, including Internet Group Management Protocol (IGMP) snooping, source-specific multicast (SSM) mapping, multicast call admission control (CAC), and multicast group configuration.

- Layer 3 multicast management

The U2000 supports IGMP, Protocol Independent Multicast (PIM), Multicast Source Discovery Protocol (MSDP), and Layer 3 VPN rendezvous point RP (L3VPN) configuration and management.

VPN Management

In NE VPN management, provider edge (PE) devices can be configured in per-site mode to establish services that do not have basic service information such as service names and associated customers. Data configured for NE VPN management and IP end-to-end services can be shared in the U2000 database. That is, VPN management data configured in the NE Explorer can be used by IP end-to-end services.

VPN management supports functions such as tunnel policy management, PW template management, CCC management, PW management, SPW management, MAC address binding, VSI management, VRF management, and VPN group management.

MPLS Management

Multiprotocol label switching (MPLS) is used to transparently transmit packets between users. The U2000 supports NE-level MPLS management.

You can perform the following operations on the U2000:

- Enable MPLS, Label Distribution Protocol (LDP), MPLS Layer 2 virtual private network (L2VPN), and MPLS OAM globally or on interfaces.
- Configure MPLS traffic engineering (TE), Constraint Shortest Path First (CSPF), Resource Reservation Setup Protocol with Traffic-engineering Extensions (RSVP-TE), OSPF-TE, and IS-IS TE capabilities.
- Configure and debug LDPS.
- Configure static unidirectional and bidirectional label switched paths (LSPs).
- View label forward information bases (FIBs).
- Count LSPs.
- Configure tunnels.
Configuring basic tunnel capabilities, tunnel attributes, tunnel applications, and tunnel protection.
- Configure MPLS OAM detection and MPLS OAM protection groups.

QoS Management

Quality of Service (QoS) functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users. The U2000 performs QoS management on Datacom devices through the CBQoS, HQoS, discard policy, DS domain policy, interface QoS configuration, mirroring configuration, and system QoS tool. You can perform the following operations on the U2000:

- Configure and manage traffic classifications, traffic behavior, and traffic policies.
- Configure and manage interface QoS and system QoS.

- Configure DiffServ domain policies.
- Configure and manage traffic mirroring and port mirroring. In this manner, the product does not resolve or process the captured data.
- Configure and manage hierarchical QoS (HQoS) functions, including discard policies, HQoS traffic queue policies, HQoS traffic queue mapping, HQoS schedulers, HQoS user scheduling, and QoS templates.
- Generate a global template from certain existing QoS configurations and bulk apply the template to NEs, improving deployment efficiency.

Ethernet OAM Management

Ethernet operation, administration, and maintenance (OAM) is mainly used to check connectivity, evaluate performance, and locate faults for Ethernet links. The IEEE 802.1ag and IEEE 802.3ah are used to implement Ethernet OAM. With IEEE 802.1ag, the U2000 can continuously monitor user services, and acknowledge and locate faults. With IEEE 802.3ah, the U2000 can monitor last-mile user services and report faults.

You can perform the following operations on the U2000:

- Manage global information.
- Use IEEE 802.1ag-related functions. Specifically, manage and maintain the following items: maintenance domains (MDs), maintenance associations (MAs), local maintenance association end points (MEPs), remote MEPs, and maintenance association intermediate points (MIPs). You can also perform connectivity fault management-bidirectional forwarding detection (CFM-BFD) binding and CFM-CFM binding.
- Use IEEE 802.3ah-related functions. Specifically, configure the Ethernet OAM protocol, query ports, perform loopback tests, and perform Ethernet in the first mile (EFM)-BFD binding and EFM-CFM binding.
- Manage tests and diagnoses.
- Collect OAM statistics.
- Y.1731

The following Y.1731 functions can be configured and managed:

- For PWE3, VPLS, and VLAN services in on-demand mode, packet discard and delay at a single end, delay at both ends, and OAM configuration and statistical collection are supported.
- For PWE3, VPLS, and VLAN services in proactive mode, packet discard at both ends and OAM configuration are supported.
- Test flow management: Both on-demand or continuous statistics about delay and packet loss are collected in point-to-multipoint scenarios.

MPLS-TP OAM Management

MPLS-TP OAM can effectively detect, identify, and locate faults at the MPLS-TP client layer and quickly switch traffic when links or nodes fail.

- Performs MPLS-TP OAM management on PWE3 services and bidirectional static LSPs.
- Performs section OAM management.
- Collects statistics about single-ended frame loss, one-way frame delay, and two-way frame delay in on-demand mode and dual-ended frame loss in proactive mode.

ATM OAM Management

ATM OAM is implemented based on ATM service streams. It is used to detect and locate ATM link connectivity faults. The U2000 supports the following ATM OAM management functions:

- Configure ATM OAM globally: to specify the locate loopback ID (LLID) for an NE in ATM OAM cell loopback detection.
- Create ATM OAM detection: Detects the running status of a link and locates an ATM link fault.
- Running an LB Test: link faults are detected and located based on whether loopback cells can be received.
- View alarm status or statistics: to understand the link status in real time and view details about any faults occurred in the link.

BFD Management

Bidirectional forwarding detection (BFD) detects the communication faults between forwarding engines. It detects connectivity of a path between two systems. The path can be either a physical or logical link (including a tunnel).

BFD Management provides global BFD attribute and global TTL configurations, session management, and BFD alarm management. After BFD management is configured, VRF, PW, MPLS TE, VSI, IS-IS, OSPF, BGP, LDP LSP, and physical links all support BFD.

VRRP

As a fault-tolerant protocol, Virtual Router Redundancy Protocol (VRRP) is used to combine a group of routers on a LAN into a virtual router and switch services to another router if the next-hop router fails. This protocol ensures communication continuity and reliability. Major VRRP management functions provided by the U2000 are global VRRP configuration, virtual router (VR) configuration, and VRRP Group Management Protocol (VGMP) configuration. With these functions, routers on a LAN can securely access external networks.

You can perform the following operations on the U2000:

- Configure global VRRP attributes, interface attributes, and interface VRs; manage VRRP alarms.
- Configure global VGMP attributes; manage VGMP members and VGMP alarms.

Multi-Node Hot Backup Management

Supports ARP remote backup service. An ARP hot backup service can be used to back up and synchronize ARP information between the active and standby NES running VRRP. After a switchover is performed between the active and standby NEs, downstream traffic is normal without ARP learning. This prevents packet loss caused by delayed ARP information obtaining after the switchover.

Security Management

Supports MAC address filtering, configuring ARP security interface, Mirroring management, interface DHCP configuration, VLAN DHCP configuration, and interface traffic suppression configuration.

 **NOTE**

The service mirroring function complies with universal standards followed by the telecommunication industry. When this function is enabled, other devices or instruments that receive mirrored service packets may need to analyze some information about end users' communications based on the requirements for operation and maintenance. The U2000 does not collect or save end users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

BRAS Management

A broadband remote access server (BRAS) provides the remote access service for broadband users.

The U2000 supports the following BRAS features of multi-service control gateways:

- Address pool management
- Authorization, authentication and accounting (AAA) management
- Domain and Point-to-Point Protocol (PPP) management
- Built-in Web server management
- Layer 3 Internet service provider (ISP) management
- Portal server management
- VLAN management
- User management
- IPv6 address pool management
- Carrier Grade NAT (CGN) management

The U2000 also supports real-time performance statistics on domains, address segments, and IP addresses.

NTP Management

The Network Time Protocol (NTP) is used for clock synchronization between network elements (NEs). NTP is of low costs in configuration and applicable to scenarios where the clock precision is not highly required (ms-level). The U2000 supports the following NTP management functions:

- Manages NE NTP clocks in client mode and queries the NTP clock status on different NEs in batches.
- Modifies or re-sets NTP clock configurations in batches.

ATN905 One-Click Health Check

The result of one-click health check provides the following data about ATN 905 health status to help quickly detect problems and improve network maintenance efficiency:

- General health status
 - Hardware status: Such data includes the board status, FMEA/temperature, voltage, CPU usage, and memory usage. Abnormal data helps you detect and address a fault in time.
 - OSPF neighbor statistics: Such data includes the information about global OSPF neighbors, processes, and instances.

- IS-IS neighbor statistics: Such data includes the neighbor status, hold duration, and neighbor type. IS-IS neighbor status indicates whether two NEs communicate properly.
- Interface status: Such data includes interface running status and statistics.
- IP connectivity status
 - Ping and tracert test results: The ping test result indicates network connectivity, and the tracert result indicates fault points.
 - Route information: Such data contains the routing entry that is most matched with the destination address, including details about active and inactive routes.
 - OSPF neighbor details: Such data includes the neighbor router ID, neighbor status, and IP address of the interface connected to the neighbor router.
 - OSPF neighbor change information: Such data is a summary about the last neighbor getting Down. The summary includes information about the area to which the neighbor belongs as well as the direct and root causes that make the neighbor get Down.
 - IS-IS neighbor details: Such data includes an IS-IS neighbor's area address, duration during which the neighbor stays Up, and IP address of its directly connected interface.
 - IS-IS neighbor change information: Such data includes the time when the status of an IS-IS neighbor changes, interface on which the IS-IS neighbor resides, as well as how and why the IS-IS neighbor changes.

8.5.2.3 Router V8 Management

Router V8 management allows you to configure and maintain routers V8 by means of the graphical user interface (GUI).

Device Management

The U2000 can automatically identify software versions to implement differentiated management.

You can configure management channels and local users (such as NETCONF) for NEs.

Panel Management

The U2000 supports the following operations:

- Display information about subracks, boards, power modules, fans, subboards, and ports on an NE panel.
- Automatically refresh alarm indicators on an NE panel.
- Display alarms
- Display real-time and historical performance data on an NE panel.
- Reset and switch boards.

NE Configuration Management

NE configuration management supports the following functions:

- Management of Ethernet, ETH-Trunk, IP-Trunk, packet over SDH/SONET (POS), tunnel, and Gigabit Ethernet (GE) interfaces

- Layer 3 virtual private network (L3VPN) management
- Multiprotocol Label Switching (MPLS) management
- Route management
- Routing policy management
- Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Border Gateway Protocol (BGP) management
- QoS management
- Access control list (ACL) management
- Alarm management
- Security management for authorization, authentication and accounting (AAA), Huawei Terminal Access Controller Access Control System (HWTACACS), and Remote Authentication Dial-In User Service (RADIUS)
- System management
- Netstream management
- Simple Network Management Protocol (SNMP) management
- NETCONF management
- Telnet/STelnet management
- Anti-attack management

8.5.2.3.1 Main Features of V8-based NE Management

This topic describes main features of V8 NE (routers and switches) management using the U2000.

The VRPv8-based NE Explorer provides functions of configuring and maintaining VRPv8-based routers and switches (V8 NEs). The VRPv8 platform is the new-generation platform that has the following advantages when working with the U2000:

1. More comprehensive NE management and more reasonable feature design.
2. Faster service deployment, with overall efficiency improved by about 30%.
3. Data consistency between the U2000 and NEs. The U2000 communicates with NEs using NETCONF to obtain NE configuration data.
4. Unified operation style, improving user experience and reducing training costs. The following lists the details:
 - Fast search for parameters: You can locate a desired feature/parameter using the search function. Specifically, to locate a feature, you can enter a keyword in the search box above the navigation tree and select a desired feature node from the search list. To locate a parameter, you can click **Create** and choose Click and then click **Find** in the displayed window.
 - Automatic association of parameters: The V8 NE Explorer automatically associates parameters that have been set with those that need to be set and their valid value ranges. Unsupported parameters will be automatically hid or become unavailable.
 - Column customization: You can customize columns to view desired information using the **Customize Column** function.
 - Parameter filter: The V8 NE Explorer enables you to filter parameters based on fields to locate your desired records quickly.
 - Online help in windows:

- When you move the cursor on a parameter, its descriptions will be displayed.
- when you move the cursor to the value range textbox, the parameter's allowed value range will be displayed.

For modified parameters, there will be even a red mark in the upper left part of their text boxes when it is not issued.

8.5.2.3.2 Quick Search for V8 NE Explorer Parameters

ParamFinder for V8 NEs provides GUI references for the V8 NE Explorer, which cover all parameters supported by the V8 NE Explorer. You can use the quick search function to quickly search for the required parameters and locate them in the NE Explorer.

NOTE

ParamFinder for V8 NEs is a web-based tool that covers all V8 series NEs and restores the device function tree. It also supports mainstream browsers, such as Internet Explorer 10+, Chrome 27+, and Firefox 4+.

For details, see [Instructions for using ParamFinder for V8 NEs](#).

To use this tool, click [ParamFinder for V8 NEs](#).

8.5.2.4 Switch Management

Switch management allows you to configure and maintain switches by means of the graphical user interface (GUI).

NOTE

Supported features may vary with NE versions. For details, contact Huawei technical engineers to obtain *Performance Event List & IP domain NE Feature List* in *Bidding Support Documents* of the mapping U2000.

Device Management

The U2000 supports the following operations:

- Automatically identify device types and software versions to implement device-based management.
- Automatically obtain and refresh information about entities such as subracks, boards, power supply units, fans, and ports, and monitor status of these entities.
- Display information about subracks, boards, power supply units, fans, and ports all in the NE panel.

Interface Management

You can configure the following interfaces on the U2000:

- Physical interfaces such as Ethernet interfaces
- Virtual interfaces such as subinterfaces, trunk interfaces, loopback interfaces, and tunnel interfaces

LLDP Management

You can configure link layer discovery protocol (LLDP) globally or on interfaces.

Ethernet Feature Management

You can perform the following operations on the U2000:

- Configure global VLANs, port VLANs, VLAN stacking, and VLAN mapping.
- Manage VLAN switches.

Ethernet OAM Management

Ethernet operation, administration, and maintenance (OAM) are used to check connectivity, evaluate performance, and locate faults for Ethernet links. The IEEE 802.1ag and IEEE 802.3ah are used to implement Ethernet OAM. With IEEE 802.1ag, the U2000 can continuously monitor user services, and acknowledge and locate faults. With IEEE 802.3ah, the U2000 can monitor last-mile user services and report faults.

You can perform the following operations on the U2000:

- Manage global information.
- Use IEEE 802.1ag-related functions, namely management and configuration of maintenance domains (MDs), maintenance associations (MAs), local maintenance association end points (MEPs), remote MEPs.
- Use IEEE 802.3ah-related functions, namely Ethernet OAM configuration, port query, and loopback detection.
- Test and diagnosis management

Route Management

You can perform the following operations on the U2000:

- Query routing information.
- Configure IP address prefixes.
- Configure static routes.
- Configure BGP routes.
- Configure OSPF routes.
- Configure IS-IS routes.
- Configure routing policies.
- Query running information about BGP peer groups, BGP peers, OSPF, and IS-IS.

MPLS Management

The U2000 supports NE-level MPLS management.

You can perform the following operations on the U2000:

- Enable MPLS-related protocols.
- Configure MPLS TE tunnels, MPLS interfaces, static label switched paths (LSPs), MPLS OAM detection, and MPLS OAM protection groups.

BFD Management

You can perform the following operations on the U2000:

- Configure bidirectional forwarding detection (BFD) attributes.
- Manage sessions.
- Manage BFD alarms.
- Perform BFD for virtual routing and forwarding (VRF), pseudo wires (PWs), MPLS TEs, virtual switch instances (VSIs), and physical links.

VRRP Management

As a fault-tolerant protocol, Virtual Router Redundancy Protocol (VRRP) is used to combine a group of routers on a LAN into a virtual router and switch services to another router if the next-hop router fails. This protocol ensures communication continuity and reliability. Major VRRP management functions provided by the U2000 are global VRRP configuration, virtual router (VR) configuration, and VRRP Group Management Protocol (VGMP) configuration. With these functions, routers on a LAN can securely access external networks.

You can perform the following operations on the U2000:

- Configure global VRRP attributes, interface attributes, and interface VRs; manage VRRP alarms.
- Configure global VGMP attributes; manage VGMP members and VGMP alarms.

VPN Management

You can manage the following items on the U2000:

- Tunnel policies
- PW templates
- PWs
- VSIs
- VRFs
- SPWs

NE Channel Management

The U2000 supports configuration and maintenance of various management channels.

You can perform the following operations on the U2000:

- Configure virtual type terminals (VTYs).
- Manage File Transfer Protocol (FTP) services and local users.
- Configure log service, alarm services, secure shell (SSH) services, and SNMP parameters.

8.5.2.5 Switch CE Management

Router V8 management allows you to configure and maintain routers V8 by means of the graphical user interface (GUI).



Supported features may vary with NE versions. For details, contact Huawei technical engineers to obtain *Performance Event List & IP domain NE Feature List* in *Bidding Support Documents* of the mapping U2000.

Device Management

The U2000 can automatically identify software versions to implement differentiated management.

You can configure management channels and local users (such as NETCONF) for NEs.

Panel Management

The U2000 supports the following operations:

- Display information about subracks, boards, power modules, fans, subboards, and ports on an NE panel.
- Automatically refresh alarm indicators on an NE panel.
- Display alarms
- Display real-time and historical performance data on an NE panel.
- Reset and switch boards.

Stacking Device Management

The U2000 supports the following operations:

- Stacking devices are displayed as an NE on the U2000, and the NE icon in the physical topology is displayed according to the type of the master device in the stacking system.
- The U2000 supports NE panel-based stacking device management. In the case of chassis-shaped stacking, the NE panel is displayed in multi-chassis mode, and the master and slave chassis can be displayed. In the case of case-shaped stacking, the NE panel is displayed in single-chassis mode, and the master and slave boards can be displayed.

NE Configuration Management

NE configuration management supports the following functions:

- Management of Ethernet, Gigabit Ethernet (GE) interfaces
- Layer 3 virtual private network (L3VPN) management
- Multiprotocol Label Switching (MPLS) management
- Route management
- Routing policy management
- Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Border Gateway Protocol (BGP) management
- QoS management
- Access control list (ACL) management
- Alarm management
- Security management
- System management
- Simple Network Management Protocol (SNMP) management
- NETCONF management
- Telnet/STelnet management

nCenter Management

The U2000 supports the following operations:

- This function provides a navigation path to eSight, the enterprise service and network management system. After accessing the eSight, you can use the nCenter to manage data center networks constructed using virtual software.
- To obtain eSight documentation, access <http://enterprise.huawei.com> and choose **Support > Product Support > Enterprise Networking > Network Management > OSS > eSight > eSight**.

8.5.2.6 Template Management

During NE configuration management, many operations need to be performed repeatedly. The template management function solves this problem by allowing you to rapidly configure NEs in batches.

On the U2000, common configurations are saved as various scenario-specific templates. After a template is selected and parameters in the template are set as needed, the relevant configurations can be deployed to NEs in batches. Default templates are available. When a template is referenced, the attribute settings on the template automatically apply to the configured resource.

Template Features

A template has the following features:

- Offline configuration
Global templates are created in advance and saved on the U2000. They are not created on NEs. The creation of global templates does not require the NE to be in any particular type of status.
- Global validity
A global template can be referenced by all NEs managed by the U2000.
- Little duplicate data
 - After a global template is applied, the U2000 keeps only one template data record for the NEs that reference this template.
 - When an NE references a global template, the U2000 does not add a template data record; the U2000 only records the reference relationship between the NE and the template.
- A global template can be referenced by a large number of NEs of the same type; therefore, the number of global templates is small. Consequently, global templates are easy to manage.

Main Templates

Access control list (ACL) template

An ACL template allows you to configure ACLs for multiple interfaces on different routers at the same time, simplifying attack defense configurations on the network access side.

IP Quality of service (QoS) profile

An ACL template allows you to configure ACLs for multiple interfaces on different routers at the same time, simplifying attack defense configurations on the network access side.

IP QoS profiles that can be configured are as follows:

- CBQoS profile
 - Policy profile
 - Classifier profile
 - Behavior profile
- DS domain profile
- HQoS profile
 - HQoS profile
 - Flow queue profile
 - Flow mapping profile
 - Flow wred profile
 - User group queue profile
 - Service template profile
 - Service priority template profile
- Port queue profile
 - Port queue profile
 - Port wred profile
- Interface CAR profile
- Interface QoS profile
- ATM Policy Profile

IP multicast template

Routers support the following IP multicast templates:

- Layer 2 call admission control (CAC) template, which can be applied to NEs, virtual switch instances (VSIs), pseudo wires (PWs), and NE interfaces to adjust and configure multicast CAC in batches
- Layer 2 static multicast group template, which can be applied to PWs and NE interfaces to adjust and configure static multicast groups in batches

Virtual private network (VPN) service template

The default templates are named according to a certain rule, such as DEFAULT_VPLS_ROUTER.

- DEFAULT: indicates that the template is a default template provided by the U2000.
- VPLS/TUNNEL/PWE3/L3VPN: indicates the type of service to which the template applies.
- ROUTER/PTN6900/PTN: indicates the type of NE to which the template applies. ROUTER, PTN6900, and PTN refer to routers, PTN6900 series NEs, and PTN series NEs respectively. The template is customized according to default settings. Parameters that are not supported are not listed in the template, which reduces human operation errors.
- ATN_CX/MIXED_VPN/IPRAN: indicates that the template is customized for the IPRAN solution. This template is used for rapid configuration in the IPRAN scenario.
- STATICROUTE/RIPROUTE/OSPFROUTE/ISISROUTE/BGPROUTE: indicates that the template is customized based on the routing protocol between the PE and CE running L3VPN services.

8.5.2.7 Node Redundancy Management

The U2000 supports two node redundancy schemes: enhanced-trunk (E-trunk) and enhanced automatic protection switching (E-APS). Node redundancy is mainly applied to protection over links between customer edges (CEs) and provided edges (PEs) and protection over PEs if the CEs are dual-homed to a virtual private LAN service (VPLS), virtual leased line (VLL), or pseudo wire emulation edge-to-edge (PWE3) network.

E-Trunk is extended based on Link Aggregation Control Protocol (LACP) and used to implement link aggregation between NEs. It helps to implement link aggregation group redundancy for NEs and improve network reliability.

The U2000 supports the following operations:

- Create an E-trunk, bind ETH-trunks interface, and configure attributes of an E-trunk and its ETH-trunks interface.
- Automatically discover configurations of specified NEs and their E-trunk protection groups according to a given NE range.

E-APS is a cross-NE protection switching mechanism. It is mainly used to implement automatic switching of services from a faulty link between a CE and a PE to a normal link if the CE is dual-homed to a VPLS, VLL, or PWE3 network.

The U2000 supports the following operations:

- Create E-APS and configure E-APS attributes.
- Automatically discover configurations of specified NEs and their E-APS protection groups according to a given NE range.

8.5.3 Service Deployment

8.5.3.1 Tunnel Service Management

Tunnel service management allows you to plan and deploy services on a Multiprotocol Label Switching (MPLS) network. Functions such as end-to-end tunnel planning, deployment, audit, and monitoring are available, which helps to reduce operation and maintenance costs for MPLS networks.

Tunnel Deployment

You can perform the following operations on the U2000:

- Enable MPLS, Label Distribution Protocol (LDP), and MPLS traffic engineering (MPLS TE) on NEs and interfaces in batches.
- Deploy end-to-end MPLS TE tunnel services to implement traffic planning of MPLS core networks.
- Deploy Static LSP or Static CR LSP services to implement MPLS access schemes.
- Configure MPLS TE protection groups, configure MPLS operation, administration, and maintenance (OAM) detection, and monitor alarms to implement end-to-end MPLS OAM protection.
- Import or export tunnel service data from an Excel file, including Static CR tunnel, Resource Reservation Protocol-TE (RSVP-TE) tunnel, and tunnel protection group.
- Configure the link bandwidth threshold.

During the establishment of a static CR LSP calculation path, the U2000 can generate a link weight based on the remaining link bandwidth and the threshold, achieving traffic balance.

Automatic Tunnel Discovery

The U2000 can, in collaboration with network administrators, discover MPLS protection rings, tunnels and related protection groups that have been deployed on networks. This type of automatic discovery is used in scenarios where MPLS protection rings and tunnels are deployed before the U2000 is installed. Network administrators do not need to spend much time and existing services are protected against incorrect operations.

Tunnel Monitoring

The U2000 supports the following operations:

- Display MPLS protection rings, Static, Static CR, RSVP-TE, LDP, IP, and other tunnels and their alarms in a network-wide tunnel view.
- Collect and display tunnel performance data.
- Locate associated MPLS protection rings or tunnels according to alarms.

Tunnel Diagnosis

The U2000 can diagnose deployed MPLS TE tunnel services and static tunnel services by means of LSP ping and LSP trace route to learn network connectivity and locate the fault rapidly by detecting the tunnel services.

8.5.3.2 VPN Service Management

The U2000 supports centralized and unified management of virtual private network (VPN) services such as Layer 3 VPN (L3VPN) services, virtual private LAN service (VPLS) services, and pseudo wire emulation edge-to-edge (PWE3) services. Detailed functions include service provisioning, service monitoring, and service diagnosis.

Service Provisioning

The U2000 provides a user-friendly graphical user interface (GUI) on which you can complete all service configuration operations. Parameters for multiple NEs can be automatically generated by using service templates. User configuration results can be previewed in the topology before being applied.

- User management
 - Add, delete, or modify users; bind users to VPN services.
- L3VPN service management
 - Configure dynamic L3VPN services.
 - Configure L3VPN services in Full-Mesh, Hub-Spoke, HVPN, or customized mode.
 - Configure VPN fast reroute (FRR) and IP FRR for L3VPN services, and bind L3VPN services to traffic engineering (TE) tunnels.
 - Configure static, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), IS-IS, and RIP private routes.

- Configure VPN services in inter-AS OptionA or inter-AS OptionB mode.
- VPLS service management
 - Manage VPLS services in Label Distribution Protocol (LDP) signaling (Martini) mode.
 - Manage VPLS services in Border Gateway Protocol (BGP) signaling (Kompella) mode.
 - Manage VPLS services for interworking of different virtual switch instances (VSIs).
- PWE3 service management
 - Configure static and dynamic PWE3 services.
 - Manage PWE3 services in circuit emulation service (CES), asynchronous transfer mode (ATM), Ethernet(ETH), IP over PW, networking function (ATM IWF), or heterogeneous interworking mode.
 - Configure management PW.
 - Back up pseudo wire (PW) configurations.
 - Configure PW FRR.
 - Configure CES FPS.
- Composite service management

You can manage the following composite services: **Customize**, **H-VPLS** and **PWE3 in Dynamic L3VPN**. The difference between the two modes is the creation operation on the NMS.:
 - Customized: Services can be combined in various types, including VPLS+PWE3, VPLS+L3VPN, PWE3+L3VPN, OptionA VPLS, OptionA PWE3, OptionA L3VPN, PWE3+PWE3, You need to manually create or select existing services, and create a connection point to combine them into a composite service.
 - H-VPLS: After an NE is added to the U2000 as a VPLS node, PWE3 node, or PW switching node, the U2000 will automatically create the desired H-VPLS composite service over the NE.
 - PWE3 in Dynamic L3VPN: The NMS automatically creates qualified PWE3+L3VPN services after the gateway IP address is set, the dynamic L3VPN is selected, and PWE3 is added.

Automatic Service Discovery

The U2000 can automatically discover L3VPN, VPLS, PWE3, E-AGGR and composite services on managed networks. It can also rapidly load services from managed networks for unified management and monitoring, without requiring much user participation.

The U2000 supports automatic discovery of the following composite services: H-VPLS, PWE3+L3VPN, VPLS+L3VPN, inter-AS Option A (PWE3, VPLS, and L3VPN).

Service Monitoring

- The U2000 can display network topologies for L3VPN, VPLS, PWE3, and composite services. Running status of resources used by services can be displayed in a topology view, which helps to rapidly locate faults. Such a resource can be an interface, virtual routing and forwarding (VRF), or VSI. In addition, you can customize topology views. For example, you can place the services of key customers in one topology view for monitoring.

- You can rapidly locate a faulty service according to an NE alarm.

Service Diagnosis

Diagnostic tools are used to check network connectivity and locate faults. You can generate diagnostic tasks according to selected services and directly perform operations on NEs in topology views. Diagnostic results can be directly displayed.

Service Check and Test

- Configuration check: The U2000 can check consistency of VPN service configurations at different sites and show configuration error locations.
- Service continuity check: The U2000 can check service connectivity by means of ping and trace route tests, and locate faulty NEs.
- Protocol status test: The U2000 can check service protocol status and forwarding tables, and display error information to help you locate faults.

8.5.3.3 IP Hard Pipe Service Management

The U2000 hard pipe solution isolates different types of services and guarantee the quality of VIP services. This solution provides SDH-like service quality assurance and O&M experience for customers and helps reduce the OPEX.

Service Provisioning

The U2000 provides a user-friendly graphical user interface (GUI) on which you can complete all service configuration operations. Parameters for multiple NEs can be automatically generated by using service templates. User configuration results can be previewed in the topology before being applied.

- Customer management
 - Add, delete, or modify customers; bind customers to VPN services.
- Tunnel management
 - Create hard-pipe tunnels.
 - Modify the bandwidth or pipe type of single-hop LSPs.
- PWE3 service management
 - Create PWE3 services of the hard-pipe type.
 - Create hard-pipe tunnels upon service triggering, and apply the interface rate limit to tunnels.
 - Specify whether each segment of a PW path is of the hard-pipe type.
 - Configure user-queue QoS on interfaces to automatically check whether the QoS bandwidth configurations on the access interfaces of both ends are consistent.
 - Modify interface bandwidth and associate interface bandwidth modification with tunnel bandwidth modification.
 - Check hard-pipe services carried by an interface and the bandwidth used by each service.
 - Check specific routes for leased line services and the remaining bandwidth of each segment of a hard pipe.

Automatic Service Discovery

The U2000 can automatically discover services on managed networks. It can also rapidly load services from managed networks for unified management and monitoring, without requiring much user participation.

Service Monitoring

- The U2000 can display network topologies for services. Running status of resources used by services can be displayed in a topology view, which helps to rapidly locate faults. In addition, you can customize topology views. For example, you can place the services of key customers in one topology view for monitoring.
- You can rapidly locate a faulty service according to an NE alarm.

Service Diagnosis

Diagnostic tools are used to check network connectivity and locate faults. You can generate diagnostic tasks according to selected services and directly perform operations on NEs in topology views. Diagnostic results can be directly displayed.

Service Check and Test

- Configuration check: The U2000 can check consistency of VPN service configurations at different sites and show configuration error locations.
- Service continuity check: The U2000 can check service connectivity by means of ping and trace route tests, and locate faulty NEs.
- Protocol status test: The U2000 can check service protocol status and forwarding tables, and display error information to help you locate faults.

8.5.4 Network Monitoring

8.5.4.1 Router Health Monitoring

Router health monitoring includes device connectivity monitoring, overall BRAS management, and overall BRAS running information monitoring.

Device Connectivity Monitoring

This function is enabled by the device connectivity monitoring software provided by the U2000. The device connectivity monitoring software supports active polling for physical links, helping users to monitor links and devices and to collect monitoring data. In addition, the monitoring data on the U2000 can be exported to a text, providing a convenient method to summarize, analyze, and report the monitoring data for routine maintenance. Details about this function are as follows:

- Device connectivity monitoring function
 - Port monitoring: O&M engineers need to monitor status about fibers/cables and some of the devices managed by the U2000. They also need to export, summarize, analyze, and report the monitoring data.
 - SNMP reachability monitoring: O&M engineers need to monitor SNMP reachability on all devices managed by the U2000. They also need to export, summarize, analyze, and report the monitoring data.

- Device restart monitoring: O&M engineers need to monitor restart events occurred on all devices managed by the U2000. They also need to export, summarize, analyze, and report the monitoring data.
- Interface ignoring: During the engineering maintenance process, O&M engineers can ignore the unconcerned device ports to narrow the monitoring range and to improve the monitoring effect.
- Historical monitoring information management
 - Historical monitoring information about port faults: O&M engineers can obtain historical monitoring information about port faults in order to assess and analyze device health status.
 - Historical monitoring information about SNMP reachability: O&M engineers can obtain historical monitoring information about port faults in order to assess and analyze device health status.

Outdoor Cabinet Management

The U2000 can be used to monitor the operating status of the outdoor cabinet in real time. If an abnormality occurs, maintenance engineers can view the alarm information to locate and rectify the fault.

An outdoor cabinet is usually far away from an equipment room. The environment status of an outdoor cabinet directly affects the operation of the device placed in the outdoor cabinet. The U2000 manages an outdoor cabinet through the device in the outdoor cabinet for easy outdoor cabinet upgrading and environment variable monitoring. The collected information is transmitted to the U2000 through the device. Network maintenance engineers can use the U2000 to learn about the environment status of the outdoor cabinet in real time. After thresholds for environment monitoring parameters are set, alarms are reported to the U2000 when values exceed the thresholds, and the network maintenance engineers can use the alarm information to rectify faults.

The environment monitoring of an outdoor cabinet covers the following aspects:

- CCU management: also called environment variable monitoring. CCU management refers to the monitoring of environment factors that may lead to device damages or faults, covering temperature, water damage, smoke detector, door status switch, and surge protection.
- Site monitoring unit (SMU) management: also called power supply monitoring. SMU management covers modules, such as the mains input, DC power distribution, power supply unit, and storage battery.
- Temperature control unit (TCU) management: also called heat exchanger monitoring. TCU management refers to the monitoring of the subrack temperature.

If a CCU, SMU, or TCU installed in the outdoor cabinet fails, you can handle the failure by resetting the board on the U2000.

Overall BRAS Management

Overall BRAS management includes searching for online users and forcing users to go offline.

When a user connected to the BRAS encounters service failure or fails to access the network, you can locate the user using the search function in a specified scope and disconnect the user from the BRAS by using the forcible offline function.

 **NOTE**

This function is applicable only to the NE40E/NE80E/CX600 V100R006 and the NE40E/NE80E/CX600/ME60 V600R002, V600R003, or later.

Overall BRAS Running Information Monitoring

Advantages of overall BRAS running information monitoring are as follows:

- Displays monitoring information in a centralized manner for easy overall BRAS status monitoring.
- Provides a BRAS list and displays all BRASs on the network.
- Supports IP address-based fast NE location, helping you locate NE faults quickly.

The U2000 supports the following functions related to overall BRAS running information:

- Viewing BRAS NE alarms

You can view current alarm information about a specific BRAS NE to locate faults when certain overall BRAS running information is abnormal.

- Exporting overall BRAS running information

You can export overall BRAS running information, and then save or back up the information. The information helps to understand overall BRAS NE status and determine whether expansion is required.

- Viewing overall BRAS running information

You can view overall BRAS running information, such as the address usage of an address pool, address usage of a user domain, interface service statistics, reasons for user login failures, and reasons for user logout failures. In the right-hand pane of the BRAS topology tree, you can view the online user information and server status information that is displayed in different tables. The following table lists the tables related to overall BRAS running information, and related application scenarios, and functions.

Table 8-3 Tables related to overall BRAS running information

Table	Application and Function
IP Pool Address Use Ratio	You can view the IP Pool Address Use Ratio table to identify whether user login failures are caused by address exhaustion.
User Domain Address Use Ratio	Multiple address pools can be bound to one user domain, and one address pool can also be bound to multiple user domains. Address usage of a user domain cannot be identified based on address usage of an address pool. To address this issue, the U2000 provides the User Domain Address Use Ratio table. You can view this table to know the number of online users in the current user domain. As an address pool may be bound to multiple user domains, address usage of the address pool read from an NE is not accurate and it is used for reference only.
Interface Service Statistics	You can view the Interface Service Statistics table to learn about services on NE interfaces, as well as administrative status and running status of the interfaces.

Table	Application and Function
User Log In Failed Statistics	You can view the User Log In Failed Statistics table to know top N reasons for user login failures, analyze the root cause, and provide solutions, accumulating experience for expansion in the future.
User Abnormality Leave Statistics	You can view the User Abnormality Leave Statistics table to know top N reasons for user logout failures, analyze the root cause, and provide solutions, accumulating experience for expansion in the future.
TACACS Server	
RADIUS Server	
Portal Server	
DHCP Server Group	You can view the TACACS Server , RADIUS Server , Portal Server , or DHCP Server Group table to check whether the TACACS, RADIUS, portal, or DHCP server status is normal. This helps to rectify faults quickly and accumulate experience for expansion in the future.

8.5.4.2 AtomEngine Management

AtomEngine-based performance monitoring solution helps detect and monitor service quality on the network with the current network unchanged, which improves O&M efficiency and reduces operating costs.

Introduction to the AtomEngine-based Performance Monitoring Solution

AtomEngines provide visibility into network performance in a plug-and-play manner. By deploying AtomEngines on live-network devices, carriers can obtain high-accuracy service quality data, such as the packet loss ratio, delay, jitter, and throughput rate, through service quality monitoring. This implementation does not require device upgrades or replacement. Currently, AtomEngines support monitoring technologies such as IP FPM, RFC 2544, and TWAMP.

Huawei AtomEngine solution involves three components:

- AtomEngine:

AtomEngines can be inserted into interfaces on traditional Huawei devices or third-party devices to perform OAM functions, such as IP Flow Performance Measurement (FPM), RFC 2544, and Two-Way Active Measurement Protocol (TWAMP).

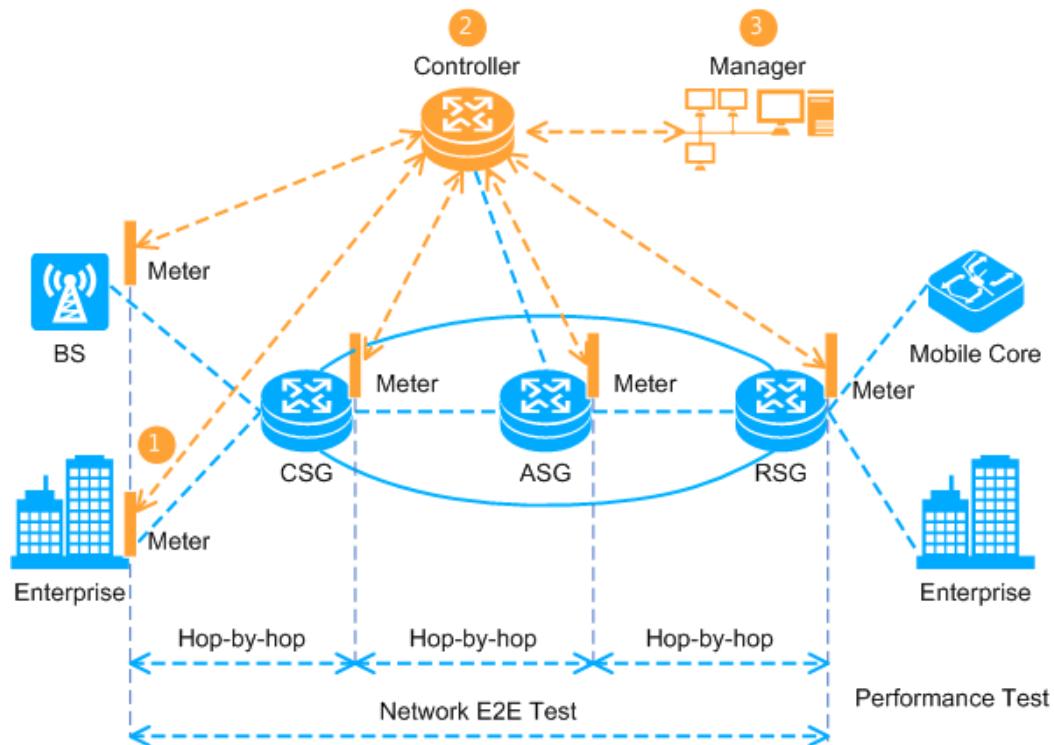
- Smart network controller (SNC):

Acts as an agent for AtomEngines. The SNC-A service board needs to be installed on an NE40E, CX600, ME60, or a PTN 6900. The U2000 communicates with AtomEngines through an SNC to implement automatic AtomEngine discovery and agent management.

- Manager:

Performs management functions, such as searching for and maintaining AtomEngines and deploying OAM measurement tasks to AtomEngines.

Figure 8-11 Huawei AtomEngine solution

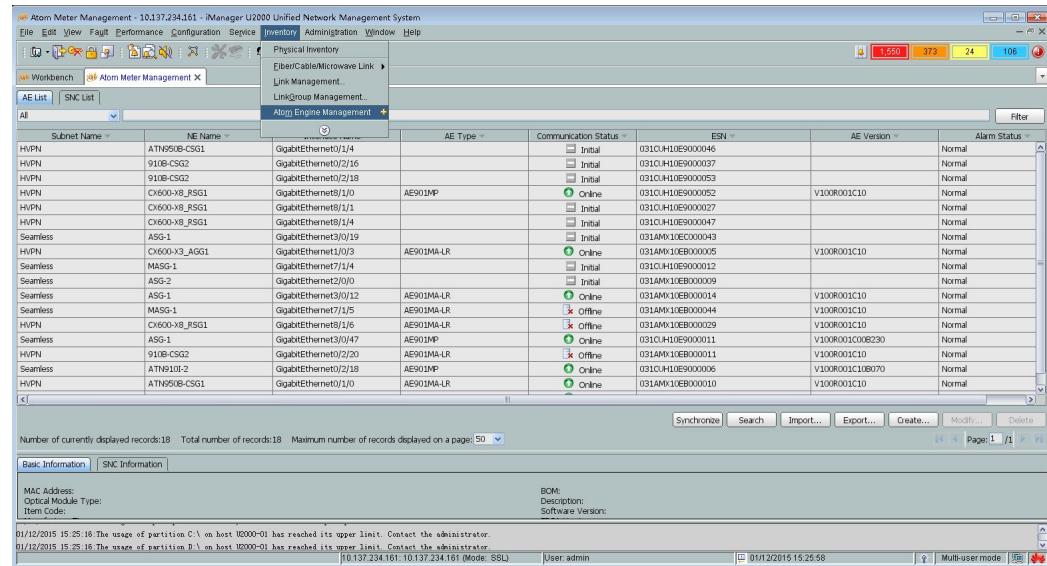


The U2000 fully takes into account the characteristics of AtomEngines, such as large quantity, versatility, dynamic status, and continuous measurement task execution and is capable of managing AtomEngines in batches. The uTraffic provides customized topology and diagram reports about IP FPM and TWAMP. The U2000, together with the uTraffic, ensure efficient and smooth AtomEngine OAM.

Introduction to the AtomEngine Management Functions of the U2000

The U2000 provides a unified navigation path for AtomEngine management. To implement AtomEngine management, choose **Inventory > Atom Engine Management** from the main menu.

The AtomEngine management GUI consists of two lists: AE list and SNC list. The AE list may contain tens of thousands of records, whereas the SNC list usually consists of dozens of records at most. The following figure shows the GUI style.



The following table describes the AtomEngine management functions of the U2000.

Table 8-4 AtomEngine management functions of the U2000

Function	Description
Importing AtomEngine and SNC Information to the U2000 in a Batch	An AE planning table that contains AtomEngine information can be used to import AtomEngine information to the U2000 in a batch. After importing the AtomEngine planning table, the U2000 automatically enables SNC on SNC devices listed in the table and adds these devices to the internal SNC list.
Manually Creating a Single AtomEngine	A single AtomEngine can be manually created on the U2000 if no AE planning table is used.

Function	Description
Managing Basic AtomEngine and SNC Information	<p>After the SNC detects AtomEngines, AtomEngine information is reported to the U2000 and then displayed. The U2000 allows you to modify or delete imported AtomEngine planning information record by record. You can also manually create an AtomEngine record on the U2000.</p> <p>A. The U2000 manages the following AtomEngine information:</p> <ul style="list-style-type: none"> ● Imported AtomEngine planning information, such as the AtomEngine ESN, housing information, and search configurations ● Information about communication between AtomEngines and the SNC and mappings between AtomEngines and housing devices ● Basic AtomEngine information obtained from AtomEngines through the SNC, such as the version number, type, and MAC address <p>B. The U2000 manages the following SNC information:</p> <ul style="list-style-type: none"> ● Basic SNC information, such as the device name, current status, and global attributes of delegated AtomEngines ● Search configurations about AtomEngines ● Status and statistics about AtomEngines delegated to SNCs <p>The AtomEngine management GUI shows the communication status between each AtomEngine and SNC, helping you determine which AtomEngines are available. One AtomEngine can be managed by a maximum of two SNCs.</p>
Monitoring the Alarm Status of AtomEngines	After receiving AtomEngine alarms forwarded by SNCs, the U2000 displays these alarms on the alarm panel as the alarms of corresponding housing devices.
Set a Key that an SNC and AtomEngines Use to Communicate	<p>A key must be periodically changed to secure communications between the SNC and AtomEngines.</p> <p>After a key is changed on an SNC, AtomEngines automatically synchronize their keys with the SNC.</p>
Replacing an AtomEngine	If an AtomEngine is replaced by another one due to some reasons, such as faults, after you replace a faulty AtomEngine and enter the ESN of the new AtomEngine, the U2000 automatically delivers the search configurations of the original AtomEngine to the SNC for AtomEngine discovery. After the new AtomEngine is discovered and goes online, the U2000 instructs the OAM service modules, such as IP FPM and TWAMP modules, to re-deliver measurement tasks to the new AtomEngine.

AtomEngine-based Service Monitoring and Deployment

AtomEngine-based service monitoring and deployment involve the following functions:

- AtomEngine-based IP FPM measurement and hop-by-hop diagnosis
- AtomEngine-based RFC 2544 measurement
- AtomEngine-based TWAMP measurement

For details, see the associated solution document.

8.5.5 Network Diagnosis

8.5.5.1 IP Device Health Check

IP device health check can be performed to check basic configuration items after network deployment or to automatically check the network and NE health status during the operation and maintenance. The check results and problem rectification suggestions can be quickly provided. Compared with the CLI-based manual check mode, the visualized and batch health check greatly improves the check efficiency and avoids the omission of check items caused by manual check.

This function helps to implement visual and batch basic configuration verification.

The check items are classified into two types: **NE-level check** and **Network-level check**.

- **NE-level check:** check items for a single NE. The peer NE and the link between NEs are not checked.
- **Network-level check:** check items for multiple NEs. The peer NE and the link between NEs are also checked.

8.5.5.2 Diagnosis Management

Diagnosis management provides easy-to-use diagnostic functions for you to test network and service connectivity. Diagnostic cases can be run manually or run automatically at scheduled times.

Test Diagnosis Functions

- The U2000 provides test cases, such as virtual private LAN service (VPLS) media access control (MAC) ping/traceroute, Internet Control Message Protocol (ICMP) ping/traceroute, pseudo wire emulation edge-to-edge (PWE3) ping/traceroute, label switched path (LSP) ping/traceroute/jitter, virtual routing and forwarding (VRF) ping/traceroute, VPLS pseudo wire (VPLS PW) ping/trace, and VPLS VCCV ping/trace, which can help you test network connectivity at each protocol layer.
- The U2000 allows you to combine several test cases into a test suite, so that you can perform test cases in batches. By diagnosing services layer by layer, the U2000 can rapidly locate the network layer where a fault occurs.
 - Application Layer Diagnosis
 - Domain name system (DNS), Dynamic Host Configuration Protocol (DHCP), DHCP Emulate, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Network Management Protocol (SNMP), and voice over (VoIP)
 - Transport Layer Diagnosis
 - Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
 - Network Layer Diagnosis
 - ICMP ping/traceroute, ICMP VRF ping/traceroute, ICMP jitter, multicast ping/trace, multicast VRF trace, and maximum transmission unit (MTU) ping

- Multiprotocol label switching (MPLS) Diagnosis
 - LSP ping, LSP trace, LSP jitter, PWE3 ping, PWE3 trace, VPLS MAC ping, VPLS MAC trace, Service Ping, MAC study, multicast forwarding information base (MFIB) ping, MFIB trace, VPLS PW ping, and VPLS PW trace
- Data Link Layer Diagnosis
 - Ethernet Service MAC ping and customer edge (CE) ping
- The U2000 supports intelligent diagnostic result analysis. A result analysis template can be customized to include diagnostic indicators such as delay, jitter, and packet loss ratio and a result analysis policy based on service levels. Diagnostic result analysis can help you rapidly determine network status.

Test Diagnosis Management

Test diagnosis management allows you to test network connectivity and quality of service (QoS) and rapidly pinpoint a fault location.

A test diagnostic tool consists of the following parts:

- Test suite
 - A test suite consists of multiple test cases. Test cases are implemented at different layers: application layer, transport layer, network layer, and data link layer. Test cases for MPLS services can also be created.
 - You can choose to perform all or some test cases in a test suite. Network quality can be determined based on the parameters, such as delay, jitter, and packet loss ratio, listed in the test results.
- Diagnosis policy
 - Test suites can be performed at a specified time: daily, weekly, or monthly.
- Network scan
 - Network information is collected, and connectivity of virtual links, IP links and L2 links is tested. The U2000 displays a scanning progress in real time and allows you to stop the scanning if needed. It also provides the trace route function to locate faults.
- Historical data
 - The U2000 records historical data about test suite operations. The historical data can be filtered and queried based on test suite names, test results, or test time, and the query results can be exported.
- Template
 - The U2000 supports intelligent diagnostic result analysis. A result analysis template can be customized to include diagnostic indicators such as delay, jitter, and packet loss ratio and a result analysis policy based on service levels. Template-based analysis can help you rapidly determine network status.

8.5.5.3 IP Network Troubleshooting

IP network troubleshooting can help you discover services paths and rapidly locate faults during operation and maintenance.

IP network troubleshooting provides the following functions:

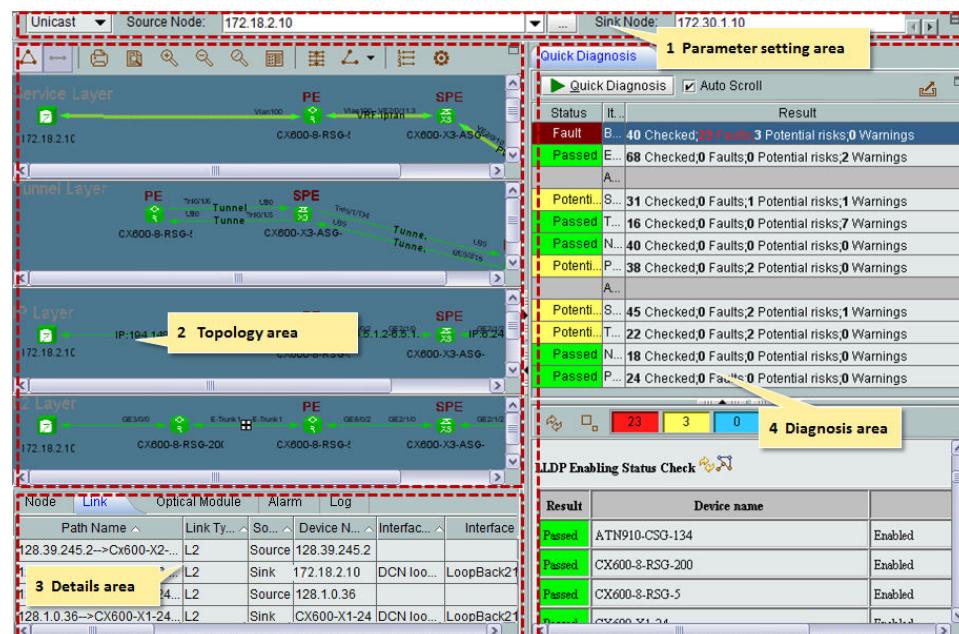
- Service path visualization: E2E service paths and backup paths are displayed in the topology. Backup paths support five backup modes: primary/secondary PW, VRRP, E-

APS, TE hot standby, and VPN FRR. The paths can be displayed as service-layer, tunnel-layer, IP-layer, and link-layer paths, showing more detailed path information. If a path is incomplete or the current path is a secondary path, a message will be displayed asking you whether to display complete non-backup and historical paths.

- Multicast service path visualization: Shared trees and shortest-path trees of multicast services are displayed in the topology. The service path can be expanded as service layer, IP layer, and link layer.
- Display of NE and link status: After you select an NE or link in the topology, a dialog box is displayed showing the performance data about the NE or the type, source, and destination information about the link. The performance data, alarm information, and optical module information about all NEs and links in the topology are displayed on tabs in the details area to help you with preliminary fault locating.
- Fast fault diagnosis: After you click **Quick Diagnosis**, path and service check items are executed layer by layer in the corresponding networking environments to detect problems. The results about each check item are displayed in a table, the check items with errors detected are marked red, and handling suggestions are provided for troubleshooting. If you click an underscored check result, the associated window in the NE Explorer is displayed helping you rectify the fault quickly.
- Partial fault detection: The packet comparison data, port loopback test, ping test, interface packet loss/error code, TDM PW statistics, path detection, smart ping, and ACL traffic statistics can be used to locate specific fault points.

Figure 8-12 shows the **IP Network TroubleShooting** window.

Figure 8-12 IP Network TroubleShooting window



N o.	Area	Description
1	Parameter setting area	This area allows you to set source and sink parameters in a simple or advanced manner.
2	Topology area	The service paths between the source and sink NEs, protection paths, and protection nodes are displayed in the topology view. A path list is also provided, showing the path information and status discovered every time in order. The topology area also provides various shortcut icons to facilitate the setting of topology and common parameters, such as performance thresholds and data backup parameters.
3	Details area	On the Node , Link , Optical Module , Alarm , and Log tabs, you can view the performance data, basic optical module information, alarm records, and log information generated during path discovery.
4	Diagnosis area	The diagnosis area contains the Quick Diagnosis and Toolbox tabs. <ul style="list-style-type: none">● On the Quick Diagnosis tab page, check items at all layers are displayed in a list. The check status at each layer is marked using different colors. The check results, including fault, potential risk, warning, manual, and passed, are displayed. The detailed check result of every check item is displayed in a table. You can refer to the problems and restoration suggestions in the check result to rectify faults.● On the Toolbox tab page, commonly used fault diagnosis tools and multicast diagnosis tools are summarized. You can choose desired tool to rectify faults.

8.6 Security NE Feature Management

This topic describes features supported by security NEs.

8.6.1 Security NE Management

Security NE management allows you to configure and maintain security NEs through the graphical user interface (GUI).

NOTE

- Security NEs include Eudemon, USG, SRG, EGW, ASG, NE40E/80E, OP-Bypass, SIG, SVN series and iCache9200 internet cache system.
- Supported features may vary with NE versions. For details, contact Huawei technical engineers to obtain *Performance Event List & IP domain NE Feature List* in *Bidding Support Documents* of the mapping U2000.

Device Management

- Automatically identify device types and software versions to implement device-based management.

- Automatically obtain and refresh information about entities such as subracks, boards, power supply units, fans, subboards, and interfaces, and monitor status of these entities.
- Display the front panel view of an NE, including subracks, boards, power supply units, fans, and interfaces in the NE Panel.
- Display the running status and alarm status of boards and interfaces in the NE Panel by using alarm indicators and colored legends.
- Perform the following operations on the NE panel: view common information and alarms of NEs, boards, and interfaces; view real-time performance of boards; view memory information; view CPU information; view hard disk information; view SPU information; reset boards; perform active/standby switchover for control boards; configure and remotely control Extended Service Platform (ESP) cards and monitor the status and configurations of these cards.
- Monitor link and NE status, collect monitoring data, and export the monitoring data to text files, which makes it convenient for users to summarize, analyze, and report the data.
- View the NE status about RADIUS Proxy.

Interface Management

You can configure a variety of media interfaces on the U2000, including physical interfaces and logical interfaces.

- Physical interfaces indicate the interfaces that physically exist on components such as boards. The U2000 supports configuration of Ethernet interfaces, packet over SDH/SONET (POS) interfaces, asynchronous transfer mode (ATM) interfaces, E1 interfaces, and other interfaces.
- Logical interfaces indicate the interfaces that do not exist physically but can exchange data. They are created through configuration. The U2000 supports configuration of subinterfaces, trunk interfaces, tunnel interfaces, loopback interfaces, virtual template (VT) interfaces, and other interfaces.

Security Zone Management

A security zone is a set of interfaces. The users connected to the interfaces have the same security attributes. Security devices regard the data flow within the same security zone as trusted. Only when data flow across different security zones occurs, security check is triggered and corresponding security policies are implemented.

You can create, modify, delete security zones, and add interfaces to security zones, or remove them from security zones.

Bridge Management

A bridge is used to connect LANs at the data link layer and transmit data between LANs.

Bridge management delivers the following functions:

- Supports the bridging function on Ethernets
The NE realizes bridging forwarding of data according to the bridge table containing the MAC address-interface mapping.
- Supports the routing and bridging functions concurrently
Traffic destined for the MAC address of this interface is forwarded through the bridge. By default, traffic is forwarded along routes.

- Supports the transparent bridging function on VLANs
If VLAN ID transparent transmission is configured on the egress of an NE added to the bridge group, the interface can directly forward packets without processing the VLAN IDs in the packets.

LLDP Management

The U2000 can discover Layer 2 links and display them if the Link Layer Discovery Protocol (LLDP) function is configured for NEs and interfaces.

You can perform the following operations on the U2000:

- Configure LLDP globally.
- Configure LLDP on interfaces.
- Synchronize LLDP neighbor information.

GTP Management

The U2000 supports configuration of GPRS Tunneling Protocol (GTP) policies. After GTP policies are configured on the U2000 and deployed to security NEs, the security NEs can filter GTP packets according to configured policies to protect general packet radio service (GPRS) networks from attacks such as GTP overbilling attacks.

PKI Management

As the integration of software and hardware systems and security policies, the PKI provides a set of security mechanisms. The PKI provides a secure network environment where the user can conveniently use encryption and digital signature technologies in various application scenarios, thus ensuring the confidentiality, integrity, and validity of data on networks. Data confidentiality determines that the data cannot be queried by unauthorized users during data transmission. Data integrity determines that the data cannot be modified by unauthorized users during data transmission. Data validity determines that data cannot be denied by users.

Automatic Registration

The U2000 can automatically update the IP address of an NE (for example, a dial-up NE) based on registration messages sent by the NE. In this manner, the NE will not go offline because of changes to IP addresses and no new IP address needs to be added. This helps to reduce maintenance costs on large-scale networks.

NE Channel Management

You can configure management channels on NEs. Detailed features are VTY configuration, log service, and alarm service.

SPU Management

You can perform the following operations on the U2000 for the SIG9810, SIG9820, and SIG9800-X:

- View service process unit (SPU) information.
- View SPU resource information.
- View the repository.

- View service blacklist/whitelist.
- View CG information.
- View sniffer information.
- View FDI information.
- View backup group.
- View SAS user information.
- View Gx interface information.

Service Management

You can view the information about the following functions for the uniform resource locator (URL) classify server:

- URL category database (UCDB) management
- URL category searching server (UCSS) management

Component Management

You can view information about the following functions for the service inspection gateway (SIG) server:

- User Interface (UI) management
- System general management server (SGMS) management
- Policy server (PLS) management
- Business interface server (BIS) management
- Data analyze server (DAS) management
- Extractive transition loading (ETL) management
- Database management
- Uninterrupted power supply (UPS) management
- Node management
- CFS management
- iPush UI management
- iPush synchronization management
- Information server management

Policy Management

You can view the following information about policy status of the SIG server:

- Policy synchronization status
- Policy deployment status
- User policy status

Cluster Management

You can view the database cluster status of the SIG server.

You can view the following information about the SIG9810, and SIG9820:

- Cluster node information
- Cluster SAS information
- Cluster user and link mapping table
- Service component information

Upgrade Management

You can view the repository upgrade status of the SIG server.

Connection Management

You can view the connection status of the SIG server and Remote Authentication Dial-In User Service (RADIUS) proxy.

Link Management

You can view information about bypass links, service links, SPS and UCSS links, and cascading interface of the SIG9810 and SIG9820.

License Management

You can view license information about the SIG9810 and SIG9820.

Statistics Management

You can view statistics information of user login requests about the RADIUS proxy.

8.6.2 Network Security Management

The U2000 provides the network security management feature to manage and monitor various security policies for security NEs. This feature is applicable to policy distribution and centralized management, monitoring, and maintenance of security NEs on medium- and large-scale networks.

Network security management consists of the following functions for service implementation:

- Security policy
 - Security policy functions include session log, packet filtering, anti-distributed denial of service (anti-DDoS), and application specific packet filter (ASPF).
- Attack defense
 - Attack defense functions include traffic attack defense, application layer attack defense, scanning attack defense, malformed packet attack defense, special packet control attack defense, and blacklist.
- NAT
 - Network address translation (NAT) functions include source NAT, destination NAT, and NAT server functions.
- Port mapping
 - Port mapping based on an access control list (ACL) is supported. You can establish mappings to application layer protocols by customizing port numbers, thereby preventing malicious attacks on known ports.

- IPS management

The IPS can inspect both the quintuple (source IP address, source port number, destination IP address, destination port number, and protocol type) of the application-layer data and packet contents. IPS devices not only detect intrusions, but also prevent the generation and development of intrusion behaviors in real time through certain response methods, protecting the information system against substantial attacks.

Network security management consists of the following functions for management:

- Policy discovery

The U2000 can discover existing NE configurations without affecting running services.

- Batch deployment

The U2000 can deploy configured NEs in batches. This simplifies operations and improves efficiency.

- Policy audit

The U2000 can compare its own configurations with NE configurations to ascertain the running status of NEs rapidly.

- Status display

The U2000 can display information such as whether a policy has been successfully deployed, whether configurations are consistent between itself and an NE, and whether an NE command has changed.

- Historical record query

The U2000 can record policy package configuration and maintenance. Operations that users have performed for policy packages can be audited.

8.6.3 Single-Point Web Configuration

Single-point Web configuration integrates existing Web functions of security NEs by embedding browser controls in client/server interfaces. Covering all configurations of security NEs and collaborating with network security management and virtual private network (VPN) service management, it provides an integrated and comprehensive security NE management solution.

Web functions of security NEs provide easy-to-use Web configuration interfaces for convenient operation and maintenance.

Single-point Web configuration is a proxy-based Web access mode. It includes two parts: Web proxy and Web browser. The Web proxy is built into the U2000 server, and users can access the Web browser from a U2000 client. Features of single-point Web configuration are as follows:

- The Web management interface of an NE can be opened on a U2000 client.
- Security login to the Web interface is available.
- Access to security NEs by means of Hypertext Transfer Protocol Secure (HTTPS) is available.
- Multiple Web technologies, such as Java script, hypertext markup language (HTML), cascading style sheet (CSS), and Applet, and technologies related to Web 2.0 are supported.
- Normal use of browsers (such as Internet Explorer and FireFox) on the PC where the U2000 is installed is not affected.
- A U2000 client and an accessed security NE can be located on different networks.

8.6.4 Security VPN Service Management

The U2000 provides the security virtual private network (VPN) service management feature to manage Internet Protocol Security end-to-end (IPSec E2E) services, remote access services, and Secure Sockets Layer VPN (SSL VPN) services.

Security VPN service management consists of the following functions:

- Service discovery
 - The U2000 can rapidly discover security VPN services on a live network, which facilitates unified service management and monitoring.
- Service configuration
 - Service creation
 - The U2000 supports batch creation of IPSec E2E services and remote access services.
 - The U2000 supports creation and cloning of SSL VPN services. You can configure network extension application services for SSL VPN services. By cloning an existing SSL VPN service for one or more NEs, you can create SSL VPN services in batches.
 - Service deployment
 - The U2000 supports single-service deployment and batch service deployment. You can deploy service configurations to NEs, which will make services take effect on the NEs.
 - Service audit
 - You can compare key configurations on NEs with those on the U2000 to identify differences in configuration between them. This function facilitates fault location and improves system maintainability.
- Service monitoring
 - Service performance management
 - You can create performance data collection tasks for security VPN services to view service performance data.
 - Service status polling
 - The U2000 supports customization of the service status polling period. You can use this function to change the interval for automatic service status updates.
- Configuration data modification
 - Service modification
 - You can modify configuration data of undeployed IPSec E2E services and remote access services.
 - You can modify configuration data of deployed SSL VPN services to implement incremental service deployment.
 - Service undeployment
 - You can undeploy security VPN services that are **Deployed**, **Deployment Failed**, or **Undeployment Failed**.
 - Service deletion
 - You can delete services from the U2000 without affecting configurations on NEs.

8.7 FTTx Network Feature Management

This topic describes the functions and features of FTTx NE management and network management.

 **NOTE**

This section describes only U2000's support to basic NE features. Information displayed on GUIs may be different for features of different types or versions of NEs.

8.7.1 OLT Management

The U2000 provides graphical user interfaces (GUIs) for configuring NEs and maintaining NE configurations. You can configure services for equipment in the GUIs.

Battery Discharge Test

You can perform the following operations on the U2000:

- Query information about network-wide battery discharge tests.
- Import NEs for which battery discharge tests will be performed.
- Start or stop a battery discharge test.
- Export test results.

NE Management

NE management includes the management of NE panels, slave subracks, basic and common NE attributes, clock sources, security, protocols, and NE templates.

NE Panel Management

You can perform the following operations on the U2000:

- Display the NE panel by double-clicking an NE.
- Query the details of equipment.
- Collect statistics on device resources.
- Query the information about shelves.
- Collect the statistics on shelf resources.
- Add, delete, enable, disable, reset, and confirm a card.
- Query the CPU usage and memory usage of cards in real time.
- Display the port view by double-clicking a card.
- Perform an active/standby switchover on the control cards.
- Configure traffic management and rate limitation for GPON cards.
- Configure rate limitation for EPON cards.

Management of Basic and Common NE Attributes

The management of basic and common NE attributes includes querying the global information about NEs and configuring global policies for NEs.

You can perform the following operations on the U2000:

- Query the system information about NEs.
- Query resource and status statistics of NEs.
- Query the license information about the functions and resources of NEs.
- Configure the system time, IP address of an NE, and the binding between a Layer 3 interface and an IP address.
- Configure the SNMP protocol port.
- Set device handshake parameters.
- Configure the policy for automatically backing up NE data.
- Enable and disable the energy-saving function of an NE.
- Configure and manage license files.

Clock Source Management

Clock source management includes the management and configuration of NE-specific clock source information, such as information about the line clock, 1588v2 clock, clock priorities and clock interface.

Security Management

You can perform the following operations on the U2000:

- Enable and disable anti-ICMP attack, anti-IP attack, anti-IP spoofing, anti-MAC spoofing, and anti-DoS attack.
- Set the aging time of an MAC address.
- Enable and disable MAC address learning.
- Configure the security attributes for user login in the CLI.

Protocol Management

You can perform the following operations on the U2000:

- Manage the Link Aggregation Control Protocol (LACP), Access Node Control Protocol (ANCP), Rapid Ring Protection Protocol (RRPP), Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP), Bidirectional Forwarding Detection (BFD), Internet Group Management Protocol (IGMP), and Network Time Protocol (NTP).
- Control the Address Resolution Protocol (ARP) proxy.
- Configure the Policy Information Transfer Protocol (PITP) mode/Relay Agent Info Option (RAIO) custom format.
- Control the Dynamic Host Configuration Protocol (DHCP) Option 82 function.
- Control the DHCP proxy and DHCP relay forwarding functions.
- Configure static routes.
- Configure IPv6 IP addresses.

Global Configuration of Services

The global configuration of services includes the configuration of the VLAN, QoS, GPON, EPON, and multicast services.

NE Template Management

By using NE template management, the U2000 manages NE templates in a centralized manner. Templates include GPON templates, EPON templates, ONU service level profile,

power shedding templates, IGMP templates, traffic templates, VLAN service templates, RAIO templates, and WRED templates. Currently, the U2000 supports querying, deleting, and generating global templates, and supports downloading global templates to NE.

Slave Subrack Management

- MA5600T/MA5603T can manage Ethernet-upstream MA5623AR slave subracks remotely. This function helps implement remote and distributed deployment of box-shaped devices.
- MA5600T/MA5603T/MA5680T/MA5683T/MA5608T can manage the Ethernet-upstream/GPON-upstream MA5633 slave subracks remotely. The Cable functions of MA5633 NE is accomplished through the OLT.

Predeployment of an offline slave subrack: Manually add an offline slave subrack for a master subrack and configure related data for the slave subracks; after the slave subrack goes online, the master subrack automatically applies the configuration data to the slave subracks.

vAN Management

MA5800 V100R017C10 and later support vAN management. One physical device is virtualized into multiple logical devices by board or port. In this manner, you can flexibly schedule resources of access networks and deploy network functions as needed, meeting the requirements of independent network resources and independent O&M in multi-service, multi-carrier, and multi-industry scenarios. Visualized management is supported. In vAN views, you can create a VS, and view and manage the resource allocation of the VS. The management experience is the same at that of managing physical OLTs.

vANs meet intelligent operation requirements, for example, the multi-service scenario.

- One OLT carrying multiple services: One physical OLT functions as multiple virtual OLTS to carry different services, saving space and power, and improving efficiency. In addition, you can use the open APIs to customize services on demand using Remote Serial Protocol (RSP).
- Private line experience: Each virtual OLT has exclusive forwarding and control resources, ensuring private line priority.
- Domain-based management and easy maintenance: Different virtual OLTS are maintained by different teams, realizing end-to-end (E2E) maintenance.
- Secure resources: Physical resources are isolated, ensuring resource security for tenants.
- Resource sharing: vANs allow multiple carriers to share the infrastructure and independently maintain and manage their resources. vANs can also be leased to tenants like hotels and data centers in batches.

Network Interface Management

Network interface management includes the management and maintenance of E1/T1 ports and Ethernet ports.

Management and Maintenance of E1/T1 Ports

E1/T1 ports are classified into TDM E1/T1 ports, CES E1/T1 ports, and IMA E1/T1 ports.

TDM E1/T1 ports can be used as access ports or upstream ports, depending on the functions of the cards.

With E1 ports for upstream transmission, you can perform (enable/disable) the loopback operation.

With E1 ports for PRA access, you can perform the following operations: configure or delete port attributes, set the alarm threshold of L2 signaling bit errors, query timeslots, and enable or disable services.

With CES E1/T1 ports, you can collect real-time performance statistics of ports, configure port attributes, set port alias, and perform loopback.

With IMA E1/T1 ports, you can query real-time performance statistics of the ports, and manage IMA groups and IMA links, including adding, deleting, modifying, resetting, blocking, and unblocking an IMA group or link.

Management of Ethernet Ports

Ethernet port management includes the management of ports and aggregation groups. You can perform the following operations on the U2000:

- Configure port attributes.
- Create, delete, query, and modify an aggregation group.
- Activate and deactivate an Ethernet port.
- Collect real-time performance statistics and delete performance statistics.
- Configure the PPPoE, DHCP Option 82, DHCP V6 Option 82, 802.3ah ETH OAM loopback, and port rate limit functions.
- Query the attributes of optical transceivers for Ethernet optical ports.
- Configure automatic control of optical signal transmission.

Connection Management

PVC

The ATM virtual connection is the logical relationship between the link endpoints in the ATM network. That is, it is the communication path for transmitting ATM cells between two or multiple endpoints. It can be used to transmit information between users, between users and networks, and between networks.

Service Virtual Port Management

A service virtual port enables user equipment to access the OLT. The service virtual port provides service streams between the user equipment and the OLT for carrying user services. You can perform the following operations on the U2000:

- Query, add, delete, modify, activate, and deactivate a service virtual port.
- Collect real-time performance statistics and delete performance statistics.
- Configure the extended attributes of a service virtual port. Extended attributes allow for greater flexibility in addressing customer requirements. Extended attributes include the maximum number of learnable MAC addresses, the PPPoE session, the encapsulation type, and the maximum number of MAC addresses that can be bound.
- Configure the connection attributes of a service virtual port, including the alias, VPI/VCI, transmit traffic profile, and receive traffic profile.
- Shift the VLAN ID of a service virtual port to change the VLAN ID of the service virtual port. After successful shifting, the service port will assume the new VLAN ID.

- Bind IP addresses to a service virtual port and query the bound IP addresses. Performing the operation will allow only users with specified IP addresses to access the service virtual port. After successful binding, the service forwarding module will check the source IP address of user packets. If the source IP address does not match any of the IP addresses bound to the service virtual port, the user packets will be dropped. This feature ensures security in user access.
- Bind static MAC addresses to a service virtual port. Performing this operation will allow only users with specified MAC addresses to access the service virtual port. After successful binding, the service forwarding module will check the source MAC address of user packets. If the source MAC address does not match any of the MAC addresses bound to the service virtual port, the user packets will be dropped. This feature ensures security in user access.
- Support the Atm-ping, detects the connectivity of the ATM link to determine whether the line between the device and the modem of the user is reachable.
- Configure service port bundles. If several service virtual ports carry the same service, a service bundle can be configured.
- Collect statistics on DHCP and PPPoE packets of service virtual ports.
- Bind and unbind static IPv4/IPv6 IP addresses.
- Query the dynamic binding of IPv6 IP addresses of service virtual ports.
- Query learned MAC addresses.

Native TDM Connection Management

TDM connection is used for transmitting the TDM service over the GPON network by encapsulating the TDM packets directly into a GPON GEM frame. In native TDM connection management, you can query, add, modify, and delete an TDM connection on the U2000.

Layer 2 Management

Layer 2 management includes the management of the VLAN, the Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), Access Node Control Protocol (ANCP), Rapid Ring Protection Protocol (RRPP), Link Layer Discovery Protocol(LLDP), G.8032 Ethernet Ring Protection Switching Protocol(ERPS).

VLAN Service Management

VLAN service management includes the management of the standard VLAN, MUX VLAN, smart VLAN, and super VLAN. You can perform the following operations on the U2000:

- Query, add, delete, and modify a VLAN.
- Collect real-time performance statistics of a VLAN.
- Clear real-time performance statistics of a VLAN.
- Manage an IPv4/IPv6 Layer 3 interface and its subinterfaces.
- Query the global unicast address of a Layer 3 interface.
- Query prefixes of IPv6 addresses.
- Query the ND information of IPv6 addresses.
- Collect statistics on the IPv6/ICMPv6 traffic and Layer 2/Layer 3 packets of an IPv6 interface.

RSTP Management

You can perform the following operations on the U2000:

- Modify and restore the default value for the trail overheads on a port.
- Collect port RSTP statistics.
- Clear port RSTP statistics.

MSTP Management

MSTP management includes the management of domains, instances, and ports. You can perform the following operations on the U2000:

- Modify and restore the default setting of a domain.
- Add, delete, and modify an instance.
- Modify a port.
- Query the statistics of a port.

ANCP Management

You can perform the following operations on the U2000:

- Add, delete, modify, enable, and disable an ANCP session.
- Query the real-time status of an ANCP session.

RRPP Management

You can query, add, delete, and modify RRPP domains.

LLDP Management

Devices' Layer 2 information obtained using the LLDP protocol is helpful for the U2000 to quickly obtain topology status of connected devices, detect configuration conflicts between devices, and find out root causes of network failures. You can configure LLDP protocol attributes and change the working modes for one LLDP port or for multiple LLDP ports at one time.

G.8032 ERPS Management

ERPS is a protocol used to block specified ports to prevent loops at the link layer of an Ethernet network. You can add, modify, configure, delete, and query ERP rings, collect Ethernet port statistics on an ERP ring, and add or delete an Ethernet port to or from an ERP ring.

Layer 3 Management

Layer 3 management includes the management of the Dynamic Host Configuration Protocol (DHCP), and Layer 3 routes.

DHCP Management

DHCP management includes the management of DHCP server groups, DHCPv6 server groups, MAC address segments, standard modes, DHCP domains, and VLAN Layer 3 interfaces. You can perform the following operations on the U2000:

- Query, add, delete, and modify a DHCP server group.
- Query, add, delete, and modify a MAC address segment.
- Query, enable, disable, and modify a standard mode.
- Query, add, delete, and modify a DHCP domain.
- Modify a VLAN Layer 3 interface.

- Bind DHCPv6 server groups.

Layer 3 Routes Management

Layer 3 routes management includes the management of static routes, RRPP domains, and RRPP rings, and the configuration of IPv6 static routes.

MPLS/VPWS/VPLS Management

The Multi-protocol Label Switching (MPLS) network adopts the standard packet switching mode to forward Layer 3 packets and the label switching mode to exchange Layer 2 packets. Virtual private LAN service (VPLS) is a Layer 2 virtual private network (VPN) technology that is based on the MPLS and Ethernet technologies. VPLS is a way to connect multiple Ethernet LANs through packet switched networks (PSNs) for the LANs to work as one LAN. Virtual private wire service (VPWS) is a VPN technology that bears Layer 2 services. VPWS emulates services such as ATM, frame relay, Ethernet, low-speed TDM circuit, and SONET/SDH in a PSN.

You can perform the following configurations for MPLS tunnels on a per-NE basis on the U2000:

- Configure MPLS interface.
- Configure LDP remote peer.
- Create static LSP.
- Query MPLS LDP session.

The U2000 supports the following VPLS configurations:

- Configure virtual switch instances (VSIs) to map actual attachment circuits (ACs) of the VPLS to each PW.
- Configure ACs to transmit frames between customer edges (CEs) and provider edges (PEs).
- Configure PWs (virtual connections between PEs) to transmit frames between PEs.
- Configure PW protection groups to quickly switch data to the other PW if a PW is faulty.

The U2000 supports the following PW configurations for the VPWS:

- Query, add, delete, modify, and deploy PWs.
- Enable and disable PWs.
- Configure protection groups.
- Configure the committed access rate (CAR).

The U2000 supports the following E2E PWE3 management functions:

- Configure, deploy, undeploy, modify, or delete an E2E PWE3 link.
- Enable or disable an E2E PWE3 link.
- Collect performance statistics for an E2E PWE3 service.
- Configure BFD for an E2E PWE3 service.
- Check link connectivity for an E2E PWE3 service.

ACL and QoS Management

ACL and QoS management includes the management of the access control list (ACL), IPv6 ACL, quality of service (QoS), time segments, and hierarchical QoS (HQoS).

In a traditional packet-based network, all packets are treated in the same way. Every router adopts the first-in first-out (FIFO) policy to process packets and makes its best effort to transmit packets to the destination. The router, however, does not make any commitment to packet transmission performance, such as the delay, delay variation (jitter), packet loss rate, and reliability. More and more networks are connecting to the Internet and new services are emerging that raise the requirements on the service capability of IP networks. Therefore, network-wide end-to-end QoS solutions are being considered which will require devices to apply QoS techniques and provide hierarchical QoS assurance for different types of service streams (especially for those highly sensitive to delay and jitter). For ACL management, you can perform the following operations on the U2000:

- Configure one or more time segments, and associate a time segment with an ACL by specifying the name of the time segment in the ACL.
- Query, modify, create, and delete the ACL of the standard, extended, Layer 2, and user-defined types.
- QoS management includes filtering packets based on ACL, tagging priorities, limiting traffic and port rate, collecting statistics on traffic, redirecting, and mirroring. On the U2000, you can query, add, modify, and delete a QoS policy. For the mirroring, the product does not resolve or process the captured data.

HQoS stands for the hierarchical QoS. It not only controls user traffic but also schedules packets according to the priorities of user services. On the U2000, you can query, add, modify, and delete an HQoS policy.

BFD Management

The BFD mechanism is used for quickly checking the link status between two devices.

To mitigate the impact of device faults on services and to improve the network availability, a network device needs to quickly detect all faults occurring between the device and its adjacent devices and then take appropriate action to ensure service continuity. The BFD enables the device to check the connectivity for a type of data protocol on the same trail between two systems. The trail can be a physical or a logical link, including a tunnel. The BFD mechanism remedies weaknesses in the existing detection mechanisms.

You can perform the following operations on the U2000:

- Configure static BFD for a PW.
- Configure dynamic BFD for a PW.
- Configure static BFD for a static LSP.
- Configure static BFD for a dynamic LSP.

User Security and System Security Management

You can perform the following operations on the U2000:

- Configure user access in PITP mode.
- Configure user access in DHCP Option 82 mode.
- Configure user access control.
- Configure system secure access.

Ethernet Connectivity Fault Management

As the Ethernet technology extends from carrier networks to metropolitan area networks (MANs) and wide area networks (WANs), carriers are increasingly concerned about the

maintainability of equipment, especially Ethernet equipment. This concern has led to a demand for the operation, administration, and maintenance (OAM) of transport equipment.

802.1ag connectivity fault management (CFM): provides a method for detecting faults end-to-end. The Ethernet OAM mechanisms supported by 802.1ag CFM include continuity check (CC), loopback (LB), link trace (LT), and forward AIS alarms. You can perform the following operations on the U2000:

- Manage maintenance domains (MDs). Ethernet CFM divides a network into up to eight levels. A bridge can span multiple levels to manage different MDs. A CFM MD is constituted by bridges. An MD is the combination of bridges and maintenance levels. MDs can be classified into three layers: user domain (levels 7-5), service provider domain (levels 4-3), and carrier domain (levels 2-0). This type of management entity used depends on the type of MD deployed.
- Manage maintenance associations (MAs). An MD can be divided into multiple MAs. Each MA maps a service instance (SI) that belongs to an MD and is identified by a VLAN. An MA can be regarded as a combination of an MD and a VLAN. According to the standards, multiple VLANs can map one SI, and one SI maps one MA.
- Manage maintenance points (MPs). An MA consists of MPs defined on the ports of bridges. An MP is a combination of a bridge port, a VLAN, and a maintenance level. MPs are classified into maintenance association end points (MEPs) and maintenance association intermediate points (MIPs). MEPs initiate and respond to CFM messages; MIPs transparently transmit or respond to CFM messages but do not initiate the messages.

Y.1731-compliant Performance Monitoring

- Y.1731-compliant Ethernet OAM implements monitoring on the performance of a single NE in an FTTx network, including the pack loss rate, delay, jitter, and throughput. You can perform the following operations on the U2000:
 - Test single-ended packet loss in an on-demand manner and view the packet loss rate.
 - Perform bidirectional delay and jitter tests and view test results.
 - Change ONTs to MEPs.
 - Perform an Ethernet OAM test on a per-ONT basis.
 - View MEPs associated with VLANs or service ports in the VLAN or service port list.
 - Configure homing parameters for a maintenance domain.
 - View all MEP lists or MEP lists of specified MAs.

Protection Group Management

Protection group management involves the protection switchover and protection group.

Protection switchover: Important card resources and port resources are generally backed up to enhance system reliability. If a fault occurs on a working member, protection switchover will be triggered to transfer services to the protection member that will continue to handle the services.

Protection group: You can manage the working member and the protection member in the protection group. In a protection group, you can manage the relationship between the members involved in the protection switchover, record the status of members, and manage the configuration data and status of the involved members.

With the protection group feature, you can protect the following objects on the U2000:

- Active and standby control cards
- Aggregation groups on active control cards and standby control cards
- Ports on active and standby control cards
- Upstream Ethernet ports
- Upstream aggregation links of Ethernet ports
- Objects configured with GPON/EPON type B protection
- Objects configured with GPON type C protection, including the three scenarios: single-homing, dual-homing, and dual PON ports on an ONU for independent upstream transmission.
- Objects configured with EPON type D protection

GPON Service Management

Gigabit passive optical network (GPON) is a passive optical transmission technology. GPON supports a downstream transmission rate of 2.448 Gbit/s and an upstream transmission rate of 1.244 Gbit/s. In addition, it supports 10G GPON features.

GPON service management supports two modes: distributed mode and profile mode. The equipment and the U2000 support both modes. In the distributed mode, GPON service management includes the management of the UNI ports, GEM ports, and ONUs. In the profile mode, GPON service management includes the management of the UNI ports and ONUs; in this mode, the GEM port is encapsulated in the line template of the UNI port.

U2000 supports the 10G GPON management, and the GUI configuration is the same as the 1G GPON services.

For GPON UNI port management, you can perform the following operations on the U2000:

- Modify the port attributes, such as the minimum reach, maximum reach, configuration status of the ONU auto-discovery function, configuration status of the downstream FEC function, status of the laser switch, and update cycle of the encryption key of the GPON UNI port.
- Enable and disable the ONU auto-discovery function for a GPON UNI port. After the ONU auto-discovery function is enabled, the OLT periodically checks whether any ONUs that were recently connected to the GPON UNI port have gone online.
- Cut over services to implement GPON port backup on the OLT. If the active GPON port on the OLT is faulty, you can switch over the ONU services from the faulty GPON port to a specified standby GPON port on the OLT.
- Query the alarms of GPON UNI ports. This function allows you to maintain and manage GPON UNI ports according to suggested solutions for active alarms.
- Enable and disable the laser of a GPON UNI port. By default, the laser of a GPON UNI port is enabled so that the ONUs connected to the GPON UNI port can go online.
- Collect statistics on optical power, perform continuous-mode ONU detection (alarms are generated when continuous-mode rogue ONUs are detected), and detect and isolate rogue ONUs connected to PON UNI ports.
- Configure the ANCP.
- Query real-time performance statistics and delete performance statistics.
- Locate to a specified port quickly in the optical distribution node (ODN) topology view. The GPON UNI port, functioning as an ODN, can be connected to a remote ONU. With

this feature, you can enter the ODN topology view and view the ODN-centered star topology. In addition, you can add, delete, and modify the ONU, and configure relevant services. Add, delete, and modify the Hand-in-Hand Topo.

- Query the running status, bandwidth usage, and last online time of an ONU.
- Query the information about an optical transceiver, including the temperature, offset current, transmitted optical power, power supply voltage, received optical power, length, wavelength, manufacturer information, and type.
- Learn the packet pass-through or drop status of a specified queue by querying the performance statistics.

A GEM port identifies the virtual service channel that carries service streams between an OLT and an ONU. An ONU can provision services only after the mapping between the GEM port, T-CONT, and service stream is configured on the ONU. For GEM port management, you can perform the following operations on the U2000:

- Enable and disable the encryption function. When the encryption function is enabled, the device encrypts the service stream carried on the GEM port. This feature enhances the security of service data.
- Bind a GEM port to an ONU to establish the mapping between the GEM port on the OLT and the T-CONT on the ONU.
- Rate limit a GEM port. You can rate limit the packets of a specified priority on a GEM port according to the specified traffic profile.
- Query real-time performance statistics and delete performance statistics of a GEM port.

An ONU provides user interfaces. A GPON UNI port can be connected to a maximum of 256 ONUs. For GPON ONU management, you can perform the following operations on the U2000:

- OLTs perform remote operations and configuration management on ONUs by using the OMCI (agent management) and SNMP protocols.
- Add, delete, modify, and confirm an ONU.
- Generate ODN topological view nodes. Perform this operation to generate nodes for ONT management in the ODN topology view.
- Directly locate an ONU in the topology view through the topological node.
- Locate an MDU in the NE Panel.
- Activate and deactivate an ONU.
- Re-register an ONU. After an online ONU is reset by force, the ONU re-registers with the OLT to update the registration information about the ONU.
- Re-discover an ONU. ONU re-discovery is applicable only to ONUs that use the once-on authentication mode.
- Configure the parameters of value-added service (VAS). The VAS feature of the GPON ONU is used for configuring services such as the VoIP service.
- Provision services. This feature is used for configuring services for a single ONU or for a single service port of MDUs by binding a global service provisioning template or by setting service parameters.
- Upgrade ONUs. This feature is used for concurrent upgrades of multiple types of ONTs. During upgrades, target versions are automatically generated based on the selected ONT version files.
- Configure the QoS.

- Enable and disable the DHCP V6 Option 82 forwarding.
- Query real-time performance statistics and delete performance statistics.
- Browse current and historical alarms and events.
- Query the MAC addresses of ONTs in batches.
- Query and configure the UNI port of an ONT, including Ethernet ports and POTS ports.
- Configure CAR.
- Query E8C or non E8C terminal.
- Query the details, running Info. (such as running status, power supply condition, online duration and last up time), alarm status, service port and last online time of an ONU.

- Details

GPON UNI Port		GPON ONU		ONU Details	
Status	Operation Status	Config Status	Frame	Slot	Port
Active (...	Activate	Normal	0	5	0
No.1, Total: 1, Selected: 1 Updated at: 07/07/2016 13:43:27					
Details	Running Info	Alarm State	>>		
Frame	= 0				
Slot	= 5				
Port	= 0				
ONU ID	= 6				
Name	= 10.185.214.193/Frame0/Slot5/Port0/OnuID6				
Alias	= --				
Rate Type	= Auto				
Authentication Mode	= SW				
Discovery Mode	=				
SN	= 485754430F77C909				
Password	= --				
Timeout Period (h)	= --				
Re-authentication Mode	= --				
Alarm Profile	= --				
ONU Capacity Profile	= test				
ONU Service Level Profile	= alarm-policy_0				
ONU VAS Profile	= --				
ONU General VAS Profile	= --				
T-ROG99 Server Profile	= --				
ONU Power Reduction Profile	= --				
Multicast Forward Mode	= Unconcern				
Multiple Multicast VLAN Configuration	= Close				
Multicast Forward VLAN(1~4095)	= --				
Multicast Mode	= Unconcern				
Upstream IGMP User VLAN 1	= --				
ONU Upstream IGMP packet forward mode 1	= Unconcern				
Upstream IGMP packet forward VLAN 1	= --				
Upstream IGMP Packet Forwarding Priority 1	= --				
Upstream IGMP User VLAN 2	= --				
ONU Upstream IGMP packet forward mode 2	= --				
Upstream IGMP packet forward VLAN 2	= --				
Upstream IGMP Packet Forwarding Priority 2	= --				

- Running Info.

GPON UNI Port - GPON ONU - ONU Details														
Status	Operation Status	Config Status	Frame	Slot	Port	ONU ID	Name	Alias	Vendor ID	Terminal Type	Software Version	Is E8C Device	Line Profile	Service Profile
Activate	Normal	Normal	0	3	2	0 10.144.194...--	HWTC	5698	V8R313C00	Unknown	MDU-5620G	—	line-profile_d_	srv-profile
Activate	Normal	Normal	0	3	2	1 10.144.195...--	HWTC	HG8245H	V3R016C00	False	line-profile_d_	srv-profile	—	—
No.3, Total: 5, Selected: 1 Updated at 03/24/2015 11:46:23														
Add E2E Service... Real-Time Performance ONU Details														
Line Profile Service Profile Alarm Profile Multicast Forwarding Entry IP Host POTS User MG WAN Interface UMAC-VMAC Info RTP Interface T-CONT GEM Port FEC Details														
Details Running Info Alarm State ONU Optics Module Info Current ONU: UNI Port Info Service Port Info IGMP User T-CONT GEM Port FEC Details														
Running Info														
Running Status	= Online													
Operation Status	= Activate													
Config Status	= Normal													
Work Mode	= Normal Mode													
DBA Type	= SR													
Match Status	= Match													
Discovery Status	= --													
DMT Battery State	= Holding													
OMCI Status	= Normal													
Number of Learned MAC Addresses	= 0													
Bridge MAC Address	= 00-E0-PC-55-55-88													
Ranging Value (s)	= 38													
ONU Off Line Reason	= --													
Last Up Time	= 03/21/2015 19:52:54													
Last Down Time	= --													
Last Down Cause	= --													
Last Dying Gasp Occur Time	= --													
SDI alarm	= None													
SFI alarm	= None													
DOWS alarm	= None													
LOGi alarm	= None													
UNI Online Duration	= 2 Days 16 Hours 11 Minutes 36 Seconds													
Interoperation Mode	= iGurt													
EITH DAM Support Capability	= Not Support													
Used mutual auth	= No													
Anti-Broadcast-Attack Ont Query Remain Time(minute)	= --													

- Service Port Info.

GPON UNI Port - GPON ONU - ONU Details														
Status	Operation Status	Config Status	Fra...	Slot	Port	ONU ID	Name	Alias	Vendor ID	Terminal Type	Software Version	Is E8C Device	Line Profile	Service Profile
Activate	Normal	Normal	0	3	2	1 10.144.195...--	HWTC	HG8245H	V3R016C00	False	line-profile_d_	srv-profile	alarm-profile	—
Activate	Normal	Normal	0	3	2	2 10.144.195...--	HWTC	HG8110H	V3R016C00	False	6245_3	8245_0204	alarm-profile	—
No.3, Total: 5, Selected: 1 Updated at 03/24/2015 11:52:39														
Add E2E Service... Real-Time Performance ONU Details														
Line Profile Service Profile Alarm Profile Multicast Forwarding Entry IP Host POTS User MG WAN Interface UMAC-VMAC Info RTP Interface T-CONT GEM Port FEC Details														
Details Running Info Alarm State ONU Optics Module Info Current ONU: UNI Port Info Service Port Info IGMP User T-CONT GEM Port FEC Details														
WAN Interface														
Name	Service Type	Connection Type	IPv4 Connection Status	IPv4 Address	IPv6 Connection Status	IPv6 Address	VLAN ID	Priority	Option60	Admin State	MAC Address	IPv4 DNS Server		
A1	TR069	IP Route	Disconnected	--	Invalid	--	202	0	Without	Disable	00-10-26-21-24..	0.0.0.0		
4	Internet	IP Route	Disconnected	--	Invalid	--	1	0	Without	Disable	00-10-26-21-24..	0.0.0.0		
5	Internet	IP Route	Disconnected	--	Invalid	--	1	0	Without	Disable	00-10-26-21-24..	0.0.0.0		
2	Internet	IP Route	Disconnected	--	Invalid	--	1	0	Without	Disable	00-10-26-21-24..	0.0.0.0		
3	Internet	IP Route	Disconnected	--	Invalid	--	1	0	Without	Disable	00-10-26-21-24..	0.0.0.0		
8	Internet	IP Route	Disconnected	--	Invalid	--	1	0	Without	Disable	00-10-26-21-24..	0.0.0.0		
6	Internet	IP Route	Disconnected	--	Invalid	--	1	0	Without	Disable	00-10-26-21-24..	0.0.0.0		
7	Internet	IP Route	Disconnected	--	Invalid	--	1	0	Without	Disable	00-10-26-21-24..	0.0.0.0		

EPON Service Management

The Ethernet passive optical network (EPON) is a new-generation broadband access technology that uses point to multi-point (P2MP) structures and passive optical fiber transmission modes. As a new technology of fiber broadband access for the "last mile", the PON does not require node devices but only a simple optical splitter at the optical branching point. Therefore, the PON has the following features:

- Fewer optical fibers.
- Shared bandwidth between branches.
- Less investment in telecommunications rooms.
- Higher equipment security.
- Faster network deployment.
- Lower overall costs for network construction.

The EPON uses the wavelength division multiplexing (WDM) technology for concurrent bidirectional signal transmission. Upstream and downstream signals are transmitted over different wavelengths: upstream uses a 1310 nm wavelength and downstream uses a 1490 nm wavelength. The EPON provisions the voice, data, and video services for users over a single optical fiber.

Currently, the EPON supports a maximum symmetric transmission rate of 1.25 Gbit/s upstream and downstream, and a maximum transmission reach of 20 km. In downstream direction, the EPON broadcasts encrypted data to different users; in upstream direction, the EPON employs time division multiplexing (TDM) technology. In this way, the EPON shares bandwidth in upstream and downstream directions and accommodates the bandwidth requirements of access users.

U2000 supports the 10G EPON management, and the GUI configuration is the same as the 1G EPON services.

EPON service management includes the management of EPON UNI ports and ONUs.

The EPON UNI port is the downstream port for the EPON access. The OLT is connected to various types of ONUs (including MDUs) through the UNI port to provision high-speed Internet service for users. For EPON UNI port management, you can perform the following operations on the U2000:

- Modify the attributes of an EPON UNI port, including the alias, ONU auto-discovery function, the maximum distance between an ONU and the OLT, and the tag attribute of packets.
- Locate to a specified port quickly in the ODN topology view. The EPON UNI port, functioning as an ODN, can be connected to a remote ONU. With this feature, you can enter the ODN topology view and view the ODN-centered star topology. In addition, you can add, delete, and modify the ONU, and configure relevant services.
- Enable, disable, and reset an EPON UNI port. The laser of an EPON UNI port is enabled by default so that the ONUs connected to the EPON UNI port can go online.
- Collect statistics on optical power, perform continuous-mode ONU detection (alarms are generated when continuous-mode rogue ONUs are detected), and detect and isolate rogue ONUs connected to PON UNI ports.
- Enable and disable the ONU auto-discovery function for an EPON UNI port. After the ONU auto-discovery function is enabled, the OLT periodically checks whether any ONUs that were recently connected to the EPON UNI port have gone online.
- Cut over services to implement EPON port backup on the OLT. If the active EPON port on the OLT is faulty, you can switch over the ONU services from the faulty EPON port to a specified standby EPON port on the OLT.
- Query the alarms of EPON UNI ports. This function allows you to maintain and manage EPON UNI ports according to suggested solutions for active alarms.
- Query real-time performance statistics and delete performance statistics.
- Query the running status, bandwidth usage, and last online time of an ONU.
- Query the information about an optical transceiver, including the temperature, offset current, transmitted optical power, power supply voltage, and received optical power.
- Learn the packet pass-through or drop status of a specified queue by querying the performance statistics.

An ONU provides user interfaces. For EPON ONU management, you can perform the following operations on the U2000:

- OLTs perform remote operations and configuration management on ONUs by using the OMCI (agent management) and SNMP protocols.
- Add, delete, and modify an ONU.
- Generate ODN topological view nodes. Perform this operation to generate nodes for ONT management in the ODN topology view.

- Directly locate an ONU in the topology view through the topological node.
- Locate an MDU in the NE Panel.
- Activate and deactivate an ONU.
- Re-register an ONU. After an online ONU is reset by force, the ONU re-registers with the OLT to update the registration information about the ONU.
- Re-discover an ONU. ONU re-discovery is applicable only to ONUs that use the once-on authentication mode.
- Configure the parameters of value-added service (VAS). The VAS feature of the EPON ONU is used for provisioning VAS, such as the VoIP service.
- Provision services. This feature is used for configuring services for a single ONU or for a single service port of MDUs by binding a global service provisioning template or by setting service parameters.
- Upgrade ONUs.
- Query real-time performance statistics and delete performance statistics.
- Browse current and historical alarms and events.
- Query and configure the UNI port of an ONT, including Ethernet ports and POTS ports.
- Query E8C or non E8C terminal.
- Query the details, running Info. (such as running status, power supply condition, online duration and last up time), alarm status, service port and last online time of an ONU.

- Details

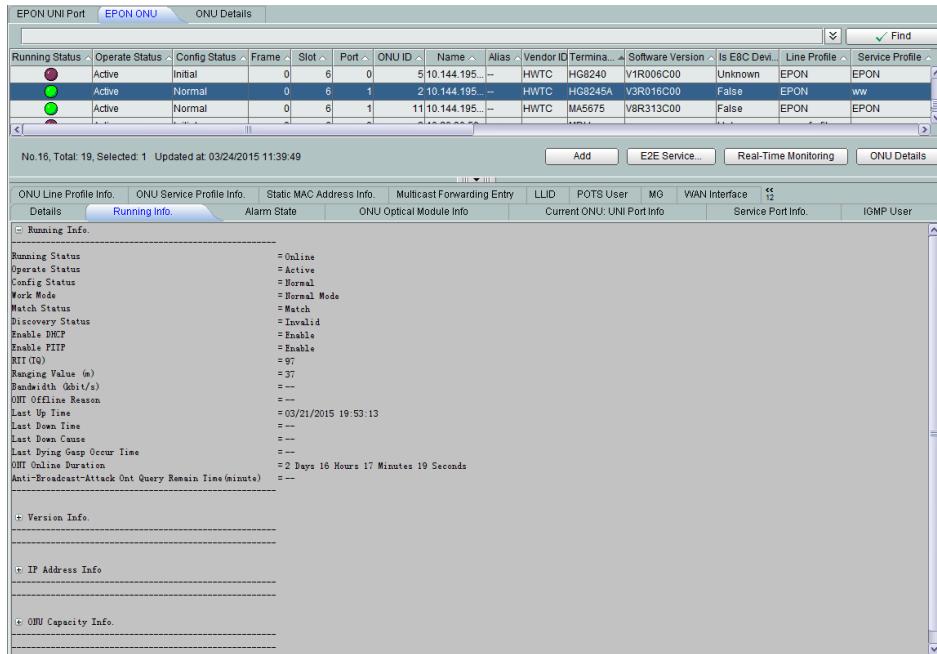
EPON ONU											
ONU Details											
Running Status	Operate Status	Config Status	Frame	Slot	Port	ONU ID	Name	Alias	Vendor ID	Termina...	Software Version
Active	Initial		0	6	0	5 10.144.195.---	HWTc	HG8240	V1R006C00	Unknown	EPON
Active	Normal		0	6	1	2 10.144.195.---	HNTc	HG8245A	V3R016C00	False	EPON
Active	Normal		0	6	1	11 10.144.195.---	HWTc	MA5675	V8R313C00	False	EPON

No. 16, Total: 19, Selected: 1 Updated at 03/24/2015 11:39:49

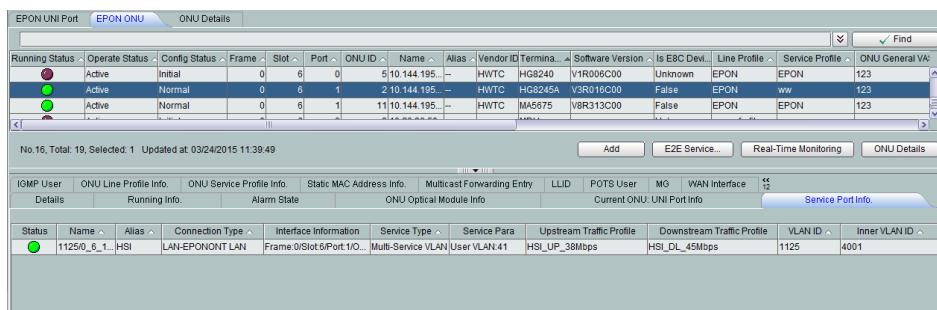
Add E2E Service... Real-Time Monitoring ONU Details

ONU Line Profile Info.	ONU Service Profile Info.	Static MAC Address Info.	Multicast Forwarding Entry	LLID	POTS User	MG	WAN Interface	Current ONU: UNI Port Info	Service Port Info.	IGMP User
Frame	Slot	= 0								
Slot	Port	= 6								
Port	ONU ID	= 1								
ONU ID	Splitter Port ID	= 2								
Splitter Port ID	Spanner Port ID	= --								
Spanner Port ID	Name	= 10.144.195.45 Frame/Slot6/Port1/OnuID2								
Name	Alias	= 10.144.195.45								
Alias	Rate Type	= 1G/1G								
Rate Type	Line Profile	= EPON								
Line Profile	Service Profile	= --								
Service Profile	MAC Address	= alarm-policy_0								
MAC Address	Vendor ID	= 00-E0-FC-00-00-08								
Vendor ID	Terminal Type	= HWTc								
Terminal Type	Software Version	= HG8245A								
Software Version	ONU VAS Profile	= V3R016C00								
ONU VAS Profile	ONU General VAS Profile	= --								
ONU General VAS Profile	TDR09 Server Profile	= 123								
TDR09 Server Profile	Is EEC Device	= --								
Is EEC Device	ONT Description	= False								
ONT Description	Authentication Mode	= EchoLife HG8245A EPON Terminal (PK20/PRODUCT ID:)								
Authentication Mode	Authentication Type	= MAC Address								
Authentication Type	Timeout Period (s)	= --								
Timeout Period (s)	Protection Role	= Working								
Protection Role	Optical Alarm Profile	= --								
Optical Alarm Profile	IGMP Mode	= IGMP snooping								
IGMP Mode	Downstream Traffic Profile	= DEFAULT_MOCOS								
Downstream Traffic Profile	Epon Alarm Profile	= f								
Epon Alarm Profile	Epon Warning Profile	= --								
Epon Warning Profile	Anti-Broadcast-Attack Ont Rate (pps)	= --								

- Running Info.



- Service Port Info.



Multicast Service Management

Multicast is a point-to-multipoint (P2MP) communication mode in which the source sends information to a specified subset of objects under a network node. Multicast services are applicable to the streaming media, distance learning, video conferencing, video on demand (VOD), network gaming, data replication, and other P2MP transmission.

Multicast communication uses a class D IP address (224.0.0.0 to 239.255.255.255) as the destination IP address. A source host sends out a packet that uses a class D IP address as the destination. If other hosts in the network are interested in the multicast packet, these hosts can send a request to join the multicast group and receive the packet. Hosts outside of the group cannot receive the packets sent by the source host.

In controllable multicast, network equipment determines whether a user has the rights to watch programs by identifying the join or request packets of the user. Then, the access device controls and forwards the multicast services accordingly.

There are two multicast modes:

- **IGMP snooping:** IGMP snooping is a multicast control mechanism at the data link layer. It is used to manage and control multicast services.
- **IGMP proxy:** In a tree topology, the OLT does not set up routes for forwarding multicast packets; the OLT only relays and forwards multicast protocol packets. To multicast

users, the OLT is a multicast router that implements the router functions defined in the IGMP protocol. To multicast routers, the OLT is a multicast user.

You can perform the following operations on the U2000 to manage multicast services:

- Manage multicast users.
- Manage multicast VLANs.
- Manage the virtual upstream ports of multicast services.
- Manage multicast subtending ports.

Support IPv6 multicast: By using IPv6 multicast technologies, the network device can manage, control, and forward IPv6 video services and in this way meets carriers' requirements for provisioning IPv6 video services.

Global Template Management

A global template is a set of attributes that features offline configuration, global effectiveness, and less duplication of data. You can add, delete, copy, modify, and apply a global template to NEs on the U2000. The U2000 supports global templates such as ADSL templates, VDSL2 templates, G.SHDSL templates, Vector templates, TID templates, digital map templates, digital map group templates, ETH alarm templates, VLAN service templates, Cable templates, bonding group templates, R2 signaling templates, SNMP templates, number change templates, MPLS TC field mapping templates, PQ Mapping templates, GPON templates, EPON templates, ONU service level profile, ONT VAS profile, power shedding templates, IGMP templates, traffic templates, VLAN templates, optical transceiver alarm templates, WRED templates, service provisioning template, ACL templates, RAIO templates, CoS group templates, and system parameter templates.

Alarm Responsibility Division

The alarm responsibility division function helps quickly and accurately identify the possible cause of an out-of-management alarm on an ONU, such as whether the backbone optical fiber or branch optical fiber is faulty, or whether the terminal is experiencing a power outage. In this manner, service calls to the site are reduced.

FTTH video quality demarcation

Video quality can be monitored and demarcated on OLT PON boards and ONTs. Whether faults exist on the access side can be diagnosed remotely. In this manner, the O&M cost is slashed and video quality demarcation becomes easy.

- On the U2000, set the video quality thresholds and create monitoring tasks. Then monitoring results can be easily viewed in tabular and graphical forms.
- The U2000 provides test data for indicators, assesses the excellent/good rate, and presents test results in a macro chart and micro chart so that faults can be diagnosed quickly and accurately.

ODN Topology View

An optical distribution network (ODN) contains a series of lines and equipment, which resides between the OLT and the ONUs (ONTs). The ODN provides a physical transmission channel for optical signals and also distributes power of these optical signals. An ODN network consists of passive optical components, such as optical fibers, fiber attenuator, fiber connectors, optical connectors, and optical splitters. The ODN topology view displays the

status of PON UNI ports on the OLT, optical splitters, ONUs, and optical fibers. You can perform the following operations on the U2000:

- Bulks importing tables to quickly create a topology view and display relationships between OLT PON ports, splitters, and ONUs.
- Right-click an OLT or MDU in the Main Topology to open the ODN topology view.
- Add, modify, and delete an ONU. The ONU managed object is not deleted.
- Add, delete, and modify the optical splitter. Multiple-level optical splitters can be created.
- Configure fiber attributes.
- Move one or more ONUs from one optical splitter to another optical splitter.
- Locate to the MDU, ONU list, and PON list in the Main Topology.
- Save the node locations in the topology view and zoom in nodes in the topology view.
- Display the alarm, link, and management status of fibers, ONUs, and PON ports.
- Locate to the OLT node in the Main Topology.
- Locate to an ONU in the ODN view by pressing **Ctrl+F**.
- Display the protection status of PON ports.
- Display the complete topology of dual PON ports on ONU for independent upstream.
- Add, modify, and delete Hand-in-Hand Topo.
- Update the ONU topology view in real time after the ONU running status is changed or ONUs are added, modified, or deleted.

The U2000 provides the following navigation paths for managing ONUs, OLTs, and PON ports.

- Navigation paths to the NE Panel of OLTS and MDUs.
- Navigation paths to the replacement of ONUs.
- Navigation paths to the import of configuration scripts of OLTS and MDUs.
- Navigation paths to the environment monitoring for MDUs.
- Navigation paths to the ONU real-time performance statistics collection.
- Navigation paths to the browsing, synchronization, and acknowledgment of the active alarms of OLTS and ONUs.
- Navigation paths to the browsing of active alarms of PON ports.

Line Test

The U2000 provides a dedicated system for the line test to shorten the maintenance period of line faults, and facilitate the user operations. The line test diagnoses the subscriber line from the aspects of electrical attributes (such as capacitance, resistance, and voltage), physical characteristics (such as length), and bearer services capabilities (such as upstream rate and downstream rate). The test result provides references for the line service capability predication, troubleshooting, subscription, and line selection. You can perform the following operations on the U2000:

- PSTN and POTS port caller or called emulation test
- Loop-line test
- Circuit test

- xDSL port single-ended test (SELT), dual-ended test (DELT), and MELT
- Dial monitor test
- Loop test
- Capturing, releasing, and monitoring a test bus
- CO emulation

8.7.2 ONU Management

The U2000 provides graphical user interfaces (GUIs) for configuring NEs and maintaining NE configurations. You can configure services for equipment in the GUIs.

Battery Discharge Test

You can perform the following operations on the U2000:

- Query information about network-wide battery discharge tests.
- Import NEs for which battery discharge tests will be performed.
- Start or stop a battery discharge test.
- Export test results.

NE Management

NE management includes the management of NE panels, basic and common NE attributes, clock sources, security, protocols, global configuration of services, and NE templates.

NE Panel Management

You can perform the following operations on the U2000:

- Display the NE panel by double-clicking an NE.
- Query the details of devices.
- Collect statistics on device resources.
- Query the information about shelves.
- Collect the statistics on shelf resources.
- Query inter-shelf links.
- Add, delete, enable, disable, reset, and confirm a card.
- Query real-time performance statistics on the CPU usage and memory of cards.
- Display the port view by double-clicking a card.

Management of Basic and Common Device Attributes

The management of basic and common device attributes includes querying the global information about devices and configuring global policies for devices.

You can perform the following operations on the U2000:

- Query the system information about devices.
- Query resource and status statistics of devices.
- Query the license information about the functions and resources of NEs.
- Configure the system time, IP address of an NE, and the binding between a Layer 3 interface and an IP address.

- Configure the SNMP protocol port.
- Set device handshake parameters.
- Configure the policy for automatically backing up NE data.
- Enable and disable the energy-saving function of a device.
- Configure and manage license files.

Clock Source Management

Clock source management includes the management and configuration of NE-specific clock source information, such as information about the line clock, 1588v2 clock, clock priorities and clock interface.

Security Management

You can perform the following operations on the U2000:

- Enable and disable anti-ICMP attack, anti-IP attack, anti-IP spoofing, anti-MAC spoofing, and anti-DoS attack.
- Set the aging time of an MAC address.
- Enable and disable MAC address learning.
- Configure the security attributes for user login in the CLI.

Protocol Management

You can perform the following operations on the U2000:

- Manage the Link Aggregation Control Protocol (LACP), Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP), Bidirectional Forwarding Detection (BFD), and Internet Group Management Protocol (IGMP).
- Control the Address Resolution Protocol (ARP) proxy.
- Configure the Policy Information Transfer Protocol (PITP) mode/Relay Agent Info Option (RAIO) custom format.
- Control the Dynamic Host Configuration Protocol (DHCP) Option 82 function.
- Control the DHCP proxy and DHCP relay forwarding functions.
- Configure 802.1ag attributes of the Ethernet packet.

Global Configuration of Services

The global configuration of services includes the configuration of the VLAN, QoS, xDSL, and multicast services.

Device Template Management

NE template management includes the display of different types of NE templates on the U2000. Templates include voice templates, DSL templates, Vector templates, IGMP templates, traffic templates, VLAN service templates, optical transceiver alarm templates, EOC CBAT line template, and EOC CNU line template. Currently, the U2000 supports querying, deleting, and generating global templates, and supports downloading global templates to NE.

You can search for network-wide ONUs based on location information. The location information includes IP addresses, SNs, MAC addresses, LOIDs, keys, profiles (line profiles, service profiles, and service level profiles), version information (vendor IDs, terminal types,

software versions, and E8C device attributes), ONU IDs, telephone numbers, aliases, and voice IP addresses.

Network Interface Management

Network interface management includes the management of GPON NNI ports, EPON NNI ports, Ethernet ports, and xDSL bonding groups. GPON NNI ports support an 10G PON port, which has an upstream bandwidth of 2.5 Gbit/s and a downstream bandwidth of 10 Gbit/s.

Management of GPON NNI Ports

The GPON network to network interface (NNI) is the upstream port provided by the control card. You can perform the following operations on the U2000:

- Configure the suppression level of the broadcast, multicast, and unknown unicast packet traffic.
- Configure and query the alarm thresholds of an optical transceiver.
- Collect real-time performance statistics on the number of discarded Ethernet frames, transmitted Ethernet frames, received Ethernet frames, transmitted GEM frames, received GEM frames, transmitted PLOAM messages, received PLOAM messages, transmitted OMC messages, and received OMC messages.

Management of EPON NNI Ports

EPON NNI is the upstream port provided by the ONU. You can perform the following operations on the U2000:

- Configure and query the alarm thresholds of an optical transceiver.
- Collect real-time performance statistics on the number of transmitted frames, transmitted bytes, received frames, received bytes, received OAMPDU frames, and received MPCP frames.

Management of Ethernet Ports

Ethernet port management includes the management of ports and aggregation groups. You can perform the following operations on the U2000:

- Configure port attributes.
- Create, delete, query, and modify an aggregation group.
- Activate and deactivate an Ethernet port.
- Collect real-time performance statistics and delete performance statistics.
- Configure the PPPoE, DHCP Option 82, 802.3ah ETH OAM loopback, and port rate limit functions.
- Query the attributes of optical transceivers for Ethernet optical ports.
- Configure automatic control of optical signal transmission.

Management of xDSL Bonding Groups

You can perform the following operations on the U2000:

- Create, delete, and modify an xDSL bonding group.
- Set the upstream PVC value for an xDSL bonding group.

Connection Management

PVC

The ATM virtual connection is the logical relationship between the link endpoints in the ATM network. That is, it is the communication path for transmitting ATM cells between two or multiple endpoints. It can be used to transmit information between users, between users and networks, and between networks.

Service Virtual Port Management

A service virtual port enables user equipment to access the ONU. The service virtual port provides service streams between the user equipment and the ONU for carrying user services. You can perform the following operations on the U2000:

- Query, add, delete, modify, activate, and deactivate a service virtual port.
- Collect real-time performance statistics and delete performance statistics.
- Perform ATM ping tests.
- Configure the extended attributes of a service virtual port. Extended attributes allow for greater flexibility in addressing customer requirements. Extended attributes include the maximum number of learnable MAC addresses, the PPPoE session, the encapsulation type, and the maximum number of MAC addresses that can be bound.
- Configure the connection attributes of a service virtual port, including the alias, VPI/VCI, transmit traffic profile, and receive traffic profile.
- Shift the VLAN ID of a service virtual port to change the VLAN ID of the service virtual port. After successful shifting, the service port will assume the new VLAN ID.
- Bind IP addresses to a service virtual port and query the bound IP addresses. Performing this operation will allow only users with specified IP addresses to access the service virtual port. After successful binding, the service forwarding module will check the source IP address of user packets. If the source IP address does not match any of the IP addresses bound to the service virtual port, the user packets will be dropped. This feature ensures security in user access.
- Bind static MAC addresses to a service virtual port. Performing this operation will allow only users with specified MAC addresses to access the service virtual port. After successful binding, the service forwarding module will check the source MAC address of user packets. If the source MAC address does not match any of the MAC addresses bound to the service virtual port, the user packets will be dropped. This feature ensures security in user access.
- Support the Atm-ping, detects the connectivity of the ATM link to determine whether the line between the device and the modem of the user is reachable.
- Configure service bundles. If several service virtual ports carry the same service, a service bundle can be configured.

SPC

A semi-permanent connection (SPC) can implement the connection, release, check, and protection of one or more 64 k channels of ports on the same or different cards. An SPC occupies the dedicated and fixed voice channel. Therefore, the communication requirements of special and important access users are met and the communication quality is ensured.

Native TDM Connection

E1 connection encapsulates TDM frames into GPON GEM frames and transmits the TDM service over the GPON network.

SAToP Connection

Structure-Agnostic Transport over Packet (SAToP) is the circuit emulation service simulated on the packet-based network. When data packets are transmitted on a TDM network and a

traffic stream is identified by a TDM connection ID, configure a SAToP connection in case of unstructured TDM data.

Layer 2 Management

Layer 2 management includes the management of the VLAN, the Rapid Spanning Tree Protocol (RSTP), the Multiple Spanning Tree Protocol (MSTP), and the Access Node Control Protocol (ANCP), and the configuration of PPPoE clients.

VLAN Service Management

VLAN service management includes the management of the standard VLAN, MUX VLAN, smart VLAN, and super VLAN. You can perform the following operations on the U2000:

- Query, add, delete, and modify a VLAN.
- Collect real-time performance statistics of a VLAN.
- Clear real-time performance statistics of a VLAN.
- Manage a Layer 3 interface and its subinterfaces.

RSTP Management

You can perform the following operations on the U2000:

- Modify and restore the default value for the trail overheads on a port.
- Collect port RSTP statistics.
- Clear port RSTP statistics.

MSTP Management

MSTP management includes the management of domains, instances, and ports. You can perform the following operations on the U2000:

- Modify and restore the default setting of a domain.
- Add, delete, and modify an instance.
- Modify a port.
- Query the statistics of a port.

ANCP Management

You can perform the following operations on the U2000:

- Add, delete, modify, enable, and disable an ANCP session.
- Query the real-time status of an ANCP session.

PPPoE Client Configuration

You can add, delete, enable, and disable a PPPoE client on the U2000.

Layer 3 Management

Layer 3 management includes Dynamic Host Configuration Protocol (DHCP) management and IPv4 static route management.

DHCP management

DHCP management includes the management of DHCP server groups, MAC address segments, standard modes, DHCP domains, and VLAN L3 interfaces. You can perform the following operations on the U2000:

- Query, add, delete, and modify a DHCP server group.
- Query, add, delete, and modify a MAC address segment.
- Query, enable, disable, and modify a standard mode.
- Query, add, delete, and modify a DHCP domain.
- Modify a VLAN Layer 3 interface.

Route management

Layer 3 routing supports configuration of IPv4 static routes.

ACL and QoS Management

ACL and QoS management includes the management of the access control list (ACL), quality of service (QoS), and time segments.

In a traditional packet-based network, all packets are treated in the same way. Every router adopts the first-in first-out (FIFO) policy to process packets and makes its best effort to transmit packets to the destination. The router, however, does not make any commitment to packet transmission performance, such as the delay, delay variation (jitter), packet loss rate, and reliability. More and more networks are connecting to the Internet and new services are emerging that raise the requirements on the service capability of IP networks. Therefore, network-wide end-to-end QoS solutions are being considered which will require devices to apply QoS techniques and provide hierarchical QoS assurance for different types of service streams (especially for those highly sensitive to delay and jitter). For ACL management, you can perform the following operations on the U2000:

- Configure one or more time segments, and associate a time segment with an ACL by specifying the name of the time segment in the ACL.
- Query, modify, create, and delete the ACL of the standard, extended, Layer 2, and user-defined types.
- QoS management includes filtering packets based on ACL, tagging priorities, limiting traffic and port rate, collecting statistics on traffic, redirecting, and mirroring. On the U2000, you can query, add, modify, and delete a QoS policy. For the mirroring, the product does not resolve or process the captured data.

User Security and System Security Management

You can perform the following operations on the U2000:

- Configure user access in PITP mode.
- Configure user access in DHCP Option 82 mode.
- Configure user access control.
- Configure system secure access.

BFD Management

The BFD mechanism is used for quickly checking the link status between two devices.

To mitigate the impact of device faults on services and to improve the network availability, a network device needs to quickly detect all faults occurring between the device and its adjacent devices and then take appropriate action to ensure service continuity. The BFD enables the device to check the connectivity for a type of data protocol on the same trail between two systems. The trail can be a physical or a logical link, including a tunnel. The BFD mechanism remedies weaknesses in the existing detection mechanisms.

Ethernet Connectivity Fault Management

As the Ethernet technology extends from carrier networks to metropolitan area networks (MANs) and wide area networks (WANs), carriers are increasingly concerned about the maintainability of equipment, especially Ethernet equipment. This concern has led to a demand for the operation, administration, and maintenance (OAM) of transport equipment. The 802.1ag connectivity fault management (CFM) provides a method for detecting faults end-to-end. The Ethernet OAM mechanisms supported by 802.1ag CFM include continuity check (CC), loopback (LB), link trace (LT), and forward AIS alarms. You can perform the following operations on the U2000:

- Manage maintenance domains (MDs). Ethernet CFM divides a network into up to eight levels. A bridge can span multiple levels to manage different MDs. A CFM MD is constituted by bridges. An MD is the combination of bridges and maintenance levels. MDs can be classified into three layers: user domain (levels 7-5), service provider domain (levels 4-3), and carrier domain (levels 2-0). This type of management entity used depends on the type of MD deployed.
- Manage maintenance associations (MAs). An MD can be divided into multiple MAs. Each MA maps a service instance (SI) that belongs to an MD and is identified by a VLAN. An MA can be regarded as a combination of an MD and a VLAN. According to the standards, multiple VLANs can map one SI, and one SI maps one MA.
- Manage maintenance points (MPs). An MA consists of MPs defined on the ports of bridges. An MP is a combination of a bridge port, a VLAN, and a maintenance level. MPs are classified into maintenance association end points (MEPs) and maintenance association intermediate points (MIPs). MEPs initiate and respond to CFM messages; MIPs transparently transmit or respond to CFM messages but do not initiate the messages.

xDSL Service Management

xDSL service management includes the management of the asymmetrical digital subscriber loop 2+ (ADSL2+), ATM global single-pair high-speed digital subscriber line (G.SHDSL), very high speed digital subscriber lines 2 (VDSL2), and G.fast services. The features of these services are as follows:

ADSL Service Management

ADSL is a technology for providing the asymmetric and high-speed private line access service over common twisted pairs. The ADSL supports the asymmetrical transmission in the upstream and downstream directions, which is suitable for user access services and can provide high-speed data transmission channels for users. The ADSL2+ is an extension of the ADSL technology. It supports a maximum transmission rate of 24 Mbit/s and 2.5 Mbit/s in the downstream and upstream respectively and a maximum transmission distance of 6.5 km. You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Perform and cancel a loopback.
- Initialize a port by deactivating and then activating it.
- Reconfigure port attributes.
- Configure port attributes, such as the associated line template, alarm template, extended template, and monitoring thresholds. These attributes are used to activate the ADSL port.
- Query real-time and historical performance statistics.

- Query the information about the MAC addresses learned on the port for problem location.

G.SHDSL Service Management

G.SHDSL is a technology for providing a high-rate symmetrical data service over one or two twisted pairs. The 2-wire, 4-wire, 6-wire, and 8-wire G.SHDSL access services are supported to allow for a transmission distance ranging from 3 km to 6 km. The rate ranges for different types of G.SHDSL lines are: 192 kbit/s to 5696 kbit/s (2-wire), 384 kbit/s to 4608 kbit/s (4-wire), 576 kbit/s to 17088 kbit/s (6-wire), and 768 kbit/s to 22784 kbit/s (8-wire). You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Maintain a port.
- Bind and unbind a port. You can bind multiple ATM G.SHDSL ports. This increases the bandwidth at the physical layer and improves the rate of the ATM G.SHDSL port.
- Configure port attributes, such as the associated line profile and alarm profile. These attributes are used to activate the ATM G.SHDSL port.
- Query real-time performance statistics.
- Query the information about the MAC addresses learned on the port for problem location.

VDSL2 Service Management

VDSL2 is an extension of the VDSL technology. It provides high-speed private line access in the symmetrical or asymmetrical mode over common twisted pairs. VDSL2 supports a high bandwidth with symmetric rates of up to 100 Mbit/s and multiple spectrum template and encapsulation modes. Based on these features, it provides short-distance and high-speed access solutions to the next-generation broadband access scenarios. You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Perform and cancel a loopback.
- Configure port attributes, such as the associated line profile and alarm profile. These attributes are used to activate the VDSL2 port.
- Query real-time and historical performance statistics.
- Query the information about the MAC addresses learned on the port for problem location.
- Configure vectoring, including vector members and vector groups, for VDSL2 ports, support the board level vectoring, system level vectoring, and node level vectoring.

G.fast Service Management

The G.fast access technology implements 1 Gbit/s ultra-broadband access on the basis of existing copper lines, avoiding fiber reconstruction and greatly accelerating the layout of ultra-broadband networks. In addition, G.fast is compatible with VDSL2, allowing smooth upgrades of users on the live network. You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Perform and cancel a loopback.
- Configure port attributes, such as the associated G.fast profile, alarm profile and related TR165 DSL profiles. These attributes are used to activate the G.fast port.

- Query real-time and historical performance statistics.
- Configure vectoring, including vector members and vector groups, for G.fast ports, support the board level vectoring, system level vectoring, and node level vectoring.
- Configure port QoS policy, queue shaping, traffic suppression, anti-DOS attack, ETH OAM, PPPoE session, and mark the important resource.

Ethernet Access Management

Ethernet access management includes the management of ports and aggregation groups. You can perform the following operations on the U2000:

- Configure port attributes.
- Create, delete, query, and modify an aggregation group.
- Activate and deactivate an Ethernet port.
- Collect real-time performance statistics and delete performance statistics.
- Configure the PPPoE, DHCP Option 82, 802.3ah ETH OAM loopback, and port rate limit functions.
- Query the attributes of optical transceivers for Ethernet optical ports.

You can perform the following Y.1731-related operations for ONTs on the U2000:

- Enable or disable Ethernet OAM.
- Add MEPs.
- Set MA location parameters.
- Set MD location parameters.
- Set MAC addresses in the MEP list.

Multicast Service Management

Multicast is a point-to-multipoint (P2MP) communication mode in which the source sends information to a specified subset of objects under a network node. Multicast services are applicable to the streaming media, distance learning, video conferencing, video on demand (VOD), network gaming, data replication, and other P2MP transmission.

Multicast communication uses a class D IP address (224.0.0.0 to 239.255.255.255) as the destination IP address. A source host sends out a packet that uses a class D IP address as the destination. If other hosts in the network are interested in the multicast packet, these hosts can send a request to join the multicast group and receive the packet. Hosts outside of the group cannot receive the packets sent by the source host.

In controllable multicast, network equipment determines whether a user has the rights to watch programs by identifying the join or request packets of the user. Then, the access device controls and forwards the multicast services accordingly.

There are two multicast modes:

- IGMP snooping: IGMP snooping is a multicast control mechanism at the data link layer. It is used to manage and control multicast services.
- IGMP proxy: In a tree topology, the OLT does not set up routes for forwarding multicast packets; the OLT only relays and forwards multicast protocol packets. To multicast users, the OLT is a multicast router that implements the router functions defined in the IGMP protocol. To multicast routers, the OLT is a multicast user.

You can perform the following operations on the U2000 to manage multicast services:

- Manage multicast users.
- Manage multicast VLANs.
- Manage the virtual upstream ports of multicast services.
- Manage multicast subtending ports.

Narrowband Service Management

Narrowband service management includes the management of the media gateway (MG), signaling gateway (SG), POTS ports, and IP ports.

Users can configure the H.248 and SIP protocols at the same time for MG interfaces, signaling gateways, VoIP PSTN ports, or VoIP ISDN PRA ports.

MG Management

In the next generation network (NGN), the media gateway (MG) and the media gateway controller (MGC) are separated. That is, the functions of the user plane are separated from the functions of the control plane. The messages of the user plane interact with each other by using the MG and the messages of the control plane interact with each other by using the MGC. MG management consists of the management of the MG, MGC, digital signal processor (DSP), and ringing mapping. You can perform the following operations on the U2000:

- Manage MGs.
- Manage MGCs.
- Manage ringing mapping.
- Manage DSP channels.
- Manage PPPoE clients.

SG Management

Signaling gateway (SG) management involves the management of signaling gateways and associations. An SG is a part for signaling interaction. An SG is a signaling proxy for receiving and transmitting signaling messages between the No.7 signaling network and the IP network. An SCTP association provides data transmission for the transfer of the protocol data unit of one or more ports.

VoIP PSTN Port Management

The public switched telephone network (PSTN) is a communication network that provides telephone services for public users over analog subscriber lines. It is also called plain old telephone service (POTS).

Voice over IP (VoIP) is a communication mode for delivery of voice and data over Internet Protocol (IP) networks. In the VoIP technology, voice information is transmitted in digital form in discrete packets rather than through the traditional circuit-oriented protocols of PSTN.

The VoIP PSTN service is provided through the VoIP PSTN ports on the voice service card of an ONU. A gateway is established on the ONU between the PSTN network and the IP network.

You can perform the following operations on the U2000:

- Configure and modify port attributes.
- Enable and disable services.

- Perform and cancel a loopback.
- Reset a port.
- Collect real-time performance statistics.

VoIP ISDN BRA Port Management

ISDN basic rate access (BRA) is the basic rate interface (BRI) and user-network interface provided by the ONU. The BRI supports a transmission rate of 44 kbit/s and provides 2 B channels for carrying services and 1 D channel for transmitting the call control signaling and maintaining the management signaling. The rate of B channels is 64 kbit/s and the rate of D channel is 16 kbit/s. In the upstream direction, the ONU transmits the ISDN service to the NGN network in IP networking mode. The ISDN service is called the VoIP ISDN BRA service. You can perform the following operations on the U2000:

- Configure and modify port attributes.
- Enable and disable services.
- Perform and cancel a loopback.
- Activate and deactivate a port.
- Reset a port.
- Query statistics on MG port usage and collect the number of VoIP ISDN BRA ports sorted by port status.
- Configure the alarm threshold of Layer 2 signaling errors.
- Collect real-time performance statistics.

EOC Service Management

Ethernet over coaxial cable (EOC) management includes the service management of coaxial bandwidth access terminals (CBATs) and coaxial bandwidth access terminals (CNUs). There are two types of upstream ports on the CBAT, that is, the radio frequency (RF) and PON ports. Broadband signals over PON are multiplexed by the mixer of the CBAT into a channel of RF signals. Then the RF signals are transmitted to the RF UNI port for receiving cable TV (CATV) and broadband signals. Multiple CNUs can be connected to one UNI port of the CBAT. The Ethernet ports on CNUs are used for user service access.

The service management function of the CBAT is the same as that of MDUs except for that the UNI port of the CBAT is a downstream port for transmitting the EOC service. CNUs are connected to the CBAT using the UNI port. You can perform the following operations on the U2000:

- Modify port attributes.
- Reset a port.
- Query the alarms of an EPON UNI port.
- Query and clear the real-time performance statistics.

You can perform the following operations on the U2000 to manage CNU services:

- Add, delete, and modify a CNU.
- Activate, deactivate, and reset a CNU.
- Query, delete, and confirm an automatically discovered CNU.
- Query the blacklist of CNUs, add a CNU to the blacklist, and delete a CNU from the blacklist.

- Upgrade a CNU.
- Query and clear the real-time performance statistics of a CNU UNI port.
- Configure the UNI port attributes of a CNU.
- Browse the active and historical alarms, and events.
- Configure an E2E EOC service flow.
- Search for and locate CNUs network-wide (by pressing **Ctrl+F**)
- Query the line status of a CNU.
- Query the bit allocation information of a CNU.
- Query the SNR information of a CNU.

Serial Port Access Management

ONUs use serial ports to add and transmit services. The serial port access management is applicable to a common electric utility network wherein electronic terminals collect and transmit required information for intelligent distribution of electric resources and centralized metering. In the upstream direction, an ONU encapsulates the data frames transmitted through the serial port of the data terminal units (DTU) or data terminal equipment (DTE) into TCP packets, identifies serial port IDs with port IDs, and then transmits the TCP packets to the application servers on the common electric utility network over the IP network. In the downstream direction, the TCP packets are transmitted from the application servers to the ONU over the IP network. Then the ONU extracts the original data frames and writes them to the serial port to complete the communication between the application servers and the DTU or DTE. You can perform the following operations on the U2000:

- Query and configure a serial port.
- Query, add, and delete TCP/IP connections.
- Query and clear the packet statistics of TCP/IP connections.

Global Template Management

A global template is a set of attributes. A global template features offline configuration, global effectiveness, and less duplication of data.

You can perform the following operations on the U2000:

- Add, delete, replicate, and modify a template.
- Apply a profile to NEs.

The U2000 supports the following global templates: ETH alarm templates, VLAN service templates, Cable templates, R2 signaling templates, SNMP templates, number change templates, EQAM templates, voice templates, DSL templates, Vector templates, IGMP templates, traffic templates, VLAN templates, optical transceiver alarm templates, service provisioning templates, ACL templates, QoS policy profile, system parameter templates, EOC CBAT line template, and EOC CNU line template.

Sheet-based Predeployment Management

The U2000 provides the sheet-based predeployment solution which enables you to import device data and ONU topology to the U2000 in batches. This solution provides plug-and-play (PnP) capabilities for equipment, implements software-commissioning-free, and requires only one site visit. Therefore, this solution improves deployment efficiency and reduces network

construction cost, and at the same time allows for concurrent offline configuration and on-site construction. Sheet-based predeployment has the following features:

- Offline deployment by importing a predeployed sheet
- Automatic upgrade of NE software
- Automatic issuing of configuration data

Free authentication and software commissioning of FTTM MDUs

FTTM MDUs are free of authentication and software commissioning:

- Authentication-free: FTTM MDUs that bear services of small base stations are free of authentication and can be installed at any sites.
- Software commissioning-free: FTTM MDUs that bear services of small base stations are free of onsite configuration and the U2000 directly manages channels and service channels.
- Replacement and migration of FTTM MDUs: When FTTM MDUs that bear services of small base stations are faulty or migrated, services can be restored automatically.

Authentication- and Commissioning-free Management and Automatic Upgrades and Restoration of FTTS MDUs

FTTS implements authentication- and software commissioning-free MDU power-on, automatic upgrades after deployment, and automatic configuration restoration after replacement. This improves O&M efficiency of field engineers and accelerates FTTS deployment.

- Authentication-free: For PON upstream FTTS MDUs, an automatic ONU confirmation policy is configured on the U2000 to implement MDU power-on without authentication.
- Software commissioning-free: An OLT IP address pool is configured on the U2000, and the management channels are automatically assigned with IP addresses from the pool, which frees onsite configuration for FTTS MDUs. After authentication succeeds, the management channels from FTTS MDUs to the OLT and the service channels are set up directly.
- Automatic upgrade: An upgrade policy is configured on the U2000. After the devices are deployed, automatic multi-hop upgrades are performed to accelerate FTTS deployment.
- Device replacement in the case of faults: Maintenance personnel at the NOC configure a scheduled backup policy and upgrade policy on the U2000. After the faulty devices are replaced and powered on, device replacement tasks are created on the U2000. Configurations are automatically restored after automatic ONU upgrades and backup file loading are completed. Then field engineers can complete all maintenance operations independently, which shortens the on-duty time of field engineers by 50%.

Plug-and-Play Feature Management

- Plug-and-Play Deployment

The plug-and-play (PnP) solution unifies all FTTx scenarios. A uniform configuration GUI is provided for all types of ONUs and uniform operation entrance is supported to fit the deployment and replacement procedures. This solution greatly simplifies operations, streamlines the configuration process, and reduces the O&M cost.

- Plug-and-Play Replacement

When an MDU is faulty, it is essential to locate the fault and recover services quickly. However, it is time consuming to locate and troubleshoot an internal fault in the MDU.

Therefore, it is recommended that you directly replace faulty MDUs and send them to a maintenance center for repair later on.

Solution limitations:

- The versions of the MDUs of the same type must be the same for the entire network.
- The configuration data of the MDUs must be backed up periodically to avoid data loss; the longer the time between backups, the more likely data loss will occur.
- Only one MDU can go offline and one MDU be automatically discovered during automatic replacement.

Solution implementation procedure:

- Use the DC to back up the configuration data.
- Replace MDUs that encounter a severe hardware fault.
- The hardware installation engineer replaces the faulty MDU with a new MDU and furnishes the maintenance engineer with the identification information about the new MDU.
- The maintenance engineer modifies the authentication information about the MDU on the U2000, starts the automatic upgrade of the NE software by using the DC, and loads the configuration file to the MDU.

Results:

- The MDU implements PnP and is replaced quickly.
- The configuration data is restored quickly.

MDU replacement methods:

- Manual replacement based on an MAC address (EPON) or SN (GPON)
- Automatic replacement based on the key or password
- Automatic one-to-one replacement based on the MAC address
- Replacement of different types of MDUs

Remote Software Commissioning for Ethernet-upstream devices

With remote software commissioning for Ethernet-upstream devices, carriers dispatch only hardware engineers to the site in the deployment phase, helping reduce service costs and accelerate device deployment.

Remote software commissioning for Ethernet-upstream devices supports the following functions:

- Predeploying devices in batches
Use Excel to edit parameters for to-be-deployed Ethernet-upstream devices and import the predeployment sheet to the U2000.
- Predeploying a single device
Predeploy an Ethernet-upstream device in the NE Explorer.
- Modifying and deleting a predeployment record
Modify and delete a predeployment record in the NE Explorer.
- Querying predeployment records
Query predeployment records in the NE Explorer.
- Viewing predeployed devices in the Main Topology

Remote Acceptance

To free engineers from having to perform onsite commissioning and reduce O&M costs in FTTx network construction, the deployed ONUs must support remote acceptance. With the FTTx PnP solution, you can perform the following acceptance operations:

- Narrowband emulation acceptance: Verify that the voice links are in the normal state by using the call emulation test.
- PPPoE dialup emulation acceptance: Verify that the links for Internet access are in the normal state.

ONT Automatic Bulk Upgrade

An FTTH network is deployed with a large number of ONTs. When the ONTs need to be upgraded, the following problems may be encountered:

- A user cannot determine the range of ONTs to be upgraded because ONTs were added to the network during service provisioning.
- A user cannot ensure that the ONTs installed in the place of residence are online.

The U2000 provides the automatic offline bulk upgrade solution for ONTs. You can perform the following operations on the U2000:

- Upgrade ONTs in batches by carrier.
- Upgrade ONTs automatically by creating a periodic upgrade task.
- Upgrade offline ONTs automatically when the ONTs go online.

Enhanced ONT O&M

The remote maintenance capability is enhanced on the ONT user side, which helps resolve issues quickly and reduce home visits. The enhanced maintenance measures include:

- Querying Wi-Fi configurations and status
- Querying information about external APs
- Changing the Web login user password
- Querying the MAC address of the Wi-Fi access
- Backing up ONT configuration files and logs

Line Test

The U2000 provides a dedicated system for the line test to shorten the maintenance period of line faults, and facilitate the user operations. The line test diagnoses the subscriber line from the aspects of electrical attributes (such as capacitance, resistance, and voltage), physical characteristics (such as length), and bearer services capabilities (such as upstream rate and downstream rate). The test result provides references for the line service capability predication, troubleshooting, subscription, and line selection. You can perform the following operations on the U2000:

- PSTN and POTS port caller or called emulation test
- Loop-line test
- Circuit test
- Dial monitor test

- Loop test
- Capturing, releasing, and monitoring a test bus
- CO emulation

8.7.3 Intelligent site management

With the large-scale construction of fiber to the curb (FTTC) networks, the number of outdoor sites increases rapidly and carriers are confronted with a lot of O&M challenges. The U2000 provides an intelligent site management solution, which makes sites visible and controllable remotely, supports remote power supply (RPS) management, and achieves monitoring for more and more sites without workforce increased.

- **Visible sites:** The site status, environment, and power are visible remotely, and onsite site survey is not required, which improves troubleshooting and expansion efficiency.
 - Fault detection: During site maintenance or upon fault reporting, maintenance personnel at the NOC query the temperature, humidity, battery status, current alarms, and historical alarms based on the visible information such as intra-site components, space, environment, and power provided on the U2000 and then perform comprehensive monitoring for the site components and environment. This improves the accuracy of remote fault locating and reduces site visits for maintenance.
 - Site component aging principle analysis: Maintenance personnel at the NOC query the battery backup time, aging curve, and site statistics to analyze the site component aging severity and trend, which provides reference for component replacement.
 - Site capacity expansion: When the service volume at a site reaches the upper threshold of site devices, planning engineers can query site remaining space remotely on the U2000 to provide guidance for site capacity expansion, which avoids onsite survey before site capacity expansion.
- **Remote control on electronic locks:** Rights for electronic locks are configurable, door opening and closing events are recorded, and doors can be opened remotely without keys, which enhance site maintainability and reduce the OPEX.
 - Electronic lock authorization: Rights for electronic locks can be configured remotely, set to take effect at the specified time segments, and copied to other sites, which makes right maintenance more secure and convenient.
 - Traceable door opening: After site assets are lost, maintenance personnel at the NOC can view door opening logs on the U2000 to trace the assets.
 - Opening doors remotely without keys: After an emergency occurs at a site, maintenance engineers visit the site immediately. Maintenance personnel at the NOC open the site door remotely on the U2000. Then the maintenance engineers can go to the site without swiping the IC card to make repairs. This shortens the fault rectification period and reduces loss. If the maintenance engineers forget to carry an IC card or the IC card malfunctions, they also can open the doors remotely without keys, improving site maintenance flexibility.
- **RPS management:** It provides a low-cost and fast-feed solution and Web-based management GUIs to match O&M habits.
 - Service provisioning: The power supply service is running properly on both the office and remote module sides.

- Service fault: Major alarms (user-defined) are pushed to mobile phones or emails as needed to locate fault points quickly. Security protection is provided when electric leakage occurs.
- Remote upgrade: Control boards, voltage boost modules, and fan subracks can be remotely upgraded in batches.
- **Enhanced O&M capabilities for intelligent sites:** Sites support pre-deployment, batch CCU configuration, and topological display of remote power supplies, which improves remote site deployment and maintenance capabilities and reduces O&M costs.
 - CCU pre-deployment is supported. After the CCU is installed, the U2000 automatically applies configurations to it, freeing site software commissioning.
 - CCU time can be configured in batches.
 - Site fan management and environment monitoring are supported.
 - The association relationship between the remote power supply CO end, remote end, and remote site can be managed.
 - View the remaining power and health condition of storage batteries.

8.8 D-CCAP Network Feature Management

This topic describes the functions and features of D-CCAP NE management and network management.

The MA5633 is a distributed cable modem terminal system (CMTS) head end device. It complies with data over cable service interface specification (DOCSIS) 2.0, 3.0 or 3.1. Working with a cable modem (CM), the MA5633 provides the optiCable solution. The MA5633 supports high-speed Internet (HSI), Internet Protocol television (IPTV) and other services, satisfying broadcast TV service diversification.

- In the upstream direction, the CM receives the Ethernet packets from a PC or a set top box (STB), modulates the packets onto a CATV network frequency using the DOCSIS technology, and then sends the modulated signals to the MA5633 over the CATV network. The MA5633 demodulates the received signals into Ethernet packets, and sends the packets to the OLT over the PON network.
- In the downstream direction, the MA5633 receives the Ethernet packets from the OLT on a PON port and the CATV signals (including the CATV service flow or CATV+VoD media flow) on an RF port, and modulates and mixes the received packets and signals. Then, the MA5633 transmits the mixed signals to the CM over the CATV network. The CM filters signals at different frequencies using a filter and restores the CATV signals and Ethernet packets.
- **NE management**
 - Amplifier management
 - Add amplifiers by automatically or manually synchronizing amplifier resources. The automatic synchronization is performed in two scenarios: new amplifiers go online or the preset synchronization period is due.
 - Query and remotely configure the following information about single amplifiers: station, transponder, forward path, and return path.
 - Query network-wide amplifier resources.
 - Query the following information about CMCs: device, optical receiver/transmitter, RF, SC-QAM upstream channel, SC-QAM downstream channel, D3.1 OFDMA

upstream channel, D3.1 OFDM downstream channel, GPON NNI and optical module, and CM list.

- Query the basic, running, flap, and online information about a CM.
- Manage radio frequency (RF) ports.
- Set the RF parameter template.
- Manage CMs, including resetting, deleting, querying CPE information, and collecting performance statistics.
- Configure load balance for RF access ports.
- Collect performance statistics on RF ports.
- Query the quality of signals on RF channels.
- Create dynamic voice service through PacketCable.
- IPDR management: You can configure the server profile and system parameter profile, and manage the IPDR session.

The U2000 can manage CMC clusters. With the cascading GE or PON ports, the U2000 manages a CMC device as a remote OLT subrack. Therefore, services related to the Cable are provisioned to an OLT and then to the MA5633.

● EQAM Service Configurations

Edge Quadrature Amplitude Modulation (EQAM) modulates videos of IP networks into QAM signals so that video data can now be carried on HFC networks. The existing CATV coaxial cable resources can be reused and no additional IP access network is required, reducing costs.

The built-in EQAM of a CMC supports Digital Video Broadcasting (DVB) services and Video On Demand (VOD) services.

- DVB service: The services are transmitted to OLTs through the D-CCAP upper-layer IP network. Media data in the IP format is modulated into RF signals on CMCs. DVB is similar to traditional wired broadcasting or television satellite broadcasting. Users have the same experience in watching DVB programs and traditional television programs. DVB standards are a combination of digital broadcasting standards including Digital Video Broadcasting-Satellite (DVB-S), Digital Video Broadcasting-Cable (DVB-C), and digital video broadcasting-terrestrial (DVB-T).

DVB-C video quality monitoring: You can query the input transport streams, output transport streams to monitor the program quality and collect statistics on packets at video stream forwarding points like CMCs, channels in real time. This implements E2E DVB-C video streams monitoring and fast diagnosis of video quality issues.

- Query input transport streams: Query the status information to verify that programs watched by users are sent to CMCs and check statistics on the program information of online transport streams, packet identifiers (PIDs), and EQAM DVB video domain input packets.
- Query output transport streams: Check information related to user programs and transport stream information based on CMCs or channels. Query the PID packet parsing of output transport streams, including type, maximum rate, minimum rate, interference, CC errors, and associated programs. This allows you to determine whether a DVB program is normal and whether the program traffic has packet loss.

- VOD service: Idle downstream channels are set as EQAM channels for transporting video services. Users can view desired TV programs in real time based on the program list provisioned by the digital television system.
Check the VOD mapping information of a CMC to verify that program channels are normal. Check the output statistics of CMC channels to verify that the traffic of program transport streams is normal.
- Configure the location ID of a CMC. The U2000 delivers CMC location ID to STB through the packets in the video stream. Based on the packets, the STB obtains the association relationship connected to the CMC. Then the STB feeds back the association relationship to the STB and CMC network topology in the OSS system. In this manner, users can locate video faults to the faulty CMC.

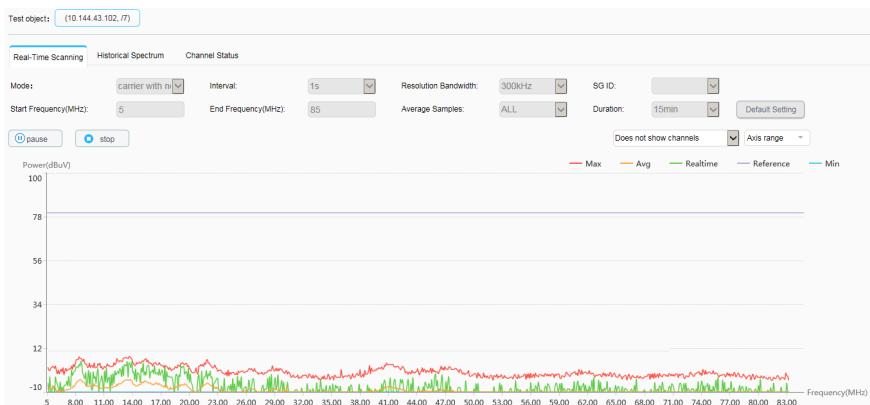
● Cable fault diagnosis

- **CMC link health scoring:** To score CMC network quality based on its running data, allowing you to identify Top N deteriorated CMCs, detect potential faults in advance and help carriers achieve proactive O&M.
 - Network-wide CMCs are scored and ranked automatically every day, showing Top N deteriorated NEs.
 - The hourly network quality of each CMC is displayed, allowing you to pinpoint the time period when multiple CMs under a CMC are faulty.
 - CM KPIs during low-quality period are also displayed, allowing you to identify the branch where faults were introduced. KPIs include upstream and downstream SNR, upstream and downstream PWR, bit error, and flap. In this manner, the fault restoration efficiency is improved by 50%.

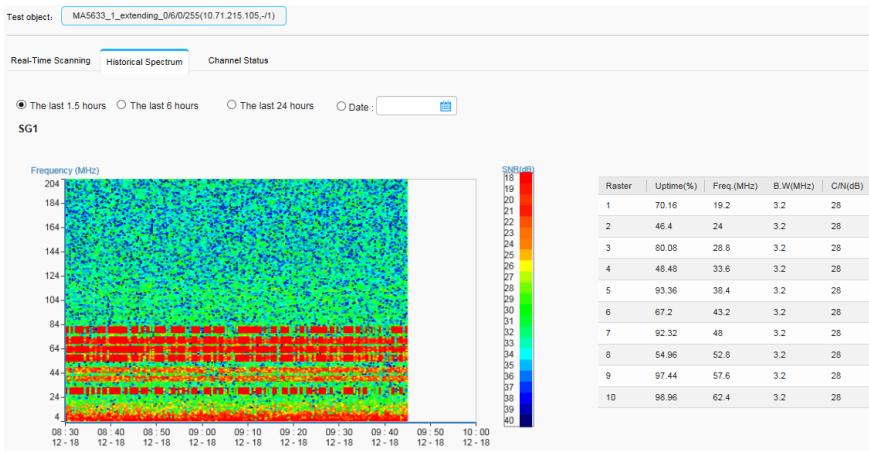
- Spectrum analysis

- Upstream spectrum scanning

Upstream noises interfere with signal transmission over upstream channels and affect cable users' service (including data and voice services) quality. With upstream spectrum scanning, users can know the high-noise frequency bands and configure services at low-noise frequency bands, minimizing noise interference on services.



- Historical spectrum query: You can query the historical spectrum in the last 1.5 hours, 6 hours, 24 hours, or the specified day.



- Query and export of alarms generated by the raster channel: You can query and export alarm data to an .xls or .csv file.
- Setting the reference level, channel, and historical spectrum

- Proactive Network Maintenance using Pre-equalization (PNM-P) Diagnosis

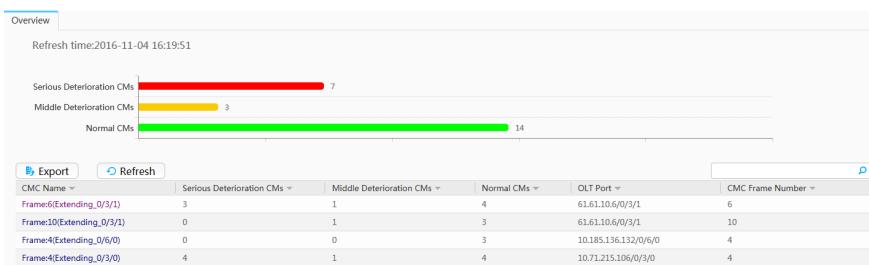
In GPON-upstream D-CCAP aggregation scenarios, PNM-P detects faults on cable networks by analyzing the pre-equalization coefficients between the CMTS and CMs and ascertains line quality through testing, collection, and analysis. It defines a special testing protocol that contributes to accurate grouping and fault location. Based on the results and CM topology from PNM-P, maintenance engineers can detect fault points on networks before user services are affected. Proactively diagnosing and recovering faults helps minimize service impact, improve carriers' service level agreements (SLAs), and reduce network maintenance costs.

Routine cable maintenance and fault reporting by CM users are supported.

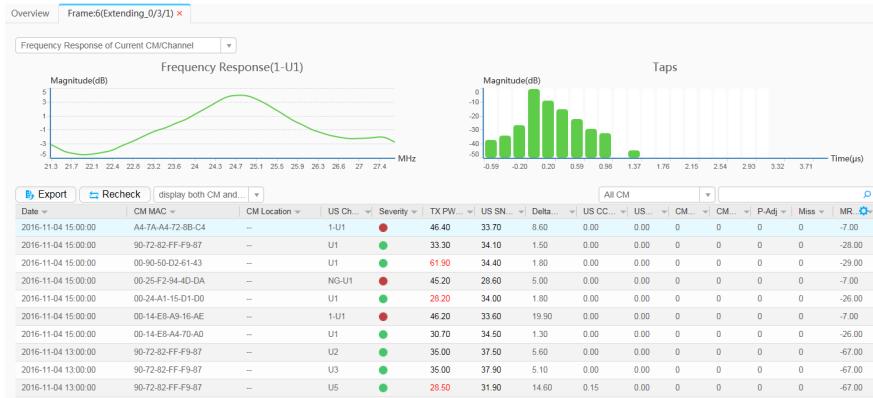
- Routine cable maintenance: Engineers at the network operations center (NOC) regularly check the PNM-P results of network-wide cables. If abnormal CMs are found, cable maintenance engineers will be dispatched for fault recovery onsite.
- Fault reporting by CM users: After a CM user reports a fault, NOC engineers check whether a cable damage report has been generated for the user's CM (MAC address) and whether other CMs are also affected by the damage. Then NOC engineers dispatch cable maintenance engineers to the site for fault recovery. After recovering the fault onsite, cable maintenance engineers will notify the NOC engineers who will then re-conduct PNM-P for the CM.

PNM-P diagnosis results can present the distribution of CMs in different health status on the entire network. Maintenance personnel must pay special attention to serious deterioration CMs and check whether the coaxial lines of the CMs are deterioration.

- Check the distribution of CMs in different health conditions: serious deterioration, mild deterioration, and normal.



- Check the CM groups under a single CMC and CM information, including the CM MAC, CM Location, US Channel&Group, Severity, TX PWR, US SNR, Delta SNR, US CCER, US UCER, CM Re-reg, CM Flap, P-Adj, Miss, MR Level, Delay, TDR, DS SNR, and RX PWR. You can click a CM record to view its frequency response diagram and tap diagram.



- DOCSIS 3.1 diagnosis

- **DOCSIS 3.1 sub-carrier diagnosis:** In network operation and maintenance (O&M), DOCSIS 3.1 sub-carrier parameters, such as bit loading and upstream modulation error ratio (MER), are tested and viewed to analyze the quality of DOCSIS 3.1 channels of the cable modem (CM). Test subcarrier MER to identify hardware defects like notch, cable, and connector defects, and detect hidden RF noise. Identify dynamic templates and configuration problems by viewing Bit distribution.



- **DOCSIS 3.1 PNM diagnosis:** The PNM standard test method is used to improve fault diagnosis precision.

- Fault diagnosis of DOCSIS 3.1 networks is supported. The full coverage of fault information, remote fault analysis, and reduced site-visit time.
- D-CCAP network faults including interface faults, line damage, component faults, and interference source diagnosis are covered.

- The test methods are various, like comprehensive CMC upstream diagnosis, and comprehensive CM upstream diagnosis.
- Comprehensive CMC upstream diagnosis: Perform multiple tests or single test for the upstream channel of a CMC, including tests on the impulsive noise, spectrum scanning, and histogram of CMC channels.
- Comprehensive CM upstream diagnosis: Perform multiple tests or single test for the upstream channel of a CM, including impulsive noise, spectrum scanning, histogram, MER, and FEC tests of CM subcarriers.
- **CM-based diagnosis:** You can diagnose faults based on the running, flap, online, and channel information about CMs.
- **MSO app:** The MSO app communicates with the U2000 through HTTPS and its authentication mode is Certificate+User name and password.
 - CMC adjustment: Upstream and downstream channel parameters can be set in a one-click parameter instead of through the CLI. Engineers do not need to insert or remove the attenuation and equalization brackets, improving the O&M efficiency.
 - Amplifier calibration: The function allows field engineers to measure upstream channel attenuation and slope to accurately configure amplifier gain and equalization. This function is used to commission devices during project deployment and verify the deployment results during project verification. It overtakes the traditional commissioning and acceptance plan that requires dedicated meters, reducing maintenance cost and improving O&M efficiency.
 - CMC configuration binding: The U2000 automatically discovers a CMC after it is installed. One engineer can deploy the CMC by binding the pre-configured CMC parameters with the installed CMC instead of through CLIs.
 - Upstream spectrum scanning: Cable upstream channels are prone to noise interference, which interrupts the proper working of CMs and affects services. During network maintenance, field engineers can scan the upstream spectrum to detect noises, facilitating fault diagnosis.
 - CM diagnosis: The function allows O&M engineers to query the CM status, channel quality, runtime quality, and basic information about CMCs and OLTs, facilitating fault diagnosis.
 - CMC diagnosis: The function can help the maintenance personnel to locate faults. This function is used to check the status of CMC NEs and performance indicators, as well as to query CM statistics, parameter details, frequency of the upstream and downstream channels, channel usage, EQAM channel and link details.
 - DOCSIS 3.1 upstream frequency response: collects statistics and displays frequency response of upstream detection signals of CMCs sent by CMs from D3.1 channels so that maintenance personnel can analyze the attenuation and transmission capabilities of the upstream line between CMs and CMCs.
 - Downstream pilot: The function is used to configure multiple downstream pilot signals to be sent from a CMC channel. A hand-held meter receives the signals and calculates the line frequency response so that maintenance personnel can analyze the attenuation and transmission capabilities of the CMC downstream line.
- **System Management**
 - Log management: The system log records users' operations on the U2000, including login, logout, NE management, fault diagnosis, and alarm management. You can query the system log.

- Authorization (including rights management, password and account policies, and user monitoring): MSO users can be created and authorized as planned to access certain menus for device monitoring and maintenance. The U2000 provides three default operation sets for MSO users: MSO Web administrators' operation set, MSO Web operators' operation set, and MSO app operation set. You can create other operation sets as needed.
- **Alarm management:** You can configure alarms, and browse and handle current and historical alarms.
- **Cable monitoring**
 - **Cable traffic report**

The cable traffic report collects cable traffic on network-wide CMC devices within the specified period of time. This report can be a traffic summary report in the granularity of OLTs or a traffic sub-report in the granularity of CMCs.

 - The cable traffic report in the granularity of OLTs collects historical traffic and inventory relationships of OLTs and CMCs in centralized management mode.
 - The cable traffic report in the granularity of OLTs collects historical traffic of OLTs and CMCs in centralized+standalone management mode.
 - The cable traffic report in the granularity of CMCs collects historical traffic of OLTs and CMCs in centralized management mode.
 - The cable traffic report in the granularity of CMCs collects historical traffic of OLTs and CMCs in centralized+standalone management mode.
 - **EQAM service monitoring**

The U2000 provides the EQAM device management and monitoring GUI that supports list-based and graphical queries for service and program views.

 - Service view: The EQAM device load condition is displayed in a list.
 - Program view: EQAM programs are graphically displayed for the MA5633 or extended subrack. The program view presents brief information about programs carried by each RF port and channel of an EQAM device. You can intuitively view the VoD and device load condition.

8.9 MSAN Network Feature Management

This topic describes the functions and features of MSAN NE management and network management.

NOTE

This section describes only U2000's support to basic NE features. Information displayed on GUIs may be different for features of different types or versions of NEs.

8.9.1 MSAN Management

For NE configuration management, the U2000 provides graphical user interfaces (GUIs) for configuring NEs and maintaining NE configurations. You can configure services for equipment in the GUIs.

NE Management

NE management includes the management of NE panels, basic and common NE attributes, clock sources, security, protocols, global configuration of services, and NE templates.

NE Panel Management

You can perform the following operations on the U2000:

- Display the NE panel by double-clicking an NE.
- Query NE details.
- Collect statistics on NE resources.
- Query the information about shelves.
- Collect the statistics on shelf resources.
- Query inter-shelf links.
- Add, delete, enable, disable, reset, and confirm a card.
- Query real-time performance statistics on the CPU usage and memory of cards.
- Display the port view by double-clicking a card.
- Perform an active/standby switchover on the control cards.
- Configure the working mode of the VDM board.

Management of Basic and Common NE Attributes

The management of basic and common NE attributes includes the query of the global information about NEs and the configuration of the global policies of NEs.

You can perform the following operations on the U2000:

- Query the system information about NEs.
- Query resource and status statistics of NEs.
- Query the license information about the functions and resources of NEs.
- Configure the system time, IP address of an NE, and the binding between a Layer 3 interface and an IP address.
- Configure the SNMP protocol port.
- Set device handshake parameters.
- Configure the policy for automatically backing up NE data.
- Enable and disable the energy-conservation function of an NE.
- Configure and manage license files.

Clock Source Management

Clock source management includes the management and configuration of NE-specific clock source information, such as information about the line clock, 1588 clock, and clock priorities.

Security Management

You can perform the following operations on the U2000:

- Enable and disable anti-ICMP attack, anti-IP attack, anti-IP spoofing, anti-MAC spoofing, and anti-DoS attack.
- Set the aging time of an MAC address.
- Enable and disable MAC address learning.
- Configure the security attributes for user login in the CLI.

Protocol Management

You can perform the following operations on the U2000:

- Manage the Link Aggregation Control Protocol (LACP), Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP), Bidirectional Forwarding Detection (BFD), and Internet Group Management Protocol (IGMP).
- Control the Address Resolution Protocol (ARP) proxy.
- Configure the Policy Information Transfer Protocol (PITP) mode/Relay Agent Info Option (RAIO) custom format.
- Control the Dynamic Host Configuration Protocol (DHCP) Option 82 function.
- Control the DHCP proxy and DHCP relay forwarding functions.
- Configure 802.1ag attributes of the Ethernet packet.

Global Configuration of Services

The global configuration of services includes the configuration of the VLAN, QoS, POTS, xDSL, and multicast services.

NE Template Management

NE template management includes the display of different types of NE templates on the U2000. Templates include voice templates, DSL templates, IGMP templates, traffic templates, number change profile and VLAN templates. Currently, the U2000 supports querying, deleting, and generating global templates, and supports downloading global templates to NE.

Network Interface Management

Network interface management includes the management and maintenance of E1/T1 ports, AG R2 ports, and Ethernet ports.

Management and Maintenance of E1/T1 Ports

E1/T1 ports are classified into TDM E1/T1 ports, CES E1/T1 ports, and IMA E1/T1 ports.

TDM E1/T1 ports can be used as access ports or upstream ports, depending on the functions of the cards.

With E1 ports for upstream transmission, you can perform (enable/disable) the loopback operation.

With E1 ports for PRA access, you can perform the following operations: configure or delete port attributes, set the alarm threshold of L2 signaling bit errors, query timeslots, and enable or disable services.

With CES E1/T1 ports, you can collect real-time performance statistics of ports, configure port attributes, set port alias, and perform loopback.

With IMA E1/T1 ports, you can query real-time performance statistics of the ports, and manage IMA groups and IMA links, including adding, deleting, modifying, resetting, blocking, and unblocking an IMA group or link.

Management of AG R2 Ports

Connecting R2 user terminals to NGNs using AG R2 ports achieves PSTN-to-NGN migration. You can perform the following operations on the U2000: Configure AG R2 users. Configure AG R2 user accounts. Maintain AG R2 ports.

Management of Ethernet Ports

Ethernet port management includes the management of ports and aggregation groups. You can perform the following operations on the U2000:

- Configure port attributes.
- Create, delete, query, and modify an aggregation group.
- Activate and deactivate an Ethernet port.
- Collect real-time performance statistics and delete performance statistics.
- Configure the PPPoE, DHCP Option 82, 802.3ah ETH OAM loopback, and port rate limit functions.
- Query the attributes of optical transceivers for Ethernet optical ports.
- Configure automatic control of optical signal transmission.

Connection Management

PVC

The ATM virtual connection is the logical relationship between the link endpoints in the ATM network. That is, it is the communication path for transmitting ATM cells between two or multiple endpoints. It can be used to transmit information between users, between users and networks, and between networks.

Service Virtual Port Management

A service virtual port enables user equipment to access the OLT. The service virtual port provides service streams between the user equipment and the OLT for carrying user services. You can perform the following operations on the U2000:

- Query, add, delete, modify, activate, and deactivate a service virtual port.
- Collect real-time performance statistics and delete performance statistics.
- Configure the extended attributes of a service virtual port. Extended attributes allow for greater flexibility in addressing customer requirements. Extended attributes include the maximum number of learnable MAC addresses, the PPPoE session, the encapsulation type, and the maximum number of MAC addresses that can be bound.
- Configure the connection attributes of a service virtual port, including the alias, VPI/VCI, transmit traffic profile, and receive traffic profile.
- Change the VLAN ID of a service virtual port. After the VLAN ID is changed, the port will assume the new VLAN ID.
- Bind IP addresses to a service virtual port and query the bound IP addresses. Performing this operation will allow only users with specified IP addresses to access the service virtual port. After successful binding, the service forwarding module will check the source IP address of user packets. If the source IP address does not match any of the IP addresses bound to the service virtual port, the user packets will be dropped. This feature ensures security in user access.
- Bind static MAC addresses to a service virtual port. Performing this operation will allow only users with specified MAC addresses to access the service virtual port. After successful binding, the service forwarding module will check the source MAC address of user packets. If the source MAC address does not match any of the MAC addresses bound to the service virtual port, the user packets will be dropped. This feature ensures security in user access.
- Support the Atm-ping, detects the connectivity of the ATM link to determine whether the line between the device and the modem of the user is reachable.

- Configure service bundles. If several service virtual ports carry the same service, a service bundle can be configured.

SPC

A semi-permanent connection (SPC) can implement the connection, release, check, and protection of one or more 64 k channels of ports on the same or different cards. An SPC occupies the dedicated and fixed voice channel. Therefore, the communication requirements of special and important access users are met and the communication quality is ensured.

SAToP Connection

Structure-Agnostic Transport over Packet (SAToP) is the circuit emulation service simulated on the packet-based network. When data packets are transmitted on a TDM network and a traffic stream is identified by a TDM connection ID, configure a SAToP connection in case of unstructured TDM data.

Layer 2 Management

Layer 2 management includes the management of the VLAN, the Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), Access Node Control Protocol (ANCP), and Rapid Ring Protection Protocol (RRPP).

VLAN Service Management

VLAN service management includes the management of the standard VLAN, MUX VLAN, smart VLAN, and super VLAN. You can perform the following operations on the U2000:

- Query, add, delete, and modify a VLAN.
- Collect real-time performance statistics of a VLAN.
- Clear real-time performance statistics of a VLAN.
- Manage a Layer 3 interface and its subinterfaces.

RSTP Management

You can perform the following operations on the U2000:

- Modify and restore the default value for the trail overheads on a port.
- Collect port RSTP statistics.
- Clear port RSTP statistics.

MSTP Management

MSTP management includes the management of domains, instances, and ports. You can perform the following operations on the U2000:

- Modify and restore the default setting of a domain.
- Add, delete, and modify an instance.
- Modify a port.
- Query port statistics.

ANCP Management

You can perform the following operations on the U2000:

- Add, delete, modify, enable, and disable an ANCP session.
- Query the real-time status of an ANCP session.

RRPP Management

Query, add, delete, and modify RRPP domains.

LLDP Management

Devices' Layer 2 information obtained using the LLDP protocol is helpful for the U2000 to quickly obtain topology status of connected devices, detect configuration conflicts between devices, and find out root causes of network failures. You can configure LLDP protocol attributes and change the working modes for one LLDP port or for multiple LLDP ports at one time.

G.8032 ERPS Management

ERPS is a protocol used to block specified ports to prevent loops at the link layer of an Ethernet network. You can add, modify, configure, delete, and query ERP rings, collect Ethernet port statistics on an ERP ring, and add or delete an Ethernet port to or from an ERP ring.

Layer 3 Management

Layer 3 management includes the management of Dynamic Host Configuration Protocol (DHCP), Multi-protocol Label Switching (MPLS)/pseudo-wire emulation edge-to-edge (PWE3), and Layer 3 routes.

DHCP Management

DHCP management includes the management of DHCP server groups, MAC address segments, standard modes, DHCP domains, and VLAN L3 interfaces. You can perform the following operations on the U2000:

- Query, add, delete, and modify a DHCP server group.
- Query, add, delete, and modify a MAC address segment.
- Query, enable, disable, and modify a standard mode.
- Query, add, delete, and modify a DHCP domain.
- Modify a VLAN Layer 3 interface.

MPLS Management

The Multi-protocol Label Switching (MPLS) network adopts the standard packet switching mode to forward Layer 3 packets and the label switching mode to exchange Layer 2 packets. Virtual private LAN service (VPLS) is a Layer 2 virtual private network (VPN) technology that is based on the MPLS and Ethernet technologies. VPLS is a way to connect multiple Ethernet LANs through packet switched networks (PSNs) for the LANs to work as one LAN. Virtual private wire service (VPWS) is a VPN technology that bears Layer 2 services. VPWS emulates services such as ATM, frame relay, Ethernet, low-speed TDM circuit, and SONET/SDH in a PSN.

You can perform the following configurations for MPLS tunnels on a per-NE basis on the U2000:

- Configure MPLS interface.
- Configure LDP remote peer.
- Configure static LSP.
- Query MPLS LDP session.

The U2000 supports the following VPLS configurations:

- Configure virtual switch instances (VSIs) to map actual attachment circuits (ACs) of the VPLS to each PW.
- Configure ACs to transmit frames between customer edges (CEs) and provider edges (PEs).
- Configure PWs (virtual connections between PEs) to transmit frames between PEs.
- Configure PW protection groups to quickly switch data to the other PW if a PW is faulty.

The U2000 supports the following PW configurations for the VPWS:

- Query, add, delete, modify, and deploy PWs.
- Enable and disable PWs.
- Configure protection groups.
- Configure the committed access rate (CAR).

ACL and QoS Management

ACL and QoS management includes the management of the access control list (ACL), quality of service (QoS), time segments, and hierarchical QoS (HQoS).

In a traditional packet-based network, all packets are treated in the same way. Every router adopts the first-in first-out (FIFO) policy to process packets and makes its best effort to transmit packets to the destination. The router, however, does not make any commitment to packet transmission performance, such as the delay, delay variation (jitter), packet loss rate, and reliability. More and more networks are connecting to the Internet and new services are emerging that raise the requirements on the service capability of IP networks. Therefore, network-wide end-to-end QoS solutions are being considered which will require devices to apply QoS techniques and provide hierarchical QoS assurance for different types of service streams (especially for those highly sensitive to delay and jitter). For ACL management, you can perform the following operations on the U2000:

- Configure one or more time segments, and associate a time segment with an ACL by specifying the name of the time segment in the ACL.
- Query, modify, create, and delete the ACL of the standard, extended, Layer 2, and user-defined types.
- QoS management includes filtering packets based on ACL, tagging priorities, limiting traffic and port rate, collecting statistics on traffic, redirecting, and mirroring. On the U2000, you can query, add, modify, and delete a QoS policy. For the mirroring, the product does not resolve or process the captured data.

HQoS stands for the hierarchical QoS. It not only controls user traffic but also schedules packets according to the priorities of user services. On the U2000, you can query, add, modify, and delete an HQoS policy.

User Security and System Security

You can perform the following operations on the U2000:

- Configure user access in PITP mode.
- Configure user access in DHCP Option 82 mode.
- Configure user access control.
- Configure system secure access.
- Manage BFD sessions.

Ethernet Connectivity Fault Management

As the Ethernet technology extends from carrier networks to metropolitan area networks (MANs) and wide area networks (WANs), carriers are increasingly concerned about the maintainability of equipment, especially Ethernet equipment. This concern has led to a demand for the operation, administration, and maintenance (OAM) of transport equipment. The 802.1ag connectivity fault management (CFM) provides a method for detecting faults end-to-end. The Ethernet OAM mechanisms supported by 802.1ag CFM include continuity check (CC), loopback (LB), link trace (LT), and forward AIS alarms. Y.1731 supports service-based performance measurement, including bidirectional diagnostic test and user-side Ethernet OAM packet filtering. You can perform the following operations on the U2000:

- Manage maintenance domains (MDs). Ethernet CFM divides a network into up to eight levels. A bridge can span multiple levels to manage different MDs. A CFM MD is constituted by bridges. An MD is the combination of bridges and maintenance levels. MDs can be classified into three layers: user domain (levels 7-5), service provider domain (levels 4-3), and carrier domain (levels 2-0). This type of management entity used depends on the type of MD deployed.
- Manage maintenance associations (MAs). An MD can be divided into multiple MAs. Each MA maps a service instance (SI) that belongs to an MD and is identified by a VLAN. An MA can be regarded as a combination of an MD and a VLAN. According to the standards, multiple VLANs can map one SI, and one SI maps one MA.
- Manage maintenance points (MPs). An MA consists of MPs defined on the ports of bridges. An MP is a combination of a bridge port, a VLAN, and a maintenance level. MPs are classified into maintenance association end points (MEPs) and maintenance association intermediate points (MIPs). MEPs initiate and respond to CFM messages; MIPs transparently transmit or respond to CFM messages but do not initiate the messages.

Protection Group Management

Protection group management involves the protection switchover and protection group.

Protection switchover: Important card resources and port resources are generally backed up to enhance system reliability. If a fault occurs on a working member, protection switchover will be triggered to transfer services to the protection member that will continue to handle the services.

Protection group: You can manage the working member and the protection member in the protection group. In a protection group, you can manage the relationship between the members involved in the protection switchover, record the status of members, and manage the configuration data and status of the involved members.

With the protection group feature, you can protect the following objects on the U2000:

- Active and standby control cards
- Aggregation groups on active control cards and standby control cards
- Ports on active and standby control cards
- Upstream Ethernet ports
- Upstream aggregation links of Ethernet ports

xDSL Service Management

xDSL service management includes the management of the asymmetrical digital subscriber loop (ADSL), ADSL2+, ATM global single-pair high-speed digital subscriber line

(G.SHDSL), and very high speed digital subscriber lines 2 (VDSL2) services. The features of these services are as follows:

ADSL Service Management

ADSL is a technology for providing the asymmetric and high-speed private line access service over common twisted pairs. The ADSL supports the asymmetrical transmission in the upstream and downstream directions, which is suitable for user access services and can provide high-speed data transmission channels for users. The ADSL2+ is an extension of the ADSL technology. It supports a maximum transmission rate of 24 Mbit/s and 2.5 Mbit/s in the downstream and upstream respectively and a maximum transmission distance of 6.5 km. You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Perform and cancel a loopback.
- Initialize a port by deactivating and then activating it.
- Reconfigure port attributes.
- Configure the port attributes, such as the associated line template, alarm template, extended template, and monitoring thresholds. These attributes are used to activate the ADSL port.
- Query real-time and historical performance statistics.
- Query learned MAC addresses.

G.SHDSL Service Management

G.SHDSL is a technology for providing a high-rate symmetrical data service over one or two twisted pairs. The 2-wire, 4-wire, 6-wire, and 8-wire G.SHDSL access services are supported to allow for a transmission distance ranging from 3 km to 6 km. The rate ranges for different types of G.SHDSL lines are: 192 kbit/s to 5696 kbit/s (2-wire), 384 kbit/s to 4608 kbit/s (4-wire), 576 kbit/s to 17088 kbit/s (6-wire), and 768 kbit/s to 22784 kbit/s (8-wire). You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Perform and cancel a loopback.
- Bind and unbind a port. You can bind multiple ATM G.SHDSL ports. This increases the bandwidth at the physical layer and improves the rate of the ATM G.SHDSL port.
- Configure port attributes, such as the associated line profile and alarm profile. These attributes are used to activate the ATM G.SHDSL port.
- Query real-time performance statistics.
- Query learned MAC addresses.

G.SHDSL ports support R2 PBX access. You can configure and delete one G.SHDSL R2 user, configure and delete multiple G.SHDSL R2 users at one time, configure G.SHDSL R2 accounts and account authentication, and maintain services for G.SHDSL R2 users.

VDSL2 Service Management

VDSL2 is an extension of the VDSL technology. It provides high-speed private line access in the symmetrical or asymmetrical mode over common twisted pairs. VDSL2 supports a high bandwidth with symmetric rates of up to 100 Mbit/s and multiple spectrum template and encapsulation modes. Based on these features, it provides short-distance and high-speed access solutions to the next-generation broadband access scenarios. You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Perform and cancel a loopback.
- Reconfigure port attributes.
- Configure the port attributes, such as the associated line profile, and alarm profile. These attributes are used to activate the VDSL2 port.
- Query real-time and historical performance statistics.
- Query learned MAC addresses.

Multicast Service Management

Multicast is a point-to-multipoint (P2MP) communication mode in which the source sends information to a specified subset of objects under a network node. Multicast services are applicable to the streaming media, distance learning, video conferencing, video on demand (VOD), network gaming, data replication, and other P2MP transmission.

Multicast communication uses a class D IP address (224.0.0.0 to 239.255.255.255) as the destination IP address. A source host sends out a packet that uses a class D IP address as the destination. If other hosts in the network are interested in the multicast packet, these hosts can send a request to join the multicast group and receive the packet. Hosts outside of the group cannot receive the packets sent by the source host.

In controllable multicast, network equipment determines whether a user has the rights to watch programs by identifying the join or request packets of the user. Then, the access device controls and forwards the multicast services accordingly.

There are two multicast modes:

- IGMP snooping: IGMP snooping is a multicast control mechanism at the data link layer. It is used to manage and control multicast services.
- IGMP proxy: In a tree topology, the OLT does not set up routes for forwarding multicast packets; the OLT only relays and forwards multicast protocol packets. To multicast users, the OLT is a multicast router that implements the router functions defined in the IGMP protocol. To multicast routers, the OLT is a multicast user.

You can perform the following operations on the U2000 to manage multicast services:

- Manage multicast users.
- Manage multicast VLANs.
- Manage the virtual upstream ports of multicast services.
- Manage multicast subtending ports.

MG Management

In the next generation network (NGN), the media gateway (MG) and the media gateway controller (MGC) are separated. That is, the functions of the user plane are separated from the functions of the control plane. The messages of the user plane interact with each other by using the MG and the messages of the control plane interact with each other by using the MGC. An MG device consists of the MG, MGC, digital signal processor (DSP) management, and ringing mapping. You can perform the following operations on the U2000:

- Manage MGs.
- Manage MGCs.
- Manage ringing mapping.

- Manage DSP channels.
- Manage SIP user groups.
- Configure the H.248, MGCP and SIP protocols for MGs.

SIP User Group Management

Any SIP users can be specified and added to a registered user group (SIP user group). After user group registration is enabled, a SIP user group initiates registration and the users in the group do not need to register again. SIP users to be added to a SIP user group can be under different physical ports but they cannot be under different virtual access gateways (VAGs) or devices. You can perform the following operations on the U2000:

- Manage SIP user groups.
- Activate or deactivate SIP user groups.
- Query SIP user groups.

Hunting Group Management: When hunting groups exist on a specified SIP interface, you can configure hunting group members and accounts based on site requirements. In this manner, a group of ports can share one or more accounts. You can perform the following operations on the U2000:

- Add, modify, or delete a hunting group.
- Add, modify, or delete a hunting group member.

Group Account Management: A group account can be specified as an identifier of the calling party when a call is initiated. It applies to the scenario where a user has multiple terminals but uses the same user account for accounting. You can perform the following operations on the U2000:

- Add, modify, or delete a group account.
- Activate or deactivate a group account.
- Authenticate a group account.

CLI Group Management: You can query, add, or delete an outgoing group or an CLI group member.

SG Management

Signaling gateway (SG) management involves the management of signaling gateways and associations. An SG is a part for signaling interaction. An SG is a signaling proxy for receiving and transmitting signaling messages between the No.7 signaling network and the IP network. An SCTP association provides data transmission for the transfer of the protocol data unit of one or more ports.

Narrowband VoIP Service Management

Narrowband VoIP service management involves the management of the MG, SG, POTS ports, and IP ports.

VoIP PSTN Port Management

The public switched telephone network (PSTN) is a communication network that provides telephone services for public users over analog subscriber lines. It is also called plain old telephone service (POTS).

Voice over IP (VoIP) is a communication mode for delivery of voice and data over Internet Protocol (IP) networks. In the VoIP technology, voice information is transmitted in digital form in discrete packets rather than through the traditional circuit-oriented protocols of PSTN.

The VoIP PSTN service is provided through the VoIP PSTN ports on the voice service card of an ONU. A gateway is established on the ONU between the PSTN network and the IP network.

You can perform the following operations on the U2000:

- Configure and modify port attributes.
- Enable and disable services.
- Perform and cancel a loopback.
- Reset a port.
- Configure account and service right.
- Collect real-time performance statistics.
- Configure the H.248 and SIP protocols for MGs.
- Configure VBD for the port.H.248.

VoIP ISDN BRA Port Management

ISDN basic rate access (BRA) is the basic rate interface (BRI) and user-network interface provided by the ONU. The BRI supports a transmission rate of 44 kbit/s and provides 2 B channels for carrying services and 1 D channel for transmitting the call control signaling and maintaining the management signaling. The rate of B channels is 64 kbit/s and the rate of D channel is 16 kbit/s. In the upstream direction, the ONU transmits the ISDN service to the NGN network in IP networking mode. The ISDN service is called the VoIP ISDN BRA service. You can perform the following operations on the U2000:

- Configure and modify port attributes.
- Enable and disable services.
- Perform and cancel a loopback.
- Activate and deactivate a port.
- Reset a port.
- Query statistics on MG port usage and collect the number of VoIP ISDN BRA ports sorted by port status.
- Configure the alarm threshold of Layer 2 signaling errors.
- Configure account and service right.
- Collect real-time performance statistics.
- Configure the H.248 and SIP protocols for MGs.
- Configure VBD for the port.H.248.

VoIP ISDN PRA Port Management

ISDN primary rate access (PRA) is the primary rate interface (PRI) and user-network interface provided by the ONU. The PRI supports a transmission rate of 2.048 Mbit/s and provides 30 B channels and 1 D channel. The rates of the B channel and D channel are 64 kbit/s. In the upstream direction, the ONU transmits the ISDN service to the NGN network in IP networking mode. The ISDN service is called the VoIP ISDN PRA service. You can perform the following operations on the U2000:

- Configure and modify port attributes.

- Enable and disable services.
- Perform and cancel a loopback.
- Query statistics on MG port usage and collect the number of VoIP ISDN PRA ports sorted by port status.
- Configure the alarm threshold of Layer 2 signaling errors.
- Query the timeslots that are occupied by a specified VoIP ISDN PRA port.
- Configure account and service right.
- Configure the H.248 and SIP protocols for MGs.
- Configure VBD for the port.H.248.

V5 Voice Service Management

V5 voice service management includes the management of V5 interfaces, service ports, semi-permanent connections (SPCs), VFB cards, ATI cards, and CDI cards.

V5 Interface Management

The V5 interface is a standard digital interface between the access network (AN) and the local exchange (LE). The V5 interface supports access from a variety of integrated services. In addition, it separates access from services to optimize the network organization. You can perform the following operations on the U2000:

- Manage the attributes of V5 interfaces.
- Restart the PSTN protocol on V5 interface.
- Switch over the logical communication channels of a specified V5 interface for protection.
- Manage 2M links.
- Manage communication channels.
- Manage ISDN communication channels.
- Configure the ringing mode for users.

Service Port Management

Service ports are classified into V5 PSTN ports, V5 ISDN BRA ports, and V5 ISDN PRA ports.

You can perform the following operations to manage V5 PSTN ports on the U2000:

- Configure and modify port attributes.
- Block, delayed block, and unblock a port.
- Perform and cancel a loopback.
- Reset a port.
- Collect real-time performance statistics.

You can perform the following operations to manage V5 ISDN BRA ports on the U2000:

- Configure and modify port attributes.
- Block, delayed block, and unblock a port.
- Perform and cancel a loopback.
- Reset a port.

- Collect real-time performance statistics.

You can perform the following operations to manage V5 ISDN PRA ports on the U2000:

- Configure and modify port attributes.
- Block, delayed block, and unblock a port.

SPC Management

SPC can connect, release, check, and protect one or more 64 kbit/s channels of different ports of the same card or different cards. SPCs occupy dedicated and fixed voice channels to meet the communication requirements of special and VIP access subscribers. You can perform the following operations on the U2000:

- Set up common SPCs between narrowband service ports.
- Set up VoIP-based IP SPCs.
- Set up internal SPCs.
- Configure private lines.
- Set up V5 SPCs.
- Set up V5 pre-SPCs.

VFB Card Management

The UA5000(PVMV1) provides point-to-point voice frequency (VF) channels to transmit voice or data in dedicated networks. You can connect VF telephones or modems (connecting user terminals) to the VF channels at the two sides so that the voice or data is interconnected over dedicated lines. The VFB card of the UA5000(PVMV1) is a 2/4-wire VF dedicated line interface card and supports VF dedicated line services. The VFB card can adjust the 2/4-wire port with the software. It provides sixteen 2-wire port or eight 4-wire ports. You can perform the following operations on the U2000:

- Configure the attributes of ports provided by the VFB card.
- Add SPCs.

Certain types of dedicated networks access LEs or interwork with remote dedicated networks over the access network. In dedicated networks, many users adopt the E&M trunk ports. To access these users over the access network, ONUs must provide the E&M trunk ports.

ATI Card Management

The ATI card, when inserted in a service shelf, transparently transmits E/M signaling and 2-wire/4-wire VF signals by using SPCs. This helps the HONET system access certain dedicated networks. The ATI card provides six 2-wire/4-wire E&M trunk ports. Each port provides the 2-wire/4-wire VF line and the 1E1M signaling line. If the 1E1M signaling line is not in use, the 2-wire/4-wire VF line can be used independently to transmit VF signals. You can perform the following operations on the U2000:

- Configure the 2-wire/4-wire VF and E&M trunk service.
- Configure the hotline service of E&M trunk ports.

CDI Card Management

The CDI card is a 16-channel direct-dialing-in subscriber interface card of the HONET access system, which transparently transmits through analog subscriber ports. The CDI card implements the transparent extension inside the HONET system for the analog subscriber ports of external exchanges by means of digital-to-analog conversion between CDI ports and ASL ports, transparent transmission, and signal processing of hosts. In addition, as a foreign

exchange office (FXO) port, the CDI port works with the foreign exchange subscriber (FXS) port provided by the ASL card to allow for POTS users' analog access to the LE. You can perform the following operations on the U2000:

- Configure the Z interface extension service.
- Configure the PBX bidirectional service.
- Configure the DDI service.

Narrowband Data Service Management

Narrowband data service management includes the management of multifunctional terminal adapters (MTAs), HSL cards, and TDM G.SHDSL ports.

MTA Management

The MTA of the UA5000(PVMV1) provides the synchronous port with the rate of 64/128 kbit/s and the synchronous or asynchronous port with the sub-rate of 2.4/4.8/9.6/19.2 kbit/s. The MTA also provides physical communication channels between terminal users and the DDN network or other digital terminal users. You can perform the following operations on the U2000:

- Configure the attributes of MTA ports.
- Add SPCs.

HSL Management

The HSL card of the UA5000 (PVMV1) provides two V.35 ports and two FE1 ports to access N x 64k (n ranges from 1 to 31) data services. You can perform the following operations on the U2000:

- Configure the attributes of V.35 ports provided by the HSL card.
- Add SPCs.

TDM G.SHDSL ports

The UA5000(PVMV1) uses the SDL card to carry G.SHDSL services. The SDL card accesses the G.SHDSL service of data dedicated line subscribers in TDM mode. You can perform the following operations on the U2000:

- Configure TDM G.SHDSL services.
- Manage TDM G.SHDSL terminals.
- Configure subtend services of the TDM G.SHDSL port.

Global Template Management

A global template is a set of attributes that features offline configuration, global effectiveness, and less duplication of data. You can perform the following operations on the U2000:

- Add, delete, copy, and modify a global template.
- Apply a global template to NEs.

The U2000 supports global templates such as voice templates, DSL templates, IGMP templates, traffic templates, VLAN templates, ACL templates, digitmap group templates, and system parameter templates.

8.10 DSLAM Network Feature Management

This topic describes the functions and features of DSLAM NE management and network management.

 **NOTE**

This section describes only U2000's support to basic NE features. Information displayed on GUIs may be different for features of different types or versions of NEs.

8.10.1 DSLAM Management

For NE configuration management, the U2000 provides graphical user interfaces (GUIs) for configuring NEs and maintaining NE configurations. You can configure services for equipment in the GUIs.

NE Management

NE management includes the management of NE panels, basic and common NE attributes, clock sources, security, protocols, global configuration of services, and NE templates.

NE Panel Management

You can perform the following operations on the U2000:

- Display the NE panel by double-clicking an NE.
- Query NE details.
- Collect statistics on NE resources.
- Query the information about shelves.
- Collect the statistics on shelf resources.
- Query inter-shelf links.
- Add, delete, enable, disable, reset, and confirm a card.
- Query real-time performance statistics on the CPU usage and memory of cards.
- Display the port view by double-clicking a card.
- Perform an active/standby switchover on the control cards.

Management of Basic and Common NE Attributes

The management of basic and common NE attributes includes querying the global information about NEs and configuring global policies for NEs.

You can perform the following operations on the U2000:

- Query the system information about NEs.
- Query resource and status statistics of NEs.
- Query the license information about the functions and resources of NEs.
- Configure the system time, IP address of an NE, and the binding between a Layer 3 interface and an IP address.
- Configure the SNMP protocol port.
- Set device handshake parameters.
- Configure the policy for automatically backing up NE data.

- Enable and disable the energy-saving function of an NE.
- Configure and manage license files.

Clock Source Management

Clock source management includes the management and configuration of NE-specific clock source information, such as information about the line clock, 1588 clock, and clock priorities.

Security Management

You can perform the following operations on the U2000:

- Enable and disable anti-ICMP attack, anti-IP attack, anti-IP spoofing, anti-MAC spoofing, and anti-DoS attack.
- Set the aging time of an MAC address.
- Enable and disable MAC address learning.
- Configure the security attributes for user login in the CLI.

Protocol Management

You can perform the following operations on the U2000:

- Manage the Link Aggregation Control Protocol (LACP), Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP), Bidirectional Forwarding Detection (BFD), and Internet Group Management Protocol (IGMP).
- Control the Address Resolution Protocol (ARP) proxy.
- Configure the Policy Information Transfer Protocol (PITP) mode/Relay Agent Info Option (RAIO) custom format.
- Control the Dynamic Host Configuration Protocol (DHCP) Option 82 function.
- Control the DHCP proxy and DHCP relay forwarding functions.
- Configure 802.1ag attributes of the Ethernet packet.

Global Configuration of Services

The global configuration of services includes the configuration of the VLAN, QoS, xDSL, and multicast services.

NE Template Management

NE template management includes the display of different types of NE templates on the U2000. Templates include IGMP templates, traffic templates, xDSL templates, Vector templates, and VLAN templates. Currently, the U2000 supports querying, deleting, and generating global templates, and supports downloading global templates to NE.

Network Interface Management

Network interface management includes the management and maintenance of E1/T1 ports and Ethernet ports.

Management and Maintenance of E1/T1 Ports

E1/T1 ports are classified into TDM E1/T1 ports, CES E1/T1 ports, and IMA E1/T1 ports.

TDM E1/T1 ports can be used as access ports or upstream ports, depending on the functions of the cards.

With E1 ports for upstream transmission, you can perform (enable/disable) the loopback operation.

With E1 ports for PRA access, you can perform the following operations: configure or delete port attributes, query timeslots, and enable or disable services.

With CES E1/T1 ports, you can collect real-time performance statistics of ports, configure port attributes, set port alias, and perform loopback.

With IMA E1/T1 ports, you can query real-time performance statistics of the ports, and manage IMA groups and IMA links, including adding, deleting, modifying, resetting, blocking, and unblocking an IMA group or link.

Management of Ethernet Ports

Ethernet port management includes the management of ports and aggregation groups. You can perform the following operations on the U2000:

- Configure port attributes.
- Create, delete, query, and modify an aggregation group.
- Activate and deactivate an Ethernet port.
- Collect real-time performance statistics and delete performance statistics.
- Configure the PPPoE, DHCP Option 82, 802.3ah ETH OAM loopback, and port rate limit functions.
- Query the attributes of optical transceivers for Ethernet optical ports.
- Configure automatic control of optical signal transmission.

Connection Management

PVC

The ATM virtual connection is the logical relationship between the link endpoints in the ATM network. That is, it is the communication path for transmitting ATM cells between two or multiple endpoints. It can be used to transmit information between users, between users and networks, and between networks.

Service Virtual Port Management

A service virtual port enables user equipment to access the ONU. The service virtual port provides service streams between the user equipment and the ONU for carrying user services. You can perform the following operations on the U2000:

- Query, add, delete, modify, activate, and deactivate a service virtual port.
- Collect real-time performance statistics and delete performance statistics.
- Perform ATM ping tests.
- Configure the extended attributes of a service virtual port. Extended attributes allow for greater flexibility in addressing customer requirements. Extended attributes include the maximum number of learnable MAC addresses, the PPPoE session, the encapsulation type, and the maximum number of MAC addresses that can be bound.
- Configure the connection attributes of a service virtual port, including the alias, VPI/VCI, transmit traffic profile, and receive traffic profile.
- Change the VLAN ID of a service virtual port. After the VLAN ID is changed, the port will assume the new VLAN ID.

- Bind IP addresses to a service virtual port and query the bound IP addresses. Performing this operation will allow only users with specified IP addresses to access the service virtual port. After successful binding, the service forwarding module will check the source IP address of user packets. If the source IP address does not match any of the IP addresses bound to the service virtual port, the user packets will be dropped. Otherwise, the user packets are forwarded. This ensures the security of user access.
- Bind static MAC addresses to a service virtual port. Performing this operation will allow only users with specified MAC addresses to access the service virtual port. After successful binding, the service forwarding module will check the source MAC address of user packets. If the source MAC address does not match any of the MAC addresses bound to the service virtual port, the user packets will be dropped. This feature ensures security in user access.
- Support the Atm-ping, detects the connectivity of the ATM link to determine whether the line between the device and the modem of the user is reachable.
- Configure service bundles. If several service virtual ports carry the same service, a service bundle can be configured.

Layer 2 Management

Layer 2 management includes the management of the VLAN, the Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), Access Node Control Protocol (ANCP), and Rapid Ring Protection Protocol (RRPP).

VLAN Service Management

VLAN service management includes the management of the standard VLAN, MUX VLAN, smart VLAN, and super VLAN. You can perform the following operations on the U2000:

- Query, add, delete, and modify a VLAN.
- Collect real-time performance statistics of a VLAN.
- Clear real-time performance statistics of a VLAN.
- Manage a Layer 3 interface and its subinterfaces.

RSTP Management

You can perform the following operations on the U2000:

- Modify and restore the default value for the trail overheads on a port.
- Collect port RSTP statistics.
- Clear port RSTP statistics.

MSTP Management

MSTP management includes the management of domains, instances, and ports. You can perform the following operations on the U2000:

- Modify and restore the default setting of a domain.
- Add and modify an instance.
- Modify a port.
- Query port statistics.

Layer 3 Management

Layer 3 management includes the management of Dynamic Host Configuration Protocol (DHCP).

DHCP Management

DHCP management includes the management of DHCP server groups, MAC address segments, standard modes, DHCP domains, and VLAN L3 interfaces. You can perform the following operations on the U2000:

- Query, add, delete, and modify a DHCP server group.
- Query, add, delete, and modify a MAC address segment.
- Query and modify a standard mode.
- Query, add, delete, and modify a DHCP domain.
- Modify a VLAN Layer 3 interface.

ACL and QoS Management

ACL and QoS management includes the management of the access control list (ACL), quality of service (QoS), time segments, and hierarchical QoS (HQoS).

In a traditional packet-based network, all packets are treated in the same way. Every router adopts the first-in first-out (FIFO) policy to process packets and makes its best effort to transmit packets to the destination. The router, however, does not make any commitment to packet transmission performance, such as the delay, delay variation (jitter), packet loss rate, and reliability. More and more networks are connecting to the Internet and new services are emerging that raise the requirements on the service capability of IP networks. Therefore, network-wide end-to-end QoS solutions are being considered which will require devices to apply QoS techniques and provide hierarchical QoS assurance for different types of service streams (especially for those highly sensitive to delay and jitter). For ACL management, you can perform the following operations on the U2000:

- Configure one or more time segments, and associate a time segment with an ACL by specifying the name of the time segment in the ACL.
- Query, modify, create, and delete the ACL of the standard, extended, Layer 2, and user-defined types.
- Manage QoS, including filtering packets based on ACL, tagging priorities, limiting traffic and port rate, collecting statistics on traffic, redirecting, and mirroring. On the U2000, you can query, add, and delete a QoS policy. For the mirroring, the product does not resolve or process the captured data.

User Security and System Security

You can perform the following operations on the U2000:

- Configure user access in PITP mode.
- Configure user access in DHCP Option 82 mode.
- Configure user access control.
- Configure system secure access.

BFD Management

The BFD mechanism is used for quickly checking the link status between two devices.

To mitigate the impact of device faults on services and to improve the network availability, a network device needs to quickly detect all faults occurring between the device and its adjacent devices and then take appropriate action to ensure service continuity. The BFD enables the device to check the connectivity for a type of data protocol on the same trail between two systems. The trail can be a physical or a logical link, including a tunnel. The BFD mechanism remedies weaknesses in the existing detection mechanisms.

Ethernet Connectivity Fault Management

As the Ethernet technology extends from carrier networks to metropolitan area networks (MANs) and wide area networks (WANs), carriers are increasingly concerned about the maintainability of equipment, especially Ethernet equipment. This concern has led to a demand for the operation, administration, and maintenance (OAM) of transport equipment. The 802.1ag connectivity fault management (CFM) provides a method for detecting faults end-to-end. The Ethernet OAM mechanisms supported by 802.1ag CFM include continuity check (CC), loopback (LB), link trace (LT), and forward AIS alarms. Y.1731 supports service-based performance measurement, including bidirectional test diagnosis and user-side ETH OAM packet filtering. You can perform the following operations on the U2000:

- Manage maintenance domains (MDs). Ethernet CFM divides a network into up to eight levels. A bridge can span multiple levels to manage different MDs. A CFM MD is constituted by bridges. An MD is the combination of bridges and maintenance levels. MDs can be classified into three layers: user domain (levels 7-5), service provider domain (levels 4-3), and carrier domain (levels 2-0). This type of management entity used depends on the type of MD deployed.
- Manage maintenance associations (MAs). An MD can be divided into multiple MAs. Each MA maps a service instance (SI) that belongs to an MD and is identified by a VLAN. An MA can be regarded as a combination of an MD and a VLAN. According to the standards, multiple VLANs can map one SI, and one SI maps one MA.
- Manage maintenance points (MPs). An MA consists of MPs defined on the ports of bridges. An MP is a combination of a bridge port, a VLAN, and a maintenance level. MPs are classified into maintenance association end points (MEPs) and maintenance association intermediate points (MIPs). MEPs initiate and respond to CFM messages; MIPs transparently transmit or respond to CFM messages but do not initiate the messages.

Protection Group Management

Protection group management involves the protection switchover and protection group.

Protection switchover: Important card resources and port resources are generally backed up to enhance system reliability. If a fault occurs on a working member, protection switchover will be triggered to transfer services to the protection member that will continue to handle the services.

Protection group: You can manage the working member and the protection member in the protection group. In a protection group, you can manage the relationship between the members involved in the protection switchover, record the status of members, and manage the configuration data and status of the involved members.

With the protection group feature, you can protect the following objects on the U2000:

- Active and standby control cards
- Aggregation groups on active control cards and standby control cards

- Ports on active and standby control cards
- Upstream Ethernet ports
- Upstream aggregation links of Ethernet ports

xDSL Service Management

xDSL service management includes the management of the asymmetrical digital subscriber loop (ADSL), ADSL2+, ATM global single-pair high-speed digital subscriber line (G.SHDSL), and very high speed digital subscriber lines 2 (VDSL2) services. The features of these services are as follows:

ADSL Service Management

ADSL is a technology for providing the asymmetric and high-speed private line access service over common twisted pairs. The ADSL supports the asymmetrical transmission in the upstream and downstream directions, which is suitable for user access services and can provide high-speed data transmission channels for users. The ADSL2+ is an extension of the ADSL technology. It supports a maximum transmission rate of 24 Mbit/s and 2.5 Mbit/s in the downstream and upstream respectively and a maximum transmission distance of 6.5 km. You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Perform and cancel a loopback.
- Initialize a port by deactivating and then activating it.
- Reconfigure port attributes.
- Configure port attributes, such as the associated line template, alarm template, extended template, and monitoring thresholds. These attributes are used to activate the ADSL port.
- Query real-time and historical performance statistics.
- Query the information about the MAC addresses learned on the port for problem location.

G.SHDSL Service Management

G.SHDSL is a technology for providing a high-rate symmetrical data service over one or two twisted pairs. The 2-wire, 4-wire, 6-wire, and 8-wire G.SHDSL access services are supported to allow for a transmission distance ranging from 3 km to 6 km. The rate ranges for different types of G.SHDSL lines are: 192 kbit/s to 5696 kbit/s (2-wire), 384 kbit/s to 4608 kbit/s (4-wire), 576 kbit/s to 17088 kbit/s (6-wire), and 768 kbit/s to 22784 kbit/s (8-wire). You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Perform and cancel a loopback.
- Bind and unbind a port. You can bind multiple ATM G.SHDSL ports. This increases the bandwidth at the physical layer and improves the rate of the ATM G.SHDSL port.
- Configure port attributes, such as the associated line profile and alarm profile. These attributes are used to activate the ATM G.SHDSL port.
- Query real-time performance statistics.
- Query the information about the MAC addresses learned on the port for problem location.
- Manage SHDSL repeaters.

G.SHDSL ports support R2 PBX access. You can configure and delete one G.SHDSL R2 user, configure and delete multiple G.SHDSL R2 users at one time, configure G.SHDSL R2 accounts and account authentication, and maintain services for G.SHDSL R2 users.

VDSL2 Service Management

VDSL2 is an extension of the VDSL technology. It provides high-speed private line access in the symmetrical or asymmetrical mode over common twisted pairs. VDSL2 supports a high bandwidth with symmetric rates of up to 100 Mbit/s and multiple spectrum template and encapsulation modes. Based on these features, it provides short-distance and high-speed access solutions to the next-generation broadband access scenarios. You can perform the following operations on the U2000:

- Activate and deactivate a port.
- Perform and cancel a loopback.
- Reconfigure port attributes.
- Configure the port attributes, such as the associated line profile, and alarm profile. These attributes are used to activate the VDSL2 port.
- Query real-time and historical performance statistics.
- Query the information about the MAC addresses learned on the port for problem location.
- Configure vectoring, including vector members and vector groups, for VDSL2 ports, support the system level vectoring, and node level vectoring.

Multicast Service Management

Multicast is a point-to-multipoint (P2MP) communication mode in which the source sends information to a specified subset of objects under a network node. Multicast services are applicable to the streaming media, distance learning, video conferencing, video on demand (VOD), network gaming, data replication, and other P2MP transmission.

Multicast communication uses a class D IP address (224.0.0.0 to 239.255.255.255) as the destination IP address. A source host sends out a packet that uses a class D IP address as the destination. If other hosts in the network are interested in the multicast packet, these hosts can send a request to join the multicast group and receive the packet. Hosts outside of the group cannot receive the packets sent by the source host.

In controllable multicast, network equipment determines whether a user has the rights to watch programs by identifying the join or request packets of the user. Then, the access device controls and forwards the multicast services accordingly.

There are two multicast modes:

- IGMP snooping: IGMP snooping is a multicast control mechanism at the data link layer. It is used to manage and control multicast services.
- IGMP proxy: In a tree topology, the OLT does not set up routes for forwarding multicast packets; the OLT only relays and forwards multicast protocol packets. To multicast users, the OLT is a multicast router that implements the router functions defined in the IGMP protocol. To multicast routers, the OLT is a multicast user.

You can perform the following operations on the U2000 to manage multicast services:

- Manage multicast users.
- Manage multicast VLANs.

- Manage the virtual upstream ports of multicast services.
- Manage multicast subtending ports.

Global Template Management

A global template is a set of attributes that features offline configuration, global effectiveness, and less duplication of data. You can perform the following operations on the U2000:

- Add, delete, copy, and modify a global template.
- Apply a global template to NEs.

The U2000 supports global templates such as DSL templates, Vector templates, IGMP templates, traffic templates, VLAN templates, ACL templates, and system parameter templates.

8.11 BITS/RPS/EDFA Network Feature Management

This topic describes the functions and features of building integrated timing supply (BITS) / remote power system (RPS) / erbium-doped optical fiber amplifier (EDFA) NE management and network management.

8.11.1 BITS NE Management

The U2000 supports the functions of managing building integrated timing supply (BITS) NEs. The functions include NE management, inventory management, performance management, security management, and link management. In addition, the U2000 provides Web LCT-based NE Explorer for BITS NEs, which eases BITS NE configuration.

NE Management

NE management functions are as follows:

- BITS NE management: You can add BITS NEs in online mode or pre-deployment mode on the U2000. In addition, you can query, modify, and delete BITS NEs, synchronize the data of BITS NEs, and refresh the status of BITS NEs.
- BITS subsystem management: You can deploy the BITS subsystem by using an installation CD-ROM. You can also deploy the BITS subsystem with other subsystems such as the router subsystem and SDH subsystem.
- Web LCT-based NE Explorer: You can open the Web LCT-based NE Explorer to configure BITS NEs easily.

Inventory Management

Inventory management refers to physical inventory management of BITS NEs. It provides the following functions:

- Querying the BITS NE list, BITS card list, and BITS port list
- Collecting port statistics of BITS NEs

Performance Management

The U2000 supports the following performance parameters to implement performance management:

- Time interval error (TIE) indicates the variation in time delay of a given clock signal with respect to an ideal clock signal over a particular period (τ). You can query the required TIE performance data by time range or channel.
- Maximum time interval error (MTIE) indicates the maximum TIE within an observation time (τ) for all observation times of that length within the measurement period (T). MTIE is a statistical value and represents the maximum TIE between signals in each τ seconds, that is, maximum phase variation over the measurement period (T). MTIE is an indicator of clock signal stability. You can query MTIE by time.
- Time deviation (TDEV) is the square root of time variance. TDEV is considered the average phase variation in an observation time (τ) and it represents the stability of random phase and time. TDEV is measured in seconds. You can query TDEV in the measurement period (T).
- Frequency deviation (FREQ) indicates the maximum frequency deviation of the signals within an observation time (τ) for all observation times of that length within the measurement period (T). You can query FREQ by specifying search criteria.
- Time offset (TOFF) is the offset between the time of test signals and the universal time coordinated (UTC).

Security Management

Security management is important because it prevents unauthorized access to networks and safeguards network data by providing the following functions:

- Operation authentication: The U2000 authenticates the operations that users perform on BITS NEs, such as adding, modifying, and deleting BITS NEs.
- NE log management: The U2000 records the operations on BITS NEs, such as adding, modifying, and deleting BITS NEs. The U2000 also synchronizes the operation logs of the current NMS user from BITS NEs.

Alarm Management

- SNMP NBI for alarm management: Proactively reports alarms, synchronizes alarms (queries current alarms), clears alarms, acknowledges or unacknowledges alarms, and reports alarm acknowledgment status and clearance status.
- CORBA NBI for alarm management: Reports alarm and update events, queries alarms, and sets alarms.

Coaxial Cable Link Management

You can create or delete coaxial cable links between NEs.

8.11.2 RPS NE Management

The U2000 supports the functions of managing remote power system (RPS) NEs. The functions include NE management, alarm management, and security management. In addition, the U2000 provides Web LCT-based NE Explorer for RPS NEs, which eases RPS NE configuration.

Application Scenarios

RPS devices are introduced to FTTC networks as a low-cost and fast-feed solution. On the equipment room side, RPS devices step up voltage from -48 V to above 200 V DC for transport over twisted pairs. On the device side, RPS devices step down voltage to -48 V.

NE Management

To facilitate configuration and management on a per-NE basis, the U2000 provides the simple and easy-to-use Web configuration UI for RPS NEs and is able to visit their Web proxy server. NE management functions are as follows:

- RPS NE management: You can add or enable automatic discovery of RPS NEs. In addition, you can search for RPS NEs by pressing **Ctrl+F**, modify or delete RPS NEs, synchronize the data of RPS NEs, and refresh the status of RPS NEs.
- RPS independent management: RPS NE management is deployed as an independent component in the access domain during U2000 installation.
- License management: RPS resource licenses are supported.
- Web LCT-based NE Explorer: You can open the Web LCT-based NE Explorer to configure RPS NEs easily.

Alarm Management

- The U2000 allows users to browse, mask, clear, synchronize, and redefine alarms, perform alarm correlation analysis, and locate alarms to topologies.
- SNMP NBI for alarm management: Proactively reports alarms, synchronizes alarms (queries current alarms), clears alarms, acknowledges or unacknowledges alarms, and reports alarm acknowledgment status and clearance status.

Security Management

Security management is important because it prevents unauthorized access to networks and safeguards network data by providing the following functions:

- Operation authentication: The U2000 authenticates the operations that users perform on RPS NEs, such as adding, modifying, and deleting RPS NEs.
- NE log management: The U2000 records the operations on RPS NEs, such as adding, modifying, and deleting RPS NEs. The U2000 also synchronizes the operation logs of the current NMS user from RPS NEs.

8.11.3 EDFA NE Management

The U2000 supports the functions of managing erbium-doped optical fiber amplifier (EDFA) NEs. The functions include NE management, alarm management, and security management.

Application Scenarios

The EDFA is designed for multiple system operators (MSOs). It is an amplifying and multiplexing product that supports both the cable TV (CATV) and broadband services. Specifically, it amplifies a channel of CATV signals, divides the signals into 32 channels, multiplexes the 32 channels of CATV signals with 32 channels of PON signals, and transmits the multiplexed signals over the optical distribution network (ODN) to users' home. The EDFA is applicable in the CATV + PON fiber to the building (FTTB) and fiber to the home

(FTTH) scenarios. The U2000 manages EDFA and PON NEs uniformly, realizing flexible access of voice, IPTV, and private line services.

NE Management

NE management functions are as follows:

- EDFA NE management: EDFA NE management allows users to add EDFA NEs, query the SN, hardware version, delivery date, IP address, and MAC address of an EDFA NE, and configure the optical line protection (OLP) work mode, optical power alarm threshold, EDFA output power, and power alarm threshold.
- License management: EDFA resource licenses are supported.

Alarm Management

- The U2000 allows users to browse, mask, clear, synchronize, and redefine alarms, perform alarm correlation analysis, and locate alarms to topologies.
- SNMP NBI for alarm management: Proactively reports alarms, synchronizes alarms (queries current alarms), clears alarms, acknowledges or unacknowledges alarms, and reports alarm acknowledgment status and clearance status.

Security Management

Security management is important because it prevents unauthorized access to networks and safeguards network data. The U2000 provides users with rights to EDFA operation sets for maintenance, operation, and monitoring. By authenticating the EDFA NE management function, operations like configuring, deleting, and restarting an EDFA NE, and synchronizing the NE time are authenticated.

8.12 Third-Party NE Management

The U2000 in the transport and access domains do not support third-party NE management. Only the U2000 in the IP domain supports third-party router management.

The U2000 supports third-party router management, including topology, resource, alarm, performance, and inventory (report) management. The U2000 is also capable of managing third-party router by obtaining equipment information directly using SNMP and ICMP protocols. Third-party equipment management includes:

Table 8-5 U2000 supports third-party router management

Feature	Function	Details
Topology management	Creates an NE.	Third-party NEs can be added to the U2000 and then displayed in the topology view.
	Creates a link.	U2000 supports manually creating links and automatically discovering IP links for third-party NEs. NOTE Automatically discovering LLDP links between third-party NEs is not supported.

Feature	Function	Details
Device management	System information	Supported
	Interface information	Supported (NEs must support RFC1213)
	Inventory	Managing NE inventory information is supported.
Performance management	routine performance statistics collection for interfaces	Supported (NEs must support RFC1213)
	real-time performance statistics collection for interfaces	Supported (NEs must support RFC1213)
Alarm management	manage alarms	Supports standard alarms and some private alarms.

Table 8-6 lists the third-party NE alarms supported by the U2000.

Table 8-6 Supported third-party NE alarms

NOTE

Proprietary alarms are those with the value in the **RFC/IEEE** column being -, and the rests are standard alarms.

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.6.3.1.1.5 .1	Cold Start	ColdStart	SNMPv2-MIB	RFC1907
1.3.6.1.6.3.1.1.5 .2	Warm Start	WarmStart	SNMPv2-MIB	RFC1907
1.3.6.1.6.3.1.1.5 .3	Link Down	linkdown	IF-MIB	RFC2233
1.3.6.1.6.3.1.1.5 .4	Link Up	linkup	IF-MIB	RFC2233
1.3.6.1.6.3.1.1.5 .5	Authentication failure	authentication	SNMPv2-MIB	RFC1907
1.3.6.1.6.3.1.1.5 .6	Egp neighbor loste	egpNeighborLoss	SNMPv2-MIB	RFC1215

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.0.8802.1.1.2.0 .0.1	Alarm that the status of the remote neighbor is changed	lldpRemTablesChange	LLDP-MIB	IEEE802.1 AB
1.0.8802.1.1.3.0 .1	MEP Disconnection Alarm	dot1agCfmMepHighestPrDefect	IEEE802171-CFM-MIB	IEEE802.1ag
1.0.8802.1.1.3.1 .6.2.1.10	Alarm that the incorrect CC packet is received	dot1agCfmMepSomeRMepCcmDefect	IEEE8021-CFM-MIB	IEEE802.1ag
1.0.8802.1.1.3.1 .6.2.1.11	Remote CC receiving failure	dot1agCfmMepErrorCcmDefect	IEEE8021-CFM-MIB	IEEE802.1ag
1.0.8802.1.1.3.1 .6.2.1.12	Cross connection error	dot1agCfmMepXconCcmDefect	IEEE8021-CFM-MIB	IEEE802.1ag
1.0.8802.1.1.3.1 .6.2.1.13	Remote fault notification	dot1agCfmMepSomeRdiDefect	IEEE8021-CFM-MIB	IEEE802.1ag
1.0.8802.1.1.3.1 .6.2.1.27	Cooperation fault notification	dot1agCfmMepErrorMacStatus	IEEE8021-CFM-MIB	IEEE802.1ag
1.3.6.1.2.1.10.1 66.11.0.1	L3VPN VRF Up	mplsL3VpnVrfUp	MPLS-L3VPN-STD-MIB	RFC4382
1.3.6.1.2.1.10.1 66.11.0.2	L3VPN VRF Down	mplsL3VpnVrfDown	MPLS-L3VPN-STD-MIB	RFC4382
1.3.6.1.2.1.10.1 66.11.0.3	Route count exceed Threshhold value/mid value	mplsL3VpnVrfRouteMidThreshExceeded	MPLS-L3VPN-STD-MIB	RFC4382
1.3.6.1.2.1.10.1 66.11.0.4	Route Count Exceeded Threshold	mplsL3VpnVrfNumVrfRouteMaxThreshExceeded	MPLS-L3VPN-STD-MIB	RFC4382
1.3.6.1.2.1.10.1 66.11.0.6	Route count drops back below threshhold value	mplsL3VpnNumVrfRouteMaxThrshCleared	MPLS-L3VPN-STD-MIB	RFC4382
1.3.6.1.2.1.10.1 66.11.0.5	L3Vpn illegal label exceed threshold	mplsL3VpnNumVrfSecIlgIlblThshExcd	MPLS-L3VPN-STD-MIB	RFC4382
1.3.6.1.2.1.10.1 66.2.0.1	MPLS XC Up	mplsXCUp	MPLS-LSR-STD-MIB	RFC3813
1.3.6.1.2.1.10.1 66.2.0.2	MPLS XC Down	mplsXCDown	MPLS-LSR-STD-MIB	RFC3813
1.3.6.1.2.1.10.1 66.2.0.3	MPLS LDP session up(old)	mplsLdpSessionUp	MPLS-LDP-STD-MIB	RFC3815

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.2.1.10.1 66.2.0.4	MPLS LDP session down(old)	mplsLdpSession Down	MPLS-LDP-STD-MIB	RFC3815
1.3.6.1.2.1.10.1 66.3.0.1	Resuming MPLS Tunnel Failure	mplsTunnelUp	MPLS-TE-STD-MIB	RFC3812
1.3.6.1.2.1.10.1 66.3.0.2	MPLS Tunnel Failure	mplsTunnelDown	MPLS-TE-STD-MIB	RFC3812
1.3.6.1.2.1.10.1 66.3.0.3	MPLS Tunnel Rerouted	mplsTunnelRerouted	MPLS-TE-STD-MIB	RFC3812
1.3.6.1.2.1.10.1 66.3.0.4	MPLS Tunnel Reoptimized	mplsTunnelReoptimized	MPLS-TE-STD-MIB	RFC3812
1.3.6.1.2.1.10.1 66.3.2.0.3	LDP Session up(devicevendor)	mplsLdpSession Up	MPLS-LDP-MIB	RFC3815
1.3.6.1.2.1.10.1 66.3.2.0.4	LDP Session down(devicevendor)	mplsLdpSession Down	MPLS-LDP-MIB	RFC3815
1.3.6.1.2.1.10.1 66.3.2.0.2	LDP path vector threhold is not match	mplsLdpPathVectorLimitMismatch	MPLS-LDP-MIB	RFC3815
1.3.6.1.2.1.10.1 66.3.2.0.1	Timeout to retry backward session index	mplsLdpInitSessionThresholdExceeded	MPLS-LDP-MIB	RFC3815
1.3.6.1.2.1.10.1 66.4.0.1	Session Threshold Exceed Trap	mplsLdpInitSessionThresholdExceeded	MPLS-LDP-STD-MIB	RFC3815
1.3.6.1.2.1.10.1 66.4.0.2	MPLS LDP Path Vector Limit Mismatch	mplsLdpPathVectorLimitMismatch	MPLS-LDP-STD-MIB	RFC3815
1.3.6.1.2.1.10.1 66.4.0.3	MPLS LDP Session Up	mplsLdpSession Up	MPLS-LDP-STD-MIB	RFC3815
1.3.6.1.2.1.10.1 66.4.0.4	MPLS LDP Session Down	mplsLdpSession Down	MPLS-LDP-STD-MIB	RFC3815
1.3.6.1.2.1.10.1 8.15.0.1	DSX1 Line Status Changed	dsx1LineStatusChange	DS1-MIB	RFC2495
1.3.6.1.2.1.10.3 0.15.0.1	DSX3 Line Status Changed	dsx3LineStatusChange	DS3-MIB	RFC2496
1.3.6.1.2.1.10.3 2.0.1	Frame Relay Status Changed	frDLCIStatusChange	FRAME-RELAY-DTE-MIB	RFC2115

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.2.1.10.4 4.2.0.2	Framerelay PVC Connect Status Change	frPVCCConnectStatusNotif	FRNETSERV-MIB	RFC2954
1.3.6.1.2.1.10.5. 1	X.25 Restart	X.25Restart	RFC1382-MIB	RFC1382
1.3.6.1.2.1.10.5. 2	X.25 Reset	X.25Reset	RFC1382-MIB	RFC1382
1.3.6.1.2.1.10.9 5.0.1	l2tp Tunnel Authentification Failure	l2tpTunnelAuthFailure	L2TP-MIB	RFC3371
1.3.6.1.2.1.14.1 6.2.1	OSPF Virtual Interface State Changed	ospfVirtIfStateChange	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.2	OSPF Neighbor State Changes	ospfNbrStateChange	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.3	OSPF Virtual Neighbor State Changed	ospfVirtNbrStateChange	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.4	OSPF Interface Configuration Error	ospfIfConfigError	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.5	OSPF Virtual Interface Configuration Error	ospfVirtIfConfigError	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.6	OSPF Interface Authentication Failure	ospfIfAuthFailure	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.7	OSPF Virtual Interface Authentication Failure	ospfVirtIfAuthFailure	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.8	OSPF Interface RX Bad Packet	ospfIfRxBadPacket	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.9	OSPF Virtual Interface RX Bad Packet	ospfVirtIfRxBadPacket	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.10	OSPF Interface Retransmitted OSPF Packet	ospfTxRetransmit	OSPF-TRAP-MIB	RFC4750

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.2.1.14.1 6.2.11	OSPF Virtual Interface Retransmit OSPF Packet	ospfVirtIfTxRetransmit	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.12	OSPF Originate Lsa	ospfOriginateLsa	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.13	OSPF Max Age Lsa	ospfMaxAgeLsa	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.14	OSPF LSDB Overflowed	ospfLsdbOverflow	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.15	OSPF LSDB Will Overflow	ospfLsdbApproachingOverflow	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.16	OSPF Interface State Changed	ospfIfStateChange	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.17	OSPF Nssa Translator Status Change	ospfNssaTranslatorStatusChange	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.18	OSPF Router Restart State Changed	ospfRestartStatusChange	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.19	OSPF Neighbor Restart Helper State Changed	ospfNbrRestartHelperStatusChange	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.14.1 6.2.20	OSPF Virtual Neighbor Restart Helper State Changed	ospfVirtNbrRestartHelperStatusChange	OSPF-TRAP-MIB	RFC4750
1.3.6.1.2.1.15.7. 1	BGP establishment	bgpEstablished	BGP4-MIB	RFC1657
1.3.6.1.2.1.15.7. 2	BGP Status Changed	bgpBackwardTransition	BGP4-MIB	RFC1657
1.3.6.1.2.1.157. 0.1	The PIM neighbor is lost	pimNeighborLoss	PIM-STD-MIB	RFC5060
1.3.6.1.2.1.157. 0.2	PIM receives an invalid register message	pimInvalidRegister	PIM-STD-MIB	RFC5060
1.3.6.1.2.1.157. 0.3	PIM receives an Invalid Join/Prune message	pimInvalidJoinPrune	PIM-STD-MIB	RFC5060

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.2.1.157.0.4	The RP changes	pimRPMappingChange	PIM-STD-MIB	RFC5060
1.3.6.1.2.1.157.0.5	The interface is elected as a DR	pimInterfaceElection	PIM-STD-MIB	RFC5060
1.3.6.1.2.1.158.0.1	DOT3 OAM THRESHOLD	dot3OamThresholdEvent	DOT3-OAM-MIB	RFC4878
1.3.6.1.2.1.158.0.2	DOT3 OAM NON THRESHOLD	dot3OamNonThresholdEvent	DOT3-OAM-MIB	RFC4878
1.3.6.1.2.1.16.0.1	RMON Rising Threshold Alarm	risingAlarm	RMON-MIB	RFC2819
1.3.6.1.2.1.16.0.2	RMON Falling Threshold Alarm	fallingAlarm	RMON-MIB	RFC2819
1.3.6.1.2.1.16.1	RMON Rising Threshold Alarm	-	RFC1271-MIB	RFC1271
1.3.6.1.2.1.16.2	RMON Falling Threshold Alarm	-	RFC1271-MIB	RFC1271
1.3.6.1.2.1.17.0.2	Topology Change Alarm	topologyChange	BRIDGE-MIB	RFC1493
1.3.6.1.2.1.17.0.1	New Root	NewRoot	BRIDGE-MIB	RFC1493
1.3.6.1.2.1.191.0.1	Ospfv3 VirtIf State Change	ospfv3VirtIfStateChange	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.191.0.3	Ospfv3 Virt NbrState Change	ospfv3VirtNbrStateChange	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.191.0.5	Ospfv3 VirtIf Config Error	ospfv3VirtIfConfigError	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.191.0.7	Ospfv3 VirtIf Rx Bad Packet	ospfv3VirtIfRxBadPacket	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.191.0.11	Ospfv3 Nssa Translator Status Change	ospfv3NssaTranslatorStatusChange	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.191.0.12	Ospfv3 Restart Status Change	ospfv3RestartStatusChange	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.191.0.2	Non-virtual OSPFv3 Neighbor State Change	ospfv3NbrStateChange	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.191.0.10	Non-virtual OSPFv3 Interface State Change	ospfv3IfStateChange	OSPFV3-MIB	RFC5643

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.2.1.191.0.4	Ospfv3 If Config Error	ospfv3IfConfigError	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.191.0.6	Non-virtual OSPFv3 Interface Receive Bad Packet	ospfv3IfRxBadPacket	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.191.0.13	Neighbor Exits From The Restart Helper State	ospfv3NbrRestartHelperStatusChange	OSPFV3-MIB	RFC5643
1.3.6.1.2.1.26.0.1	Repeat Mau Jabber	rpMauJabberTrap	MAU-MIB	RFC2668
1.3.6.1.2.1.26.0.2	Interface Mau Jabber	ifMauJabberTrap	MAU-MIB	RFC2668
1.3.6.1.2.1.47.2.0.1	Entity Configuration Change	entConfigChange	ENTITY-MIB	RFC4133
1.3.6.1.2.1.55.2.0.1	Interface IPv6 status changed	ipv6IfStateChange	IPV6-MIB	RFC2465
1.3.6.1.2.1.55.2.0.2	Interface IPv6 status is down	-	IPV6-MIB	RFC2465
1.3.6.1.2.1.68.0.1	VRRP Slave Switched to Master	vrrpTrapNewMaster	VRRP-MIB	RFC2787
1.3.6.1.2.1.68.0.2	VRRP Auth Failure	vrrpTrapAuthFailure	VRRP-MIB	RFC2787
1.3.6.1.2.1.68.1	VRRP Slave Switched to Master	vrrpTrapNewMaster	VRRP-MIB	RFC2787
1.3.6.1.2.1.68.2	VRRP Auth Failure	vrrpTrapAuthFailure	VRRP-MIB	RFC2787
1.3.6.1.2.1.68.0.4	VRRP States Change	vrrpTrapMasterDown	VRRP-MIB	RFC2787
1.3.6.1.2.1.68.0.3	VRRP transfer from Master to OtherState	vrrpTrapMasterToOtherState	VRRP-MIB	RFC2787
1.3.6.1.2.1.80.0.1	Ping probe failed	pingProbeFailed	DISMAN-PING-MIB	RFC4560
1.3.6.1.2.1.80.0.2	Ping test failed	pingTestFailed	DISMAN-PING-MIB	RFC4560
1.3.6.1.2.1.80.0.3	Ping test complete	pingTestCompleted	DISMAN-PING-MIB	RFC4560

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.2.1.81.0.1	Trace Route Path Change	traceRoutePathChange	DISMAN-TRACEROUTE-MIB	RFC4560
1.3.6.1.2.1.81.0.2	Trace Route Test Failed	traceRouteTestFailed	DISMAN-TRACEROUTE-MIB	RFC4560
1.3.6.1.2.1.81.0.3	Trace Route Test Completed	traceRouteTestCompleted	DISMAN-TRACEROUTE-MIB	RFC4560
1.3.6.1.3.118.0.1	L3VPN VRF Interface Up	mplsVrfIfUp	MPLS-VPN-MIB	RFC4382
1.3.6.1.3.118.0.2	L3VPN VRF Interface Down	mplsVrfIfDown	MPLS-VPN-MIB	RFC4382
1.3.6.1.3.118.0.3	L3VPN VRF Route Num Exceed MidThresh	mplsNumVrfRouteMidThreshExceeded	MPLS-VPN-MIB	RFC4382
1.3.6.1.3.118.0.4	L3VPN VRF Route Num Exceed MaxThresh	mplsNumVrfRouteMaxThreshExceeded	MPLS-VPN-MIB	RFC4382
1.3.6.1.3.118.0.5	L3VPN VRF Illegal Label Num Exceed ThreshExceeded	mplsNumVrfSecIllegalLabelThresholdExceeded	MPLS-VPN-MIB	RFC4382
1.3.6.1.3.37.2.0.1	IS-IS Database Overload	isisDatabaseOverload	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.2	IS-IS Area Address Dropped	isisManualAddressesDrops	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.3	LSP Checksum Error	isisCorruptedLSPDetected	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.4	IS-IS LSP Sequence Number Will Exceed the Maximum	isisAttemptToExceedMaxSequence	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.5	IS-IS ID Length Mismatch	isisIDLenMismatch	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.6	IS-IS Max Area Addresses Mismatch	isisMaxAreaAddressesMismatch	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.7	Own LSP Purged	isisOwnLSPPurge	ISIS-MIB	RFC4444

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.3.37.2.0.8	IS-IS Sequence Number Skipped	isisSequenceNumberSkip	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.9	IS-IS Password Type Mismatch	isisAuthenticationTypeFailure	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.10	IS-IS Authentication Failure	isisAuthenticationFailure	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.11	Wrong IS-IS Version	isisVersionSkew	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.12	IS-IS Area ID Mismatch	isisAreaMismatch	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.13	IS-IS Adjacency Rejected	isisRejectedAdjacency	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.14	ISIS LSP too large to propagate	isisLSPTooLargeToPropagate	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.15	IS-IS Origin LSP Buffer Size Mismatch	isisOrigLSPBufferSizeMismatch	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.16	IS-IS Protocol Mismatch	isisProtocolsSupportedMismatch	ISIS-MIB	RFC4444
1.3.6.1.3.37.2.0.17	IS-IS Adjacency Changed	isisAdjacencyChange	ISIS-MIB	RFC4444
1.3.6.1.3.61.1.0.1	PIM Neighbor Loss	PIMNeighborLoss	PIM-MIB	RFC2934
1.3.6.1.3.92.1.1.0.1	Msdp Established	msdpEstablished	MSDP-MIB	RFC4624
1.3.6.1.3.92.1.1.0.2	Msdp Backward Transition	msdpBackwardTransition	MSDP-MIB	RFC4624
1.3.6.1.4.1.9.9.1.17.2.0.4	Card Remove	cefcFRURemoved	CISCO-ENTITY-FRU-CONTROL-MIB	-
1.3.6.1.4.1.9.9.1.17.2.0.3	Card Insert	cefcFRUIInserted	CISCO-ENTITY-FRU-CONTROL-MIB	-

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.4.1.9.9.1 38.2.0.1	Hardware Failure	ceAlarmAsserted	CISCO-ENTITY-ALARM-MIB	-
1.3.6.1.4.1.9.9.1 38.2.0.2	Hardware Failure Resume	ceAlarmCleared	CISCO-ENTITY-ALARM-MIB	-
1.3.6.1.4.1.9.9.1 17.2.0.1	Module Status Change	cefcModuleStatusChange	CISCO-ENTITY-FRU-CONTROL-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.2.0.22	Ethernet Port Fault	tmnxEqPortEtherAlarm	TIMETRA-PORT-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.2.0.23	Ethernet Port Fault Resume	tmnxEqPortEtherAlarmClear	TIMETRA-PORT-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.2.0.9	SFP Removed	tmnxEqPortSFPRemoved	TIMETRA-PORT-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.2.0.8	SFP Inserted	tmnxEqPortSFPIinserted	TIMETRA-PORT-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.2.0.4	Sonet Port Fault	tmnxEqPortSonetAlarm	TIMETRA-PORT-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.2.0.5	Sonet Port Fault Resume	tmnxEqPortSonetAlarmClear	TIMETRA-PORT-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.1.0.5	Power Supply Removed	tmnxEqPowerSupplyRemoved	TIMETRA-CHASSIS-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.1.0.4	Power Supply Inserted	tmnxEqPowerSupplyInserted	TIMETRA-CHASSIS-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.1.0.9	Card Removed	tmnxEqCardRemoved	TIMETRA-CHASSIS-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.1.0.8	Card Inserted	tmnxEqCardInserted	TIMETRA-CHASSIS-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.1.0.3	Power Supply Failure	tmnxEqPowerSupplyFailure	TIMETRA-CHASSIS-MIB	-

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.4.1.6527 .3.1.3.2.1.0.6	Fan Failure	tmnxEqFanFailure	TIMETRA-CHASSIS-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.1.0.7	Card Failure	tmnxEqCardFailure	TIMETRA-CHASSIS-MIB	-
1.3.6.1.4.1.6527 .3.1.3.2.1.0.2	Temperature too high	tmnxEnvTempTooHigh	TIMETRA-CHASSIS-MIB	-
1.3.6.1.2.1.10.1 66.4.2.0.3	MPLS LDP session start	-	-	-
1.3.6.1.2.1.10.1 66.4.2.0.4	MPLS LDP session close	-	-	-
1.3.6.1.2.15.7.0. 1.1	BGP neighbour connection	-	-	-
1.3.6.1.2.15.7.0. 1.2	BGP backward transition	-	-	-
1.3.6.1.4.1.2011. 6.122.60.2.11	The connection to the log collector is interrupted	hwElogCollector-Interrupted	-	-
1.3.6.1.4.1.2011. 6.122.60.2.12	The connection to the log collector is recovered	hwElogCollector-Recovered	-	-
1.3.6.1.4.1.2011. 6.122.60.2.13	Begin to dump logs	hwElogServerDumpingFull	-	-
1.3.6.1.4.1.2011. 6.122.60.2.14	Log is discarded	hwElogCollector-LogDiscarded	-	-
1.3.6.1.4.1.2011. 6.122.60.2.15	Log collector received the log from NEs which are not managed by the log collector	hwElogCollector-NotManagedLog	-	-
1.3.6.1.4.1.2011. 6.122.60.2.16	Failed in dumping the logs	hwElogCollector-DumpingFailed	-	-
1.3.6.1.4.1.2011. 6.122.60.2.17	Fail to collect NE logs	hwElogCollector-CollectFail	-	-
1.3.6.1.4.1.2011. 6.122.60.2.18	Log Collector version is not the same with log server	hwElogCollector-VersionNotSame	-	-

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.4.1.2011.6.122.60.2.19	The time of NE log collected is not consistent with the time of log collector	hwElogCollector-TimeNotSame	-	-
1.3.6.1.4.1.2011.6.122.60.2.20	The alarm on storage space for online logs	hwElogCollector-OnlineLogsStorageSpaceAlarm	-	-
1.3.6.1.4.1.2011.6.122.60.2.21	The alarm on storage space for dump logs	hwElogCollector-DumpLogsStorageSpaceAlarm	-	-
1.3.6.1.4.1.2011.6.122.60.2.22	The WMIReceiverMgr service stops abnormally	hwElogCollector-WMIReceiverStop	-	-
1.3.6.1.4.1.2011.6.122.60.2.23	Data file has been damaged	hwElogCollector-DataFileDamaged	-	-
1.3.6.1.4.1.2011.6.122.60.2.24	Disk or file IO error	hwElogCollector-IOError	-	-
1.3.6.1.4.1.2011.6.122.60.2.26	Device logs received by the collector are not consecutive	-	-	-
1.3.6.1.4.1.2011.6.122.60.2.27	Failed to upload log files using SFTP.	-	-	-
1.3.6.1.4.1.2011.6.122.60.2.28	Active/standby front-end processors switchover alarm	-	-	-
1.3.6.1.4.1.2011.6.122.60.2.29	inconsistent counts of uploaded files	-	-	-
1.3.6.1.4.1.2011.6.122.60.2.30	FTP file upload interruption	-	-	-
1.3.6.1.4.1.2011.6.122.60.2.1	The NE is offline	-	-	-
1.3.6.1.4.1.2011.6.122.60.2.2	The NE restores from the off-line status	-	-	-

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.4.1.2011. 6.122.60.2.3	The CPU usage of the server exceeds the threshold	-	-	-
1.3.6.1.4.1.2011. 6.122.60.2.4	The CPU usage restores to normal status	-	-	-
1.3.6.1.4.1.2011. 6.122.60.2.5	The memory usage of the server exceeds the threshold	-	-	-
1.3.6.1.4.1.2011. 6.122.60.2.6	The memory usage restores to normal status.	-	-	-
1.3.6.1.4.1.2011. 6.122.60.2.7	The disk usage of the server exceeds the threshold	-	-	-
1.3.6.1.4.1.2011. 6.122.60.2.8	The disk capacity usage restores to normal status.	-	-	-
1.3.6.1.4.1.2011. 6.122.60.2.9	The database usage exceeds the threshold	-	-	-
1.3.6.1.4.1.2011. 6.122.60.2.10	The database usage restores to normal status.	-	-	-
1.3.6.1.4.1.7779 .3.1.1.1.1.1	Equipment Failure Trap	ibEquipmentFail ureTrap	-	-
1.3.6.1.4.1.7779 .3.1.1.1.1.2	Processing Failure Trap	ibProcessingFai lureTrap	-	-
1.3.6.1.4.1.7779 .3.1.1.1.1.3	Threshold Crossing Event	ibThresholdCros singEvent	-	-
1.3.6.1.4.1.7779 .3.1.1.1.1.4	State Change Event	ibStateChangeEv ent	-	-
1.3.6.1.4.1.7779 .3.1.1.1.1.5	Proc Start Stop Trap	ibProcStartStop- Trap	-	-
1.3.6.1.4.1.7779 .3.1.1.1.1.6	Revoked License Trap	ibRevokedLicens eTrap	-	-
1.3.6.1.4.1.7779 .3.1.1.1.1.7	Operation Trap	ibOperationTrap	-	-

TrapOID	Alarm Name	MIB Node	MIB Name	RFC/IEEE
1.3.6.1.4.1.2011.5.25.322.2.4	hwPceLspOutOfCtrl	hwPceLspOutOfCtrl	-	-
1.3.6.1.4.1.2011.5.25.322.2.5	hwPceLspOutOfCtrlClear	hwPceLspOutOfCtrlClear	-	-
1.3.6.1.4.1.2011.5.25.322.2.11	UnKnownSessionReceived	hwPceUnKnownSessionReceived	-	-
1.3.6.1.4.1.2011.5.25.322.2.12	UnKnownSessionReceivedClear	hwPceUnKnownSessionReceived-Clear	-	-
1.3.6.1.4.1.2011.5.25.322.2.13	SessionHasNoDelegatedLsp	hwPceSessionHasNoDelegatedLsp	-	-
1.3.6.1.4.1.2011.5.25.322.2.14	SessionHasNoneDelegatedLspClear	hwPceSessionHasNoDelegatedLspClear	-	-
1.3.6.1.2.1.227.0.2	pcePcepSessDown	pcePcepSessDown	-	-
1.3.6.1.2.1.227.0.1	pcePcepSessUp	pcePcepSessUp	-	-

9 Reliability

About This Chapter

Reliability design ensures that the product will be in service for many years because measures have been taken to prevent potential risks.

9.1 Physical Machine Reliability and Protection Solution

The U2000 physical machines provide complete reliability and protection solutions for different deployment modes. The hardware, software, and system security protection solutions in different deployment modes are basically the same, and the differences are mainly reflected by the remote disaster recovery (DR) protection solution. The single-server system deployment mode does not support remote DR protection. The remote DR protection type in cold backup deployment mode is the cold backup solution, and the remote DR protection type in HA system deployment mode is the HA solution.

9.2 Virtual Machine Reliability and Protection Solution

The U2000 virtual machines (VMs) provide complete reliability and protection solutions for different deployment modes. The hardware, software, and system security protection solutions in different deployment modes are basically the same, and the differences are mainly reflected by the remote DR protection solution. The single-server system deployment mode does not support remote DR protection. The remote DR protection type in cold backup deployment mode is the cold backup solution, and the remote DR protection type in HA system deployment mode is the HA solution.

9.1 Physical Machine Reliability and Protection Solution

The U2000 physical machines provide complete reliability and protection solutions for different deployment modes. The hardware, software, and system security protection solutions in different deployment modes are basically the same, and the differences are mainly reflected by the remote disaster recovery (DR) protection solution. The single-server system deployment mode does not support remote DR protection. The remote DR protection type in cold backup deployment mode is the cold backup solution, and the remote DR protection type in HA system deployment mode is the HA solution.

Table 9-1 describes the protection solutions of the U2000 physical machines under the Huawei delivery scenario.

Table 9-1 Application scenarios of the U2000 protection solutions

Protection Type	Protection Solution	Application Scenario
Hardware protection	Hardware redundancy	The U2000 enhances reliability by providing redundancy protection for hardware such as the power supply, fan, switch board, and network adapter.
	Hard disk redundancy backup	A hardware disk group (logical) is composed of multiple hard disks (physical) to provide higher storage performance and data redundancy protection.
Software protection	Backup	Data backup improves the reliability of the important U2000 data. When a fault occurs on the data, for example, the U2000 or database reports an error, you can use the backup data to restore the data.
	Process protection	When the U2000 detects unexpected process termination or faults, it automatically handles the problem or notifies users of the problem.
Remote DR protection	HA system	Two sets of U2000 are configured as primary and secondary sites. The mainstream Veritas remote hot backup technology in the industry is used to implement real-time synchronization of data volumes between the primary and secondary sites. When the primary site fails, the U2000 application is automatically switched to the secondary site without interruption.
	Cold backup system	Two sets of U2000 are configured as primary and secondary sites. The primary site periodically backs up the U2000 database file, and the secondary site periodically obtains the U2000 database file from the primary site for restoration. The secondary site is ready to take over the live network upon primary site failure.
System security	OS hardening and anti-virus	The U2000 provides hardening tools and anti-virus solutions for the OS to fix vulnerabilities and prevent risks.
	Communication security	Reliable communication protocols and encryption policies are adopted to ensure communication security between network nodes. In addition, DCN protection also improves the reliability of the communication connection between the U2000 and devices.

Protection Type	Protection Solution	Application Scenario
	U2000 operation security	The U2000 leverages user access control, centralized authentication, audit tracing, and security events and alarms to ensure operation security of the application layer.

Hardware Redundancy

- It is advisable to set up a U2000 distributed system environment with the hardware that supports redundancy.
- Hardware redundancy is provided by blade server hardware and disk arrays. Specific hardware redundancy types include power supply redundancy, fan redundancy, switch board 1+1 redundancy, and management module redundancy for the blade server. The redundancy types available to disk arrays include controller redundancy, power supply redundancy and so on. When this hardware is damaged, protection is automatically implemented
- Redundancy involves instant protection switching without impact on the U2000.

Hard Disk Redundancy Backup

The hard disk redundancy backup function helps to improve the reliability of disk data on the U2000 server.

RAID Technologies Used by the U2000

Redundant array of independent disks (RAID) is a technology that is used to form a logical hard disk group by combining multiple independent physical hard disks in different modes. In this way, RAID provides a storage capability higher than that of a single hard disk and implements the data redundancy protection. The different modes of forming hard disk groups are called RAID levels.

- RAID 0: consists of more than two hard disks by summing up their capacities. In a disk array group, these hard disks are concurrently processed. During data access, data is read and written respectively in each hard disk at the same time. This greatly improves the efficiency of accessing and writing data.
- RAID 1: RAID 1, also called disk mirroring, mirrors the data of one hard disk to another hard disk. Without affecting performance, disk mirroring ensures the reliability and restorability of the system to the greatest extent. This provides a strong capability of data redundancy. RAID 1 requires at least two hard disks.
- RAID 10: a combination of RAID 0 and RAID 1. Two hard disks are used to configure RAID 1 and two hard disk groups for RAID 1 are used to configure RAID 0. RAID 10 features the advantages of both RAID 0 and RAID 1. Four hard disks are required to configure a RAID 10.

Principles of Planning the Hard Disk Redundancy Backup

With reference to [Table 9-2](#), plan the hard disk redundancy backup according to the server hardware and the number of hard disks in the U2000 server.

Table 9-2 Recommended RAID level

Server Hardware	Configuration Principle
Windows server	<p>For the single-server system (Windows):</p> <ul style="list-style-type: none"> ● The RAID10 and hot spare disk (hot backup) is recommended for eight hard disks. Specifically, configure RAID 10 by using any four hard disks, two for hot spare disks, and the remaining two for further use. ● The RAID 10 and hot spare disk are recommended for six hard disks. Specifically, configure RAID 10 by using any four hard disks and use the remaining two as a hot spare disk. ● The RAID 10 and hot spare disk are recommended for five hard disks. Specifically, configure RAID 10 by using any four hard disks and use the remaining one as a hot spare disk. ● RAID 10 is recommended for four hard disks. Specifically, configure RAID 1 by using two hard disks and then configure RAID 0 by using the two RAID 1 hard disk groups. ● RAID 1 is recommended for two hard disks.
	<p>For the single-server system (SUSE Linux) and the high availability system (SUSE Linux), 8 hard disks are configured by default:</p> <ul style="list-style-type: none"> ● The first and second hard disks are configured as RAID 1 for installing OS software and data. ● The third, fourth, fifth, and sixth hard disks are configured as RAID 10 for storing service data and software. ● The seventh hard disk is configured as RAID 0 to back up full system. ● The eighth hard disk is configured as RAID 0 to back up the database.
Solaris workstation	<ul style="list-style-type: none"> ● RAID 1 is recommended for two hard disks. ● Two RAID 1 groups are recommended for four hard disks.
Disk array	<ul style="list-style-type: none"> ● OceanStor S3900/5500 V3: The RAID 10 and hot spare disk are recommended for the disk array where 12 hard disks are configured. Specifically, configure RAID 10 by using any 10 hard disks and use the remaining 2 as hot spare disks. ● OceanStor S2600: The RAID 5 and hot spare disk are recommended for the disk array where six hard disks are configured. Specifically, configure RAID 5 by using any four hard disks and use the remaining one as a hot spare disk.

Data Backup

The data backup function helps to improve the reliability of important U2000 data. The following table lists the data backup solutions provided by the U2000.

Table 9-3 Data backup

Data to Be Backed Up	Solution	Remarks
Alarm log, abnormal event log, performance log, security log, and operation log	Dump logs.	Perform these operations on the U2000 client. For details, see the <i>U2000 Online Help</i> .
Configuration data	Export the configuration data to script files. The script files neglect the database structural differences among the U2000s of different versions and are suitable for data backup in the case of a version upgrade. The script files supported by the U2000 include network-wide configuration files, U2000 naming files, NE configuration files, NE list files, U2000 computer information files, service implementation configuration files, network-layer information files, and network simulation and planning information files.	
Database	Back up all data in the U2000 database.	
NE database	Back up the NE data.	

Process Protection

- When the U2000 detects that a process stops abnormally or is faulty, it records system logs. Then, the system restarts the process automatically and ensures that the process is running properly. The system can also generate an alarm that urges a user to manually resolve the problem.
- In the case of an HA system, when the active server is faulty (for example, software applications fail or the database quits unexpectedly), switchover is performed between the active server and the standby server and then the standby server starts to monitor networks.

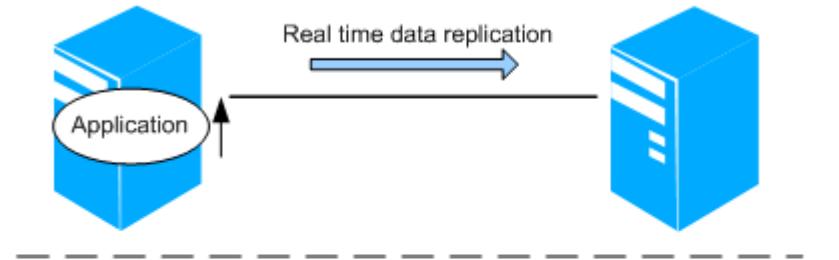
HA System

The use of an HA system improves the reliability of the U2000 servers.

In a HA system, the U2000 servers work in 1+1 backup mode. If the primary site fails, the U2000 applications are automatically switched to the secondary site without being interrupted. For details, see [Figure 9-1](#).

Figure 9-1 Switchover between primary and secondary sites in an HA system

Normal Status



When a fault occurs, the NMS application is switched to the standby site.



The protection mechanism of an HA system has two features:

- Database synchronization and backup between the primary and secondary sites
- Automatic application switchover between the primary and secondary sites

The reliability of the HA system can be measured by data.

Table 9-4 Reliability indicators of the U2000

Item	Indicator
MTBF	The average fault interval is larger than 6 months. The fault is defined as database crash.
MTTR	The average fault recovery time is no more than 15 minutes. The fault is defined as database crash.
HA switching time	≤ 15 minutes NOTE 70% of the management capacity For physical machines, HA switching time does not include the fault detection time; for virtual machines, HA switching time includes the fault detection time.

Cold Backup System

If only one single server U2000 is deployed at a site, network management functions will become unavailable if the U2000 fails. The cold backup feature is therefore introduced by HUAWEI to implement fast restoration in the case of a system failure.

In the cold backup solution, two single server U2000 systems with the same version, deployment domain, language, OS type, server time, and time zone are deployed. One system is run on the primary site and the other is run on the secondary site.

- In normal conditions, the primary site provides the network management functions. The network management process and maintenance tool on the secondary site are standby while the database is running. The primary site backs up the network management data periodically, and the secondary site obtains the backup file from the primary site at regular intervals.
- If the U2000 on the primary site fails, the U2000 on the secondary site starts immediately to provide network management functions.

The backup object is the entire database, including the custom data at the U2000 side (excluding the custom options of the system), network layer trail data, NE-side configuration data, alarm data and performance data. In addition, a backup is created for the structure of the entire database, all database tables (including the system tables and the user tables), table structure, and stored procedures.

NOTE

- The personal information (including personal name, phone numbers and addresses) on the U2000 and all user names and passwords are also backed up. Therefore, you are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the personal data of users is fully protected.
- The following data is not backed up when you back up the U2000 database:
 - The data that is not saved at the NE side, that is, the data that cannot be uploaded.
 - The custom options of the system. For example, font, color setting, and audio setting.

OS Hardening and Anti-virus

- The U2000 physical machines run the general OSs (Windows, Solaris, and SUSE Linux). Generally, the default OS configurations cannot meet security requirements of telecom management systems. For example, by default the OS runs services and opens external communication ports that are redundant or unnecessary for the U2000, and uses Transmission Control Protocol/Internet Protocol (TCP/IP) parameters that make the U2000 vulnerable. Therefore, the OS easily becomes a weakness in the security of the U2000. To ensure that the U2000 runs securely and stably, Huawei releases the U2000 with OS security hardening software and provides default security hardening policies. Security hardening takes effect after you manually import the policy file into the system. The U2000 provides corresponding system hardening tools for different OSs.

Table 9-5 OS hardening tools

OS	Hardening Tool
Solaris	SetSolaris
Windows	Setwin
SUSE Linux	SetSUSE

- The Windows OS is vulnerable to viruses, leading to abnormal U2000 running or even system crash.

A virus scan using Symantec, OfficeScan, McAfee, Avira AntiVir and Kaspersky software is run before the U2000 is released. The U2000 has also passed the OfficeScan compatibility test. The U2000 software package includes OfficeScan to protect the system against viruses. OfficeScan is only applied to the Windows.

Communication Security

- Information is transmitted on networks at the risk of being eavesdropped, tampered, or copied and resent. The U2000 and gateway device adopt the TCP/IP protocol for communication, and the communication channel uses the standard SNMPv3, SSL, SSH, SFTP, or HTTPS protocol for encryption to ensure security.
- You can use a data communication network (DCN) to connect the U2000 to a standby gateway NE (GNE). This improves the reliability of the communication connection between the U2000 and equipment. Only the MSTP, WDM, RTN, PTN, and router series NEs support DCN protection.

The communication between non-GNEs and the U2000 is forwarded by the GNE. In the U2000, you can set the active GNE and standby GNE for NEs in advance. When the communication between the active GNE and the U2000 is interrupted, the U2000 automatically switches to the standby GNE for communication, so that the communication between the U2000 and NEs is not interrupted. When the communication between the U2000 and the active GNE recovers, the U2000 determines whether to use the active GNE again according to the preset revertive mode.



For Transport Domain, the recommended number of non-gateway NEs (including non-gateway NEs that connects to the GNE by using the extended ECC) that connect to each GNE is fewer than 50. Once the limit is exceeded, the number of GNEs should be increased.

U2000 Operation Security

- User Access Control: Access control includes user management, automatic lock-out policy, online user monitoring, and user permission division.
- Centralized Authentication: The U2000 provides three user authentication modes: local authentication, Remote Authentication Dial-In User Service (RADIUS) authentication, and Lightweight Directory Access Protocol (LDAP) authentication. Local authentication: The U2000 server implements user management, login authentication, and security policies in a unified manner. Local authentication is the default user authentication management mode provided by the U2000. RADIUS authentication: During user login, the U2000 verifies and authenticates users' login requests through the RADIUS server and authorizes login users based on the permissions of the belonging user group. LDAP authentication: During user login, the U2000 verifies and authenticates users' login requests through the LDAP server and authorizes login users based on the permissions of the belonging user group. LDAP authentication is similar to RADIUS authentication, but the protocols used are different.
- Audit Tracing: The U2000 provides complete log information about running status, security events, and operations and configurations for query and audit, real-time check, analysis, and protection. With the log information, proper measures can be taken if services on live networks are affected by users' operations. Logs of each NE can also be managed by the U2000 in a uniform manner. Based on log impacts on the U2000, logs

are divided into security log, operation log, and system log. Logs can be forwarded to a third-party server.

- Security Event Alarms: After the system detects an event or behavior that is against the configured security policies or the event or behavior will bring security risks to the system, the system reports information about the security event to the security alarm management platform (such as the U2000) so that administrators can immediately handle the event or behavior to eliminate security risks.

9.2 Virtual Machine Reliability and Protection Solution

The U2000 virtual machines (VMs) provide complete reliability and protection solutions for different deployment modes. The hardware, software, and system security protection solutions in different deployment modes are basically the same, and the differences are mainly reflected by the remote DR protection solution. The single-server system deployment mode does not support remote DR protection. The remote DR protection type in cold backup deployment mode is the cold backup solution, and the remote DR protection type in HA system deployment mode is the HA solution.

Table 9-6 describes the protection solutions of the U2000 VMs under the Huawei delivery scenario.

Table 9-6 Application scenarios of the U2000 protection solutions

Protection Type	Protection Solution	Application Scenario
Hardware protection	Hardware redundancy	The U2000 enhances reliability by providing redundancy protection for hardware such as the power supply, fan, switch board, and network adapter.
	Hard disk redundancy backup	A hardware disk group (logical) is composed of multiple hard disks (physical) to provide higher storage performance and data redundancy protection.
	vSphere HA cluster-based protection(VMware)	By installing the VMware management software, you can define multiple blades as a cluster. When a blade server is damaged, the VMs on the blade will be automatically switched to the failover host for proper running. After the damaged blade is restored to be the same as the previous configuration, the VMs on the failover host are switched back to the repaired blade.
Software protection	Backup	Data backup improves the reliability of the important U2000 data. When a fault occurs on the data, for example, the U2000 or database reports an error, you can use the backup data to restore the data.

Protection Type	Protection Solution	Application Scenario
	Snapshot protection of VMs	A VM snapshot is an image of a VM disk file at a specific time point and is used to back up the current system status. When VM system upgrade or patch installation fails and cannot be recovered, you can restore the VM to the previous status using snapshots.
	Process protection	When the U2000 detects unexpected process termination or faults, it automatically handles the problem or notifies users of the problem.
Remote DR protection	HA system	Two sets of U2000 are configured as primary and secondary sites. The mainstream Veritas remote hot backup technology in the industry is used to implement real-time synchronization of data volumes between the primary and secondary sites. When the primary site fails, the U2000 application is automatically switched to the secondary site without interruption.
	Cold backup system	Two sets of U2000 are configured as primary and secondary sites. The primary site periodically backs up the U2000 database file, and the secondary site periodically obtains the U2000 database file from the primary site for restoration. The secondary site is ready to take over the live network upon primary site failure.
System security	OS hardening and anti-virus	The U2000 provides hardening tools and anti-virus solutions for the OS to fix vulnerabilities and prevent risks.
	Communication security	Reliable communication protocols and encryption policies are adopted to ensure communication security between network nodes. In addition, DCN protection also improves the reliability of the communication connection between the U2000 and devices.
	U2000 operation security	The U2000 leverages user access control, centralized authentication, audit tracing, and security events and alarms to ensure operation security of the application layer.

Hardware Redundancy

- It is advisable to set up a U2000 distributed system environment with the hardware that supports redundancy.
- Hardware redundancy is provided by blade server hardware and disk arrays. Specific hardware redundancy types include power supply redundancy, fan redundancy, switch

board 1+1 redundancy, and management module redundancy for the blade server. The redundancy types available to disk arrays include controller redundancy, power supply redundancy and so on. When this hardware is damaged, protection is automatically implemented.

- Redundancy involves instant protection switching without impact on the U2000.

Hard Disk Redundancy Backup

The hard disk redundancy backup function helps to improve the reliability of disk data on the U2000 server.

RAID Technologies Used by the U2000

Redundant array of independent disks (RAID) is a technology that is used to form a logical hard disk group by combining multiple independent physical hard disks in different modes. In this way, RAID provides a storage capability higher than that of a single hard disk and implements the data redundancy protection. The different modes of forming hard disk groups are called RAID levels.

- RAID 0: consists of more than two hard disks by summing up their capacities. In a disk array group, these hard disks are concurrently processed. During data access, data is read and written respectively in each hard disk at the same time. This greatly improves the efficiency of accessing and writing data.
- RAID 1: RAID 1, also called disk mirroring, mirrors the data of one hard disk to another hard disk. Without affecting performance, disk mirroring ensures the reliability and restorability of the system to the greatest extent. This provides a strong capability of data redundancy. RAID 1 requires at least two hard disks.
- RAID 10: a combination of RAID 0 and RAID 1. Two hard disks are used to configure RAID 1 and two hard disk groups for RAID 1 are used to configure RAID 0. RAID 10 features the advantages of both RAID 0 and RAID 1. Four hard disks are required to configure a RAID 10.

Principles of Planning the Hard Disk Redundancy Backup

With reference to [Table 9-7](#), plan the hard disk redundancy backup according to the server hardware and the number of hard disks in the U2000 server.

Table 9-7 Recommended RAID level

Server Hardware	Configuration Principle
E9000 server	Add the two hard disks of each compute node to RAID 1 using the LSI SAS3108 RAID controller card installed on the E9000.
Disk array	OceanStor S3900/5500 V3: The RAID 10 and hot spare disk are recommended for the disk array where 12 hard disks are configured. Specifically, configure RAID 10 by using any 10 hard disks and use the remaining 2 as hot spare disks.

Hardware Protection based on vSphere HA

The vSphere HA cluster is a protection solution provided by VMware. This solution can be configured only when the U2000 is installed and runs on the VM VMware.

Hardware Protection based on vSphere HA supports local blade protection. When a blade server is damaged, the VMs on the blade will be automatically switched to the failover host for proper running. After the damaged blade is restored to be the same as the previous configuration, the VMs on the failover host are automatically switched back to the repaired blade.

Data Backup

The data backup function helps to improve the reliability of important U2000 data. The following table lists the data backup solutions provided by the U2000.

Table 9-8 Data backup

Data to Be Backed Up	Solution	Remarks
Alarm log, abnormal event log, performance log, security log, and operation log	Dump logs.	Perform these operations on the U2000 client. For details, see the <i>U2000 Online Help</i> .
Configuration data	Export the configuration data to script files. The script files neglect the database structural differences among the U2000s of different versions and are suitable for data backup in the case of a version upgrade. The script files supported by the U2000 include network-wide configuration files, U2000 naming files, NE configuration files, NE list files, U2000 computer information files, service implementation configuration files, network-layer information files, and network simulation and planning information files.	
Database	Back up all data in the U2000 database.	
NE database	Back up the NE data.	

Snapshot protection of VMs

A VM snapshot is a copy of the status and data of a VM at a specified time. When system upgrade or patch installation fails and cannot be recovered, you can perform a rollback using the stored snapshots.

- Generating snapshots: VM snapshots need to be generated before system upgrade or patch installation.
- Managing snapshots: It is recommended that the number of snapshots on a VM be no more than two and the stored time of each snapshot be no more than three days, to avoid occupying the storage space and affecting performance of VMs and hosts.
- Restoring snapshots: When system upgrade or patch installation fails and cannot be recovered, you need to restore the VM using snapshots. Only the status and data of the VM when the snapshots are created can be restored. After restoration, the current VM data is unavailable.

Process Protection

- When the U2000 detects that a process stops abnormally or is faulty, it records system logs. Then, the system restarts the process automatically and ensures that the process is running properly. The system can also generate an alarm that urges a user to manually resolve the problem.
- In the case of an HA system, when the active server is faulty (for example, software applications fail or the database quits unexpectedly), switchover is performed between the active server and the standby server and then the standby server starts to monitor networks.

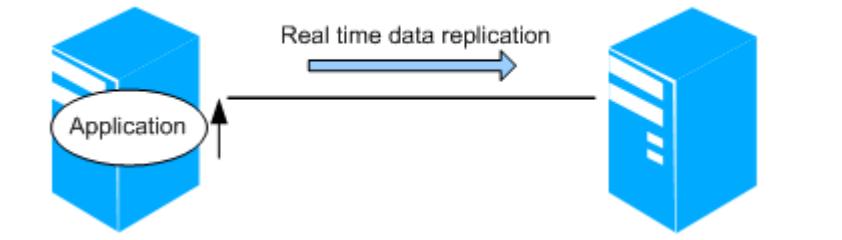
HA System

The use of an HA system improves the reliability of the U2000 servers.

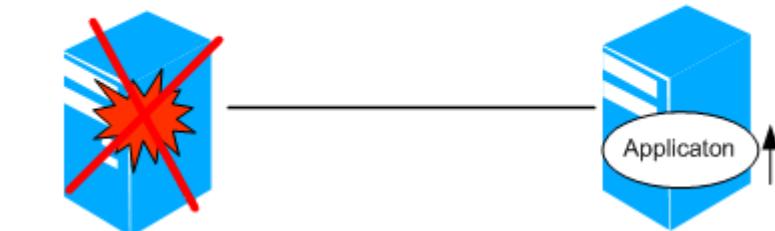
In a HA system, the U2000 servers work in 1+1 backup mode. If the primary site fails, the U2000 applications are automatically switched to the secondary site without being interrupted. For details, see [Figure 9-2](#).

Figure 9-2 Switchover between primary and secondary sites in an HA system

Normal Status



When a fault occurs, the NMS application is switched to the standby site.



The protection mechanism of an HA system has two features:

- Database synchronization and backup between the primary and secondary sites
- Automatic application switchover between the primary and secondary sites

The reliability of the HA system can be measured by data.

Table 9-9 Reliability indicators of the U2000

Item	Indicator
MTBF	The average fault interval is larger than 6 months. The fault is defined as database crash.
MTTR	The average fault recovery time is no more than 15 minutes. The fault is defined as database crash.
HA switching time	≤ 15 minutes NOTE 70% of the management capacity For physical machines, HA switching time does not include the fault detection time; for virtual machines, HA switching time includes the fault detection time.

Cold Backup System

If only one single server U2000 is deployed at a site, network management functions will become unavailable if the U2000 fails. The cold backup feature is therefore introduced by HUAWEI to implement fast restoration in the case of a system failure.

In the cold backup solution, two single server U2000 systems with the same version, deployment domain, language, OS type, server time, and time zone are deployed. One system is run on the primary site and the other is run on the secondary site.

- In normal conditions, the primary site provides the network management functions. The network management process and maintenance tool on the secondary site are standby while the database is running. The primary site backs up the network management data periodically, and the secondary site obtains the backup file from the primary site at regular intervals.
- If the U2000 on the primary site fails, the U2000 on the secondary site starts immediately to provide network management functions.

The backup object is the entire database, including the custom data at the U2000 side (excluding the custom options of the system), network layer trail data, NE-side configuration data, alarm data and performance data. In addition, a backup is created for the structure of the entire database, all database tables (including the system tables and the user tables), table structure, and stored procedures.

NOTE

- The personal information (including personal name, phone numbers and addresses) on the U2000 and all user names and passwords are also backed up. Therefore, you are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the personal data of users is fully protected.
- The following data is not backed up when you back up the U2000 database:
 - The data that is not saved at the NE side, that is, the data that cannot be uploaded.
 - The custom options of the system. For example, font, color setting, and audio setting.

OS Hardening and Anti-virus

- The U2000 VMs run the SUSE Linux OS. Generally, the default OS configurations cannot meet security requirements of telecom management systems. For example, by default the OS runs services and opens external communication ports that are redundant or unnecessary for the U2000, and uses Transmission Control Protocol/Internet Protocol (TCP/IP) parameters that make the U2000 vulnerable. Therefore, the OS easily becomes a weakness in the security of the U2000. To ensure that the U2000 runs securely and stably, Huawei releases the U2000 with OS security hardening software and provides default security hardening policies. Security hardening takes effect after you manually import the policy file into the system. For the SUSE Linux OS, the U2000 VMs provide the system hardening tool SetSUSE.
- The OS is vulnerable to viruses, leading to abnormal U2000 running or even system crash.

A virus scan using Symantec, OfficeScan, McAfee, Avira AntiVir and Kaspersky software is run before the U2000 is released. The U2000 has also passed the OfficeScan compatibility test. The U2000 software package includes OfficeScan to protect the system against viruses. OfficeScan is only applied to the Windows.

Communication Security

- Information is transmitted on networks at the risk of being eavesdropped, tampered, or copied and resent. The U2000 and gateway device adopt the TCP/IP protocol for communication, and the communication channel uses the standard SNMPv3, SSL, SSH, SFTP, or HTTPS protocol for encryption to ensure security.
- You can use a data communication network (DCN) to connect the U2000 to a standby gateway NE (GNE). This improves the reliability of the communication connection between the U2000 and equipment. Only the MSTP, WDM, RTN, PTN, and router series NEs support DCN protection.

The communication between non-GNEs and the U2000 is forwarded by the GNE. In the U2000, you can set the active GNE and standby GNE for NEs in advance. When the communication between the active GNE and the U2000 is interrupted, the U2000 automatically switches to the standby GNE for communication, so that the communication between the U2000 and NEs is not interrupted. When the communication between the U2000 and the active GNE recovers, the U2000 determines whether to use the active GNE again according to the preset revertive mode.



For Transport Domain, the recommended number of non-gateway NEs (including non-gateway NEs that connects to the GNE by using the extended ECC) that connect to each GNE is fewer than 50. Once the limit is exceeded, the number of GNEs should be increased.

U2000 Operation Security

- User Access Control: Access control includes user management, automatic lock-out policy, online user monitoring, and user permission division.
- Centralized Authentication: The U2000 provides three user authentication modes: local authentication, Remote Authentication Dial-In User Service (RADIUS) authentication, and Lightweight Directory Access Protocol (LDAP) authentication. Local authentication: The U2000 server implements user management, login authentication, and security policies in a unified manner. Local authentication is the default user authentication management mode provided by the U2000. RADIUS authentication: During user login, the U2000 verifies and authenticates users' login requests through the RADIUS server and authorizes login users based on the permissions of the belonging user group. LDAP authentication: During user login, the U2000 verifies and authenticates users' login requests through the LDAP server and authorizes login users based on the permissions of the belonging user group. LDAP authentication is similar to RADIUS authentication, but the protocols used are different.
- Audit Tracing: The U2000 provides complete log information about running status, security events, and operations and configurations for query and audit, real-time check, analysis, and protection. With the log information, proper measures can be taken if services on live networks are affected by users' operations. Logs of each NE can also be managed by the U2000 in a uniform manner. Based on log impacts on the U2000, logs are divided into security log, operation log, and system log. Logs can be forwarded to a third-party server.
- Security Event Alarms: After the system detects an event or behavior that is against the configured security policies or the event or behavior will bring security risks to the system, the system reports information about the security event to the security alarm management platform (such as the U2000) so that administrators can immediately handle the event or behavior to eliminate security risks.

10 Performance Indicators

This topic describes the performance indicators of the U2000.

Performance indicators

Table 10-1 Performance indicators

Item	Subitem	Indicator
NMS startup and shutdown	NMS start time (70% of the management capacity)	≤ 10 minutes
	NMS shutdown time (70% of the management capacity)	≤ 10 minutes
Database restoration time		≤ 60 minutes
Storage capacity	Capacity of current alarms	Maximum: 100,000
	Capacity of historical alarms	Maximum: 2,000,000 Storage period in the database: 180 days
	Capacity of logs, including operation logs and system logs	Maximum: 1,000,000 Storage period in the database: 90 days
Resources occupied	CPU usage	Equal to or less than 10%
Link capacity	Number of manageable links in the topology	Maximum: 200,000

Item	Subitem	Indicator
Processing capability	Response speed of handling an alarm	Usually equal to or less than 10 seconds. Response speed of handling an alarm indicates the interval from the time at which an alarm is generated on the equipment to the time at which the alarm is displayed on the U2000.
	Performance collection capability	Maximum performance collection capability in each collection mode: <ul style="list-style-type: none"> ● SNMP collection: 150,000 equivalent statistics records/15 minutes ● BULK collection: <ul style="list-style-type: none"> - IP equipment: 500,000 equivalent statistics records/15 minutes - Access equipment: 2,000,000 equivalent statistics records/15 minutes ● Qx collection: 100,000 equivalent statistics records/15 minutes NOTE For the performance collection capability of the U2000 on different hardware platforms, see Table 7-7 .
	Alarm handling capability	100 (400 maximum) alarms. Alarm handling capability indicates the number of alarms that can be handled per second by a full-domain U2000. When managing only access equipment, the U2000 can handle 50 alarms per second. When managing only IP equipment or transport equipment, the U2000 can handle 100 alarms per second.
U2000 user management capability	User	Maximum: 500
	User group	Maximum: 50
	Object set	Maximum: 100
	Operation Set	Maximum: 255
Concurrent NE upgrades		Maximum: 60
HWECC/IP over DCC networking capacity	Number of manageable GNEs	Maximum: 3000 NOTE The U2000 can manage 500 GNEs by a single instance.
	Number of manageable NEs for a GNE	Recommended: <= 50; maximum: <= 60

DCN bandwidth requirements

Table 10-2 DCN bandwidth requirements

Item	Bandwidth
Bandwidth required for communication between a U2000 client and the U2000 server	2 Mbit/s
Bandwidth required for communication between N Equivalent NEs and the U2000 server	<p>A bandwidth of 2 Mbit/s may not meet the bandwidth requirements for certain types of networks. In this case, you can set the CIR (Committed Information Rate) or PIR (Peak Information Rate) by using the following formulas. The bandwidth of the live network should meet the PIR requirement in large bandwidth consuming scenarios, such as network-wide data synchronization, performance data collection, and batch upgrade.</p> <p>CIR:</p> <ul style="list-style-type: none"> ● $N > 56$: $2048 \text{ kbit/s} + (N - 56) \times 0.5 \text{ kbit/s}$ ● $N \leq 56$: 2 Mbit/s <p>PIR:</p> <ul style="list-style-type: none"> ● $N > 56$: $10240 \text{ kbit/s} + (N - 56) \times 5 \text{ kbit/s}$ ● $N \leq 56$: 10 Mbit/s
Bandwidth required for communication between an OSS and the U2000 server	<p>2 Mbit/s</p> <p>NOTE A minimum of 2 Mbit/s is required.</p>

HA system bandwidth requirements

Table 10-3 Bandwidth planning requirements for the communication between the primary and secondary sites in the HA system (without the performance data collection function disabled)

Network Scale	Minimum Bandwidth	Recommended Bandwidth
Common-scale network with less than 2000 equivalent NEs	2 Mbit/s	4 Mbit/s

Network Scale	Minimum Bandwidth	Recommended Bandwidth
Medium-scale network with 2000 to 6000 equivalent NEs	6 Mbit/s	12 Mbit/s
Large-scale network with 6000 to 15000 equivalent NEs	15 Mbit/s	30 Mbit/s
Super-large-scale network: 15000-30000 equivalent NEs	30 Mbit/s	60 Mbit/s

Table 10-4 Bandwidth planning requirements for the communication between the primary and secondary sites in the HA system (with the SNMP performance data collection function enabled)

Network Scale	Performance Collection Capability (Without Max/Min Data Aggregation Enabled, Max Equivalent Statistics Record/15 Minutes)	Minimum Bandwidth	Recommended Bandwidth
Common-scale network with less than 2000 equivalent NEs	20000	4 Mbit/s	8 Mbit/s
Medium-scale network with 2000 to 6000 equivalent NEs	60000	12Mbit/s	24 Mbit/s
Large-scale network with 6000 to 15000 equivalent NEs	150000	28 Mbit/s	56 Mbit/s
Super-large-scale network: 15000-30000 equivalent NEs	150000	44 Mbit/s	88 Mbit/s

Table 10-5 Bandwidth planning requirements for the communication between the primary and secondary sites in the HA system (transport NE performance monitoring)

Network Scale	Minimum Bandwidth	Recommended Bandwidth
Common-scale network: < 2,000 equivalent NEs	4 Mbit/s	8 Mbit/s
Medium-scale network: 2,000-6,000 equivalent NEs	9 Mbit/s	18 Mbit/s
Large-scale network: 6,000-15,000 equivalent NEs	20 Mbit/s	40 Mbit/s
Super-large-scale network: 15000-30000 equivalent NEs	36 Mbit/s	72 Mbit/s

 **NOTE**

The bandwidth required between the primary and secondary sites in the HA system increase with the network scale and the number of performance monitoring instances.

11 Management Capability

About This Chapter

Management capability refers to the capability of the NMS to manage network resources, which are expressed in the number of equivalent NEs.

11.1 U2000 Management Capability

The management capability of the U2000 depends on the U2000 system itself and its hardware performance.

11.2 NE Equivalent Coefficient

The NE equivalent coefficient is the ratio of the resources used by physical NEs or ports to the resources used by equivalent NEs.

11.3 Management Capabilities of Standard Delivery Models

The management capabilities of U2000 vary according to the standard delivery model.

11.4 Management Capabilities of Compatible Models

The management capabilities of U2000 vary according to the compatible model.

11.1 U2000 Management Capability

The management capability of the U2000 depends on the U2000 system itself and its hardware performance.

The key technical specifications include the number of equivalent NEs, number of clients, and number of physical NEs. The management capability of the U2000 on a network that consists of different types of NEs is affected by the following factors:

- The management capability refers to the maximum number of equivalent NEs that can be managed by the U2000. The management capability depends on the hardware and varies with the hardware configuration.



Table 11-6 and **Table 11-7** list the management capabilities, service capability and performance collection capability of the IP and transmission domain on different hardware platforms. **Table 11-6**, **Table 11-8** list the management capabilities and performance collection capability of the access domain on different hardware platforms.

- If a client also runs on the computer where the server is running, the management capability is reduced by 50%. Running the client and server on different computers is recommended.
- The system limits the number of physical nodes, which in turn limits the management capability.

Table 11-1 shows the management capability of a single U2000.

Table 11-1 U2000 management capability

Item	Subitem	Indicator	Related to Hardware
Management capability	Number of managed equivalent NEs	Maximum: 30,000 equivalent NEs A maximum of 20,000 equivalent NEs can be supported when the U2000 manages only PTN networks.	Yes
	Number of managed clients	Maximum: 200 clients (by deploying multiple desktop service instances) The number of clients can reach 300 by deploying multiple desktop service instances on the U2000 that manages only access equipment.	Yes
	Number of managed physical nodes	Maximum: 20,000 physical NEs <ul style="list-style-type: none"> ● The maximum of managed physical NEs in IPRAN networks is 30,000. ● The maximum of managed MDUs in access networks is 60,000. ● There is no limit to the number of subnets. The maximum of physical nodes in each subnet is recommended to be 500; 200 is optimal. The maximum of subnet nests is recommended to be 6. 	No

Item	Subitem	Indicator	Related to Hardware
	Number of managed ONTs	Maximum: 4,000,000 ONTs If the U2000 manages only access NEs, the number of managed ONTs is not restricted to the maximum number of manageable equivalent NEs, 30,000.	Yes
	Number of managed CMs	Maximum: 1,000,000 CMs	Yes
Service capability	Number of managed SDH trails	Maximum: 500,000 SDH trails	Yes
	Number of managed WDM trails	Maximum: 300,000 WDM trails	Yes
	Number of managed IP service access interfaces (SAIs)	Maximum: 1,000,000 IP service access interfaces (SAIs) A maximum of 1,500,000 IP service access interfaces (SAIs) can be supported when the U2000 manages only IPRAN networks.	Yes
	Number of managed tunnels	Maximum: 100,000 A maximum of 150,000 tunnels can be supported when the U2000 manages only IPRAN networks.	Yes
	Number of managed sites (single-point services, such as VRF and VSI)	Maximum: 300,000 A maximum of 450,000 sites can be supported when the U2000 manages only IPRAN networks.	Yes

Table 11-2 shows the simple calculation methods of the maximum management capability on different network scales in FTTH, FTTB/C, and MSAN/DSLAM scenarios. (The maximum management capability is calculated based on lines, that is, ports.) If multiple scenarios exist on the actual network, the management scale in each scenario needs to be converted to the number of equivalent NEs and then summed up. **Table 11-6** lists the standard delivery models to be delivered on different network scales, and **Table 11-8** lists the compatible server models on different network scales.

Table 11-2 Management scale and restrict of access NEs in different scenes

Network Scale	FTTH Scene	FTTB/C Scene	DSLAM/MSA/N Scene	D-CCA P Scene
Small-scale network: less than 500 equivalent NEs	50,000 (lines)	50,000 (lines)	200,000 (lines)	50,000 CMs
Common-scale network: 500-2000 equivalent NEs	200,000 (lines)	200,000 (lines)	500,000 (lines)	200,000 CMs
Medium-scale network: 2000-6000 equivalent NEs	600,000 (lines)	600,000 (lines)	1,000,000 (lines)	400,000 CMs
Large-scale network: 6000-15000 equivalent NEs	1,200,000 (lines) Number of physical NEs less than 30,000	1,200,000 (lines) Number of physical NEs less than 30,000	1,920,000 (lines) Number of physical NEs less than 30,000	800,000 CMs
Super-large-scale network: 15000-30000 equivalent NEs	4,000,000 (lines) Number of physical NEs less than 60,000	2,000,000 (lines) Number of physical NEs less than 60,000	4,000,000 (lines) Number of physical NEs less than 60,000	1,000,000 CMs

11.2 NE Equivalent Coefficient

The NE equivalent coefficient is the ratio of the resources used by physical NEs or ports to the resources used by equivalent NEs.

Equivalent NE and Equivalent Coefficient

- Equivalent NE: The functional features, cross-connect capacity, and number of boards, ports, or channels are specific to the NE types. As such, the number of NEs that the NMS can manage depends on the types of NEs in the networks. To simplify the description

and calculation of the management capability, the concept of equivalent NE was defined so that NEs of different types or a number of ports can be converted to equivalent NEs by a uniform criteria according to the system resources that they require. The system resources required by an equivalent NE are equal to the resources for managing an STM-1 transport NE.

- Equivalent coefficient: Equivalent coefficient = (Resources used by physical NEs or ports)/(Resources used by equivalent NEs)

As demonstrated by the results of objective testing conducted on the U2000 in different types of environments, a single U2000 can manage a maximum of 20,000 physical NEs or 30,000 equivalent NEs. The management capacity is 20,000 physical NEs if they equal fewer than 30,000 equivalent NEs. The management capacity is 30,000 equivalent NEs if physical NEs equal more than 30,000 equivalent NEs. The U2000 supports concurrent logins of 200 clients.

The management scales of the U2000 are defined as follows:

- Small-scale network: less than 500 equivalent NEs
- Common-scale network: 500-2000 equivalent NEs
- Medium-scale network: 2000-6000 equivalent NEs
- Large-scale network: 6000-15000 equivalent NEs
- Super-large-scale network: 15000-30000 equivalent NEs

Calculating the Number of Equivalent NEs

Generally, the number of equivalent NEs that the U2000 can manage is calculated according to the following rules:

- The basic unit of an equivalent NE for the U2000 is OptiX Metro 1000.
- Virtual NE is equal to one equivalent NE. A pre-configured NE is equal to a real NE. One third-party NE is equal to one equivalent NE. The calculations of equivalent coefficients for the OEM equipment and Huawei equipment are the same.
- Number of equivalent NEs = Number of equivalent NEs in the transport domain + Number of equivalent NEs in the IP domain + Number of equivalent NEs in the access domain.

11.2.1 Equivalent Coefficients of NEs in the Transport Domain

Number of equivalent NEs in the transport domain = Number of transport NEs of type_1 x Equivalent coefficient of type_1 + ... + Number of transport NEs of type_n x Equivalent coefficient of type_n

NOTE

For example, there are 5 OptiX OSN 9500 (equivalent coefficient: 10), 10 OptiX OSN 7500 (equivalent coefficient: 6.5), and 100 OptiX OSN 3500 (equivalent coefficient: 4.5). Calculate the number of equivalent NEs in the transport domain as follows:

$$\text{Number of equivalent NEs in the transport domain} = 5 \times 10 + 10 \times 6.5 + 100 \times 4.5 = 565$$

The number of NEs that the U2000 can manage varies with what types of transport NEs are deployed and the equivalent coefficient assigned to each device. Equivalent coefficients of NEs in the transport domain are shown in **Table 11-3**.

Table 11-3 Equivalent coefficients of NEs in the U2000 transport domain

NE Series	NE Type	Equivalent Coefficient for the U2000
OSN series	OptiX OSN 50	0.5
	OptiX OSN 80	2
	OptiX OSN 500	1
	OptiX OSN 550	2.5
	OptiX OSN 580	4
	OptiX OSN 1500	2.5
	OptiX OSN 1500 (With ASON)	3.5
	OptiX OSN 2000	2
	OptiX OSN 2500	3.5
	OptiX OSN 2500REG	
	OptiX OSN 2500 (With ASON)	4.5
	OptiX OSN 2500REG (With ASON)	
	OptiX OSN 3500	4.5
	OptiX OSN 3500 (With ASON)	6.5
	OptiX OSN 3580	4.5
	OptiX OSN 7500	6.5
	OptiX OSN 7500 (With ASON)	10
	OptiX OSN 7500II	6.5
	OptiX OSN 9500	10
	OptiX OSN 9500 (With ASON)	15
	OptiX OSN 9560	20
	OptiX OSN 9560 (With ASON)	25
MSTP series	OptiX Metro 100	0.5
	OptiX Metro 200	0.5

NE Series	NE Type	Equivalent Coefficient for the U2000
OptiX Metro series	OptiX Metro 500	1
	OptiX 155/622H(Metro 1000)	1
	OptiX Metro 1000V3	1
	OptiX Metro 1050	1.5
	OptiX Metro 1100	1.5
	OptiX 155/622(Metro 2050)	2
	OptiX 2500+(Metro 3000)	3
	OptiX Metro 3100	3
	OptiX 10G(Metro 5000)	4
SDH series	OptiX 155C	1
	OptiX 155S	1
	OptiX 155/622B	2
	OptiX 2500	3
	OptiX 2500 REG	1.5
Metro WDM series	OptiX Metro 6020	1
	OptiX Metro 6040	1
	OptiX Metro 6040 V2	1
	OptiX Metro 6100	1.5
	OptiX Metro 6100V1	1.5
	OptiX Metro 6100V1E	1.5
	OptiX OSN 900A	1
LH WDM series	OptiX BWS OAS, OptiX BWS OCS, OptiX BWS OIS	1.5
	OptiX BWS 320GV3	1.5
	OptiX BWS 1600G Subrack	1.5*N N refers to the number of slave subracks
	OptiX BWS 1600G OLA Subrack	
Marine series	OptiX OTU40000	1
	OptiX SLM 1630	1

NE Series	NE Type	Equivalent Coefficient for the U2000
NG WDM series	OptiX PFE 1670	1
	OptiX BWS 1600S	1.5
	OptiX BWS 1600S T16	4
	HUAWEI OSN902	1
	OptiX OSN 1800	1
	OptiX OSN 1800 V Subrack	4*N N refers to the number of slave subracks
	OptiX OSN 1832 X8	1
	OptiX OSN 1832 X16	4
	OptiX OSN 3800	1.5
	OptiX OSN 3800 (With ASON)	3.5
	OptiX OSN 6800 Subrack	2*N N refers to the number of slave subracks
	OptiX OSN 6800 (With ASON) Subrack	4*N N refers to the number of slave subracks
	OptiX OSN 8800 Subrack	2*N N refers to the number of slave subracks
	OptiX OSN 8800 T16 Subrack	4*N N refers to the number of slave subracks
	OptiX OSN 8800 T16 (With ASON) Subrack	8*N N refers to the number of slave subracks
	OptiX OSN 8800 T32 Subrack	6*N N refers to the number of slave subracks
	OptiX OSN 8800 T32 (With ASON) Subrack	10*N N refers to the number of slave subracks
	OptiX OSN 8800 T64 Subrack	12*N N refers to the number of slave subracks

NE Series	NE Type	Equivalent Coefficient for the U2000
	OptiX OSN 8800 T64 (With ASON) Subrack	16*N N refers to the number of slave subracks
	OptiX OSN 9600 Subrack	2*N N refers to the number of slave subracks
	OptiX OSN 9600 (With ASON) Subrack	4*N N refers to the number of slave subracks
	OptiX OSN 9600 U16 Subrack	6*N N refers to the number of slave subracks
	OptiX OSN 9600 U16(With ASON) Subrack	10*N N refers to the number of slave subracks
	OptiX OSN 9600 U32 Subrack	10*N N refers to the number of slave subracks
	OptiX OSN 9600 U32 (With ASON) Subrack	14*N N refers to the number of slave subracks
	OptiX OSN 9600 U64 Subrack	20*N N refers to the number of slave subracks
	OptiX OSN 9600 U64 (With ASON) Subrack	24*N N refers to the number of slave subracks
	OptiX OSN 9800 Subrack	2*N N refers to the number of slave subracks
	OptiX OSN 9800 (With ASON) Subrack	4*N N refers to the number of slave subracks
	OptiX OSN 9800 U16 Subrack	6*N N refers to the number of slave subracks
	OptiX OSN 9800 U16(With ASON) Subrack	10*N N refers to the number of slave subracks

NE Series	NE Type	Equivalent Coefficient for the U2000
	OptiX OSN 9800 U32 Subrack	10*N N refers to the number of slave subracks
	OptiX OSN 9800 U32 (With ASON) Subrack	14*N N refers to the number of slave subracks
	OptiX OSN 9800 U64 Subrack	20*N N refers to the number of slave subracks
	OptiX OSN 9800 U64 (With ASON) Subrack	24*N N refers to the number of slave subracks
RTN series	OptiX RTN 310	0.5
	OptiX RTN 320	1
	OptiX RTN 380	1
	OptiX RTN 380e	1
	OptiX RTN 380H	1
	OptiX RTN 605	0.4
	OptiX RTN 610	0.4
	OptiX RTN 620	0.5
	OptiX RTN 905	0.5
	OptiX RTN 905e	0.5
	OptiX RTN 910	0.5
	OptiX RTN 910A	0.5
	OptiX RTN 950/950A	1
	OptiX RTN 980	2.5
	NEC 5000S	1
	OptiX RTN FlexPort80	1
	OptiX RTN 360	1
	OptiX RTN 980L	2.5
	PTP 250	1
	PTP 500	1
	PTP 650	1

NE Series	NE Type	Equivalent Coefficient for the U2000
	PMP 450	1
	X-1200	1
PTN series	OptiX PTN 1900	2.5
	OptiX PTN 3900	4.5
	OptiX PTN 3900-8	4
	OptiX PTN 912	0.5
	OptiX PTN 910	0.5
	OptiX PTN 910-F	0.4
	OptiX PTN 950	1
	OptiX PTN 960	1.5
	OptiX PTN 905	0.4
	OptiX PTN 905A	0.4
	OptiX PTN 905B	0.4
	OptiX PTN 905E	0.5
	OptiX PTN 906A	0.4
	OptiX PTN 906AI	0.4
	OptiX PTN 990	2.5
WDM (NA) series	OptiX PTN 6900	5
	OptiX PTN 7900-32	5.5
	OptiX PTN 7900-24	5
	OptiX PTN 7900-12	4.5
	OptiX PTN 970	2.5
	OptiX BWS 1600A	1.5
	OptiX BWS 1600G(NA)	1.5
	OptiX OSN 1800(NA)	1
	OptiX OSN 3800A	1.5
	OptiX OSN 6800A	2+2*N N refers to the number of slave subracks

NE Series	NE Type	Equivalent Coefficient for the U2000
	OptiX OSN 8800 T16(NA)	4+4*N N refers to the number of slave subracks
	OptiX OSN 8800 T32(NA)	6+6*N N refers to the number of slave subracks
	OptiX OSN 8800 T64(NA)	10+10*N N refers to the number of slave subracks
RTN (NA) series	OptiX RTN 910 (NA)	0.5
	OptiX RTN 950 (NA)	1

11.2.2 Equivalent NEs in the IP Domain

Number of equivalent NEs in the IP domain = Number of IP NEs of type_1 x Equivalent coefficient of type_1 + ... + Number of IP NEs of type_n x Equivalent coefficient of type_n.

NOTE

For example, there are 5 NE5000E (equivalent coefficient: 10), 200 S5300 (equivalent coefficient: 1.25), and 1000 CX200 (equivalent coefficient: 0.625). Calculate the number of equivalent NEs in the IP domain as follows:

$$\text{Number of equivalent NEs in the IP domain} = 5 \times 10 + 200 \times 1.25 + 1000 \times 0.625 = 925$$

The number of NEs that the U2000 can manage varies with which types of IP NEs are deployed and the equivalent coefficient assigned to each device. Equivalent coefficients of NEs in the IP domain are shown in [Table 11-4](#).

Table 11-4 Equivalent coefficients of NEs in the U2000 IP domain

NE Series	NE Type	Equivalent Coefficient for the U2000
Router	NE05/ NE08(E)/ NE16(E)	0.75
	NE05E-S/ NE05E-M	0.5
	NE08E-S/ NE08E-M	1.0

NE Series	NE Type	Equivalent Coefficient for the U2000
	NE20/ NE20E	1.25
	NE20E-S4	0.5
	NE20E-S8/S16	1.0
	NE20E-M2E/ NE20E-M2F	0.5
	NE40/NE80	5.0
	NE40E-X1	0.5
	NE40E-X2	1.0
	NE40E-X3	1.25
	NE40E-4	1.25
	NE40E-X8	2.5
	NE40E-8	2.5
	NE40E-X16	5.0
	NE40E-M2E/ NE40E-M2F	0.5
	NE80E	5.0
	NE5000E	10.0*N (N: number of chassis)
	AR150	0.125
	AR200	0.125
	AR1200/ AR2200/ AR3200/ AR3600	0.25
	NE16EX	0.25
	R series	1.0

NE Series	NE Type	Equivalent Coefficient for the U2000
	AR18/19/28 /29/46/49 series	0.25
	NE9000	10.0
	RM9000	1.0
Switch	S2000 series	0.125
	S2300 series	0.625
	S2700 series	0.625
	S3000 series	0.125
	S3300 series	0.75
	S3500 series	0.125
	S3700 series	0.75
	S3900 series	0.125
	S5000 series	0.25
	S5300 series	1.25
	S5500 series	0.25
	S5600 series	0.25
	S5700 series	1.25
	S6300 series	1.25
	S6500 series	0.75
	S6700 series	1.25
	S7800 series	1.25
	S8016 series	1.25
	S8500 series	1.25
	S7703 series	2.0
	S7706 series	3.5
	S7712 series	6.0

NE Series	NE Type	Equivalent Coefficient for the U2000
	S9303/ S9303E series	2.0
	S9306/ S9306E series	3.5
	S9312/ S9312E series	6.0
	S9700 series	6.0
	S12700 series	6.0
	E628 series	1.25
	E652 series	1.25
Data center switch	CE12804	6.0
	CE12808	8.0
	CE12812	10.0
	CE8800 series	1.25
	CE7800 series	1.25
	CE6800 series	1.25
	CE5800 series	1.25
PTN6900 series	PTN6900-1/ PTN6900-1-M4	0.5
	PTN6900-2/ PTN6900-2-M8/ PTN6900-2-M16	1.0
	PTN6900-3	1.25
	PTN6900-8	2.5

NE Series	NE Type	Equivalent Coefficient for the U2000
	PTN6900-16	5.0
ATN series	ATN910/910I/910B/910C	0.5
	ATN905	0.25
	ATN950	1.0
	ATN950B	1.0
	ATN950C	1.0
	ATN980	1.0
	ATN980B	1.0
	ATN990	1.0
ETN series	ETN 500	0.25
	ETN 550-A	1.0
MAN service platform	CX200 series	0.625
	CX300 series	1.25
	CX600-X1	0.5
	CX600-X2	1.0
	CX600-X3	1.25
	CX600-4	1.25
	CX600-X8	2.5
	CX600-8	2.5
	CX600-X16	5.0
	CX600-16	5.0
	CX600-M2E/CX600-M2F	0.5
	EGW2100 series	0.25

NE Series	NE Type	Equivalent Coefficient for the U2000
	EGW2200 series	0.25
	EGW3200 series	0.25
Firewall	Eudemon 300/500/1000	0.5
	Eudemon 100E	0.25
	NGFW	0.5
	Eudemon 200E-X	0.25
	Eudemon 200S	0.25
	Eudemon 1000E series	0.75
	Eudemon 1000E-X	0.75
	Eudemon 8040	3.0
	Eudemon 8080	6.0
	Eudemon 8080E	4.0
	Eudemon 8160E	8.0
	Eudemon 8000E-X3	1.5
	Eudemon 8000E-X8	4.0
	Eudemon 8000E-X16	8.0
	Eudemon 6080E	4.0
	NE40E-FW	4.0

NE Series	NE Type	Equivalent Coefficient for the U2000
	NE80E-FW	8.0
	vRouter6000V series	0.75
USG	USG9110	2.0
	USG9120	4.0
	USG9310	4.0
	USG9320	8.0
	USG9520	1.5
	USG9560	4.0
	USG9580	8.0
	USG5500 series	0.75
	USG5300 series	0.75
	USG5100 series	0.25
	USG3000	0.25
	USG2100 series	0.25
	USG2200 series	0.25
	USG50	0.25
SRG	SRG1200 series	0.25
	SRG20 series	0.25
	SRG2200 series	0.25
	SRG3200 series	0.25
	SRG1300 series	0.25

NE Series	NE Type	Equivalent Coefficient for the U2000
	SRG2300 series	0.25
	SRG3300 series	0.25
SIG	SIG9810	4.0
	SIG9820	8.0
	SIG9800-X3	1.5
	SIG9800-X8	4.0
	SIG9800-X16	8.0
	SIG Server	4.0
	URL Classify Server	0.25
	RADIUS Proxy	0.25
SeMG9811	SeMG9811-X3	1.5
	SeMG9811-X8	4.0
	SeMG9811-X16	8.0
NE-DPI	NE40E-DPI	4.0
	NE80E-DPI	8.0
	NE40E80E-DPI Server	4.0
	URL Classify Server-DPI	0.25
	RADIUS Proxy-DPI	0.25
SVN	SVN3000	0.25
	SVN2200	0.25

NE Series	NE Type	Equivalent Coefficient for the U2000
	SVN5300	0.75
	SVN5500	0.75
ASG	ASG2100	0.25
	ASG2200	0.25
	ASG2600	0.75
	ASG2800	0.75
NIP	NIP6600	0.75
CE-FWA	CE-FWA	0.75
CE-IPSA	CE-IPSA	0.75
OP-Bypass	OP-Bypass	0.25
iCache	iCache9200 RSS	1.0
	iCache9200 DSS	1.0
	iCache9200 MSS	1.0
	iCache9200 CSS-HTTP	1.0
	iCache9200 CSS-BT	1.0
	iCache9200 CSS-EM	1.0
	iCache9200 CSS-WEB	1.0
	iCache9200 CSS-PPS	1.0
	iCache9200 CSS-PPL	1.0
Broadband access	iCache9200 CSS-QQL	1.0
	MA5200E/F series	1.5

NE Series	NE Type	Equivalent Coefficient for the U2000
	MA5200G series	10.0
	ME60 series	10.0
	BGW9916	5.0
Voice gateway	VG1040/10 41 series	0.25
VNE1000	VNE1000 (Throughput < 500M)	0.25
	VNE1000 (500M <= Throughput < 5G)	0.75
	VNE1000 (5G <= Throughput < 20G)	1.25
	VNE1000 (20G <= Throughput < 100G)	2
VNE9000	VNE9000 (Throughput < 500M)	0.25
	VNE9000 (500M <= Throughput < 5G)	0.75
	VNE9000 (5G <= Throughput < 20G)	1.25
	VNE9000 (20G <= Throughput < 100G)	2

NE Series	NE Type	Equivalent Coefficient for the U2000
VSIG9800	VSIG9800 (Throughput < 500M)	0.25
	VSIG9800 (500M <= Throughput < 5G)	0.75
	VSIG9800 (5G <= Throughput < 20G)	1.25
	VSIG9800 (20G <= Throughput < 100G)	2

11.2.3 Equivalent NEs in the Access Domain

Number of equivalent NEs in the access domain = Number of FTTx OLT equivalent NEs + Number of FTTx MDU equivalent NEs + Number of MSAN equivalent NEs + Number of DSLAM equivalent NEs + Number of equivalent NEs of other access equipment

NOTE

The access capacity is commonly referred to as the number of lines. The number of ports is equal to the number of lines in **Table 11-5**. That is, one port indicates one line.

- Number of FTTx OLT equivalent NEs = Number of ONTs x Equivalent coefficient of ONTs + Number of MDUs x Equivalent coefficient of MDUs + Number of P2P ports x Equivalent coefficient of P2P ports
- Number of FTTx MDU equivalent NEs = Number of ports of type_1 x Equivalent coefficient of type_1 + ... + Number of ports of type_n x Equivalent coefficient of type_n
- Number of MSAN equivalent NEs = Number of ports of type_1 x Equivalent coefficient of type_1 + ... + Number of ports of type_n x Equivalent coefficient of type_n
- Number of DSLAM equivalent NEs = Number of ports of type_1 x Equivalent coefficient of type_1 + ... + Number of ports of type_n x Equivalent coefficient of type_n
- Number of equivalent NEs of other access equipment = Number of NEs of type_1 x Equivalent coefficient of type_1 + ... + Number of NEs of type_n x Equivalent coefficient of type_n

The number of NEs that the U2000 can manage varies with which types of access NEs are deployed and the equivalent coefficient assigned to each device. Equivalent coefficients of access NEs are shown in **Table 11-5**.

Table 11-5 Equivalent coefficients of NEs in the U2000 access domain

NE Series	Calculated based on	Equivalent Coefficient for the U2000
FTTx OLT (calculated based on the number of ONTs, MDUs, and P2P ports)	ONT in the P2MP scenario	1/80
	MDU in the P2MP scenario	1/32
	P2P port	1/64
FTTx MDU (calculated based on the number of user ports)	xDSL port	1/128
	E1 port	1/128
	ETH port	1/128
	POTS/ISDN BRA/ISDN PRA port	1/160
	CNU port	1/128
	G.fast port	1/128
	Serial port	1/64
MSAN (calculated based on the number of user ports)	xDSL port	1/128
	E1 port	1/128
	ETH port	1/128
	POTS/ISDN BRA/ISDN PRA port	1/160
DSLAM (calculated based on the number of user ports)	xDSL port	1/128
	E1 port	1/128
	ETH port	1/128
RPS (calculation based on the number of frames)	RPS frame	1/3
EDFA (calculation based on the number of NEs)	EDFA	1/3
CCU (calculation based on the number of CCUs)	CCU	1
Other NEs (calculated based on NE types)	BITS	1
	CMC (MA5633)	1
	CM	1/200
	Amplifier	1/40

11.3 Management Capabilities of Standard Delivery Models

The management capabilities of U2000 vary according to the standard delivery model.

NOTE

- [5.1.1 Hardware Configuration](#) and [5.2.1 Hardware Configuration](#) list the standard delivery models. If other models are used, Huawei does not guarantee that the U2000 can be properly installed, deployed, or run.
- Standard delivery models that meet the management capability requirements are recommended based on the number of equivalent NEs. If the number of physical NEs or equivalent NEs exceeds the maximum management capability, it is recommended that two standard delivery models that meet the management capability requirements be configured.
- Cross-domain management requires more advanced servers due to complex technologies involved.
- The SNMP-based performance collection capability complies with the following two conditions:
 - NEs must respond to collection requests sent from the U2000 in 0.05s. Otherwise, the actual performance collection capability compromises.
 - The performance collection capability listed in the following table is based on SNMPv1 and SNMPv2c. The SNMPv3-based performance collection capability achieves only two thirds. For example, on a large-scale network, the performance collection capability for SNMPv1 and SNMPv2c is 150,000, and for SNMPv3 is 100,000 when max/min data aggregation is disabled.

Management Capabilities

Table 11-6 Management capabilities of the U2000 on different hardware platforms

Management Capability (Number of Equivalent NEs)	Number of Clients	Service Capability	Performance Collection Capability
Small-scale network: less than 500 equivalent NEs	16	<ul style="list-style-type: none">● Transmission domain: 7500 SDH trails, 2500 WDM trails● IP domain: 25,000 IP SAIs, 2500 IP tunnels	<ul style="list-style-type: none">● SNMP collection (Max Equivalent Statistics Record/15 Minutes):<ul style="list-style-type: none">- 5,000 (Without Max/Min Data Aggregation Enabled)- 3,000 (With Max/Min Data Aggregation Enabled)● BULK collection (Max Equivalent Statistics Record/15 Minutes)<ul style="list-style-type: none">- IP equipment: 16,000- Access equipment: 66,000● Qx collection (Max Equivalent Statistics Record/15 Minutes): 5,000

Management Capability (Number of Equivalent NEs)	Number of Clients	Service Capability	Performance Collection Capability
<p>Common-scale network: 500-2000 equivalent NEs</p> <p>NOTE In Table 5-1, a maximum of 6000 equivalent NEs and 64 clients are supported when only access NEs are managed.</p>	32	<ul style="list-style-type: none"> ● Transmission domain: 30,000 SDH trails, 10,000 WDM trails ● IP domain: 100,000 IP SAIs, 10,000 IP tunnels 	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 20,000 (Without Max/Min Data Aggregation Enabled) - 13,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes) <ul style="list-style-type: none"> - IP equipment: 66,000 - Access equipment: 266,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 20,000
<p>Medium-scale network: 2000-6000 equivalent NEs</p> <p>NOTE In Table 5-1, a maximum of 15,000 equivalent NEs and 100 clients are supported when only access NEs are managed.</p>	64	<ul style="list-style-type: none"> ● Transmission domain: 90,000 SDH trails, 30,000 WDM trails ● IP domain: 300,000 IP SAIs, 30,000 IP tunnels 	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 60,000 (Without Max/Min Data Aggregation Enabled) - 40,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes) <ul style="list-style-type: none"> - IP equipment: 200,000 - Access equipment: 800,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 40,000
<p>Large-scale network: 6000-15000 equivalent NEs</p> <p>NOTE In Table 5-1, a maximum of 20,000 equivalent NEs and 300 clients are supported when only access NEs are managed.</p>	100	<ul style="list-style-type: none"> ● Transmission domain: 220,000 SDH trails, 70,000 WDM trails ● IP domain: 700,000 IP SAIs, 70,000 IP tunnels 	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data Aggregation Enabled) - 100,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes) <ul style="list-style-type: none"> - IP equipment: 500,000 - Access equipment: 2,000,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 80,000

Management Capability (Number of Equivalent NEs)	Number of Clients	Service Capability	Performance Collection Capability
Super-large-scale network: 15000-30000 equivalent NEs	200	<ul style="list-style-type: none"> ● Transmission domain: 500,000 SDH trails, 300,000 WDM trails ● IP domain: 1,500,000 IP SAIs, 150,000 IP tunnels 	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data Aggregation Enabled) - 100,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes) <ul style="list-style-type: none"> - IP equipment: 500,000 - Access equipment: 2,000,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 100,000

Configuration Example

Server configuration principles: Standard delivery models that meet the management capability requirements are recommended based on the number of equivalent NEs. If the number of physical NEs or equivalent NEs exceeds the maximum management capability, it is recommended that two standard delivery models that meet the management capability requirements be configured.

- **Configuration in the Case Where There Is Equipment in Only the Transport Domain**

As required by Operator X, 100 clients should be configured to manage 4000 OptiX OSN 1800, and 1000 OptiX OSN 3800 (with ASON). In this case, how to configure the NMS server?

The equivalent coefficient of the OptiX OSN 1800 is 1. The equivalent coefficient of the OptiX OSN 3800 (with ASON) is 3.5. The total number of equivalent NEs is 7500 ($1 \times 4000 + 3.5 \times 1000$). The total number of physical NEs is 5000 ($4000 + 1000$).

Recommended mainstream models that can manage 15,000 equivalent NEs:

RH5885H V3+disk array

- CPU: 4 x Xeon 10-core 2.0 GHz
- Memory: 128 GB
- Hard disk: 2 x 600 GB

Disk array: 48 GB memory, 12 x 600 GB or 16 GB memory, 12 x 600 GB

- **Configuration in the Case Where the Number of Physical NEs Exceeds the Maximum Management Capability of the U2000**

As required by Operator XX, 100 clients should be configured to manage 13000 S5000 switches and 10000 AR-series routers. In this case, how to configure the NMS server?

The equivalent coefficient of the S5000 is 0.25. The equivalent coefficient of the AR-series router is 0.25. The total number of equivalent NEs is $5750 (0.25 \times 13,000 + 0.25 \times 10,000)$. The total number of physical NEs is 23,000 ($13,000 + 10,000$). The total number of equivalent NEs to be managed is 5000, which does not exceed the maximum management capability of the U2000, that is, 30,000 equivalent NEs. The number of physical NEs, however, is 23000, which exceeds the maximum number of physical NEs that can be managed by the U2000, that is, 15000. In this case, multiple sets of the NMS should be configured.

Recommended mainstream models that can manage 6000 equivalent NEs:

RH5885H V3

- CPU: 4 x Xeon 10-core 2.0 GHz
- Memory: 64 GB
- Hard disk: 8 x 600 GB

● **Configuration in the Case Where the Number of Equivalent NEs Exceeds the Maximum Management Capability of the U2000**

As required by Operator XX, 100 clients should be configured to manage 3,000 NE5000E, 1000 S8500, and 2000 CX600-X16. In this case, how to configure the NMS server?

The equivalent coefficient of the NE5000E is 10. The equivalent coefficient of the S8500 is 1.25. The equivalent coefficient of the CX600-X16 is 5. The total number of equivalent NEs is $41250 (10 \times 3000 + 1.25 \times 1000 + 5 \times 2000)$. The total number of physical NEs is 6000 ($3000 + 1000 + 2000$). The total number of equivalent NEs exceeds the maximum management capability of the U2000, that is, 30,000 equivalent NEs. In this case, multiple sets of the NMS should be configured.

Recommended mainstream models that can manage 20,000 equivalent NEs:

RH5885H V3 + **disk array**

- CPU: 4 x E7-8860 18-Core 2.2 GHz
- Memory: 256 GB
- Hard disk: 2 x 600 GB

Disk array: 48 GB memory, 12 x 600 GB or 16 GB memory, 12 x 600 GB

11.4 Management Capabilities of Compatible Models

The management capabilities of U2000 vary according to the compatible model.

 **NOTE**

- If an incompatible model is used, Huawei does not guarantee that the U2000 can be properly installed, deployed, or run.
- The U2000 can be installed and upgraded on compatible server models.
If the management scale is close to the upper limit of the management capability, use the mainstream models that have the same management capability.
- Cross-domain management requires more advanced servers due to complex technologies involved.
- The SNMP-based performance collection capability complies with the following two conditions:
 - NEs must respond to collection requests sent from the U2000 in 0.05s. Otherwise, the actual performance collection capability compromises.
 - The performance collection capability listed in the following table is based on SNMPv1 and SNMPv2c. The SNMPv3-based performance collection capability achieves only two thirds. For example, on a large-scale network, the performance collection capability for SNMPv1 and SNMPv2c is 150,000, and for SNMPv3 is 100,000 when max/min data aggregation is disabled.

Management Capabilities (Compatible Models in Transport and IP Domains)

Table 11-7 Management capabilities of the U2000 on different hardware platforms

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Number of Clients	Service Capability	Performance Collection Capability
Common-scale network: less than 2000 equivalent NEs	IBM (supporting Windows or SUSE Linux OS)	X3650 M3(2 x 2.66GHZ/32G/6 x 300G)	32	<ul style="list-style-type: none"> ● Transmission domain: 30,000 SDH trails, 10,000 WDM trails ● IP domain: 100,000 IP SAIs, 10,000 IP tunnels 	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 20,000 (Without Max/Min Data Aggregation Enabled) - 13,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 66,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 20,000
	IBM (supporting Windows or SUSE Linux OS)	X3650 M4(2 x 2.5GHZ/32G/8 x 300G)			
	Huawei (supporting Windows or SUSE Linux OS)	Tecal RH2288HV2 <ul style="list-style-type: none"> ● CPU: 2 x Xeon 6-core 2.6 GHz ● Memory: 32 GB ● Hard disk: 8 x 300 GB 			

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Number of Clients	Service Capability	Performance Collection Capability
	Sun (supporting solaris OS)	Netra SPARC T4-1 <ul style="list-style-type: none"> ● CPU: 1 CPU (4-core) x 2.85 GHz ● Memory: 32 GB ● Hard disk: 4 x 600 GB 			
Medium-scale network: 2000-6000 equivalent NEs	IBM (supporting Windows or SUSE Linux OS)	X3850 X5(4 x 2.0GHZ/32G/8 x 300G)	64	<ul style="list-style-type: none"> ● Transmission domain: 90,000 SDH trails, 30,000 WDM trails ● IP domain: 300,000 IP SAIs, 30,000 IP tunnels 	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 60,000 (Without Max/Min Data Aggregation Enabled) - 40,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 200,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 20,000
	IBM (supporting Windows or SUSE Linux OS)	X3850 X5(4 x 2.0GHZ/32G/6 x 300G)			
	IBM (supporting Windows or SUSE Linux OS)	X3850 X5(4 x 2.66GHZ/32G/6 x 300G)			
	Huawei (supporting Windows or SUSE Linux OS)	RH5885H V3(E7 V2+DDR3) <ul style="list-style-type: none"> ● CPU: 4 x Xeon 8-core 2.0 GHz ● Memory: 32 GB ● Hard disk: 8 x 300 GB 			

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Number of Clients	Service Capability	Performance Collection Capability
	Huawei (supporting SUSE Linux OS)	RH5885H V3 <ul style="list-style-type: none"> ● CPU: 4 x Xeon 8-core 2.0 GHz ● Memory: 64 GB ● Hard disk: 8 x 300 GB 			<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 60,000 (Without Max/Min Data Aggregation Enabled) - 40,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 200,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 40,000
	Sun (supporting solaris OS)	Netra SPARC T4-1 <ul style="list-style-type: none"> ● CPU: 1 CPU (4-core) x 2.85 GHz ● Memory: 32 GB ● Hard disk: 4 x 600 GB 			
<ul style="list-style-type: none"> ● Transmission Domain: 10000 ● IP Domain (excluding PTN NEs): 10000 ● PTN NEs: 10000 	Sun (supporting solaris OS)	M4000(4*2.66GHz/32G/2*300G) + disk array (16 GB memory, 12 x 600 GB)	100	<ul style="list-style-type: none"> ● Transmission domain: 220,000 SDH trails, 70,000 WDM trails ● IP domain: 700,000 IP SAIs, 70,000 IP tunnels 	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 100,000 (Without Max/Min Data Aggregation Enabled) - 67,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Number of Clients	Service Capability	Performance Collection Capability
NOTE For multi-domain case, only 8000 equivalent NEs can be managed .	Sun (supporting solaris OS)	M4000(4*2.53GHz/32G/2*300G) + disk array (16 GB memory, 12 x 600 GB)			<p>Record/15 Minutes): 330,000</p> <ul style="list-style-type: none"> ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 40,000
<ul style="list-style-type: none"> ● IP Domain (excluding PTN NEs): 15000 ● PTN NEs: 15000 NOTE For multi-domain case, only 8000 equivalent NEs can be managed .	Sun (supporting solaris OS)	M4000(4*2.53GHz/64G/2*300G) + disk array (16 GB memory, 12 x 600 GB)	100	IP domain: 700,000 IP SAIs, 70,000 IP tunnels	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data Aggregation Enabled) - 100,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 500,000
Large-scale network: 6000-1500 equivalent NEs	IBM (supporting SUSE Linux OS)	X3850 X5(4*2.0GHZ/64G/2*300G) + disk array (16 GB memory, 12 x 600 GB)	100	<ul style="list-style-type: none"> ● Transmission domain: 220,000 SDH trails, 70,000 WDM trails 	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Number of Clients	Service Capability	Performance Collection Capability
	Huawei (supporting SUSE Linux OS)	RH5885H V3 + disk array <ul style="list-style-type: none"> ● CPU: 4 x Xeon 8-core 2.0 GHz ● Memory: 64 GB ● Hard disk: 2 x 300 GB disk array: 16 GB memory, 12 x 600 GB		<ul style="list-style-type: none"> ● IP domain: 700,000 IP SAIs, 70,000 IP tunnels 	<ul style="list-style-type: none"> ● Aggregation Enabled) <ul style="list-style-type: none"> - 100,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 500,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 40,000
	Huawei (supporting SUSE Linux OS)	RH5885H V3+ disk array <ul style="list-style-type: none"> ● CPU: 4 x Xeon 8-core 2.0 GHz ● Memory: 128 GB ● Hard disk: 2 x 300 GB disk array: 48 GB memory, 12 x 600 GB or 16 GB memory, 12 x 600 GB			<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data Aggregation Enabled) - 100,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 500,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 80,000

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Number of Clients	Service Capability	Performance Collection Capability
	Sun (supporting solaris OS)	Oracle SPARC T4-1 + disk array <ul style="list-style-type: none"> ● CPU: 1 CPU (8-core) x 2.85 GHz ● Memory: 64 GB ● Hard disk: 2 x 600 GB disk array:16 GB memory, 12 x 600 GB			
Super-large-scale network: 15000-20000 equivalent NEs	Sun (supporting solaris OS)	Netra SPARC T4-2 + disk array <ul style="list-style-type: none"> ● CPU: 2 CPU (8-core) x 2.85 GHz ● Memory: 128 GB ● Hard disk: 2 x 600 GB disk array:16 GB memory, 12 x 600 GB	<ul style="list-style-type: none"> ● Transmission domain: 300,000 SDH trails, 150,000 WDM trails ● IP domain: 1,000,000 IP SAIs, 100,000 IP tunnels 	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data Aggregation Enabled) - 100,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 500,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 100,000 	

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Number of Clients	Service Capability	Performance Collection Capability
	Sun (supporting solaris OS)	Oracle SPARC T4-2 + disk array <ul style="list-style-type: none"> ● CPU: 2 CPU (8-core) x 2.85 GHz ● Memory: 128 GB ● Hard disk: 2 x 600 GB disk array: 16 GB memory, 12 x 600 GB			<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data Aggregation Enabled) - 100,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 500,000 ● Qx collection (Max Equivalent Statistics Record/15 Minutes): 80,000
	Sun (supporting solaris OS)	M5000(8 x 2.66GHz/64G/2 x 300G) + disk array (16 GB memory, 12 x 600 GB)			
	Sun (supporting solaris OS)	M5000(8 x 2.53GHz/64G/2 x 300G) + disk array (16 GB memory, 12 x 600 GB)			
	Huawei (supporting SUSE Linux OS)	RH5885H V3 + disk array <ul style="list-style-type: none"> ● CPU: 4 x Xeon 12-core 3.0 GHz ● Memory: 128 GB ● Hard disk: 2 x 600 GB disk array: 48 GB memory, 12 x 600 GB or 16 GB memory, 12 x 600 GB			<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data Aggregation Enabled) - 100,000 (With Max/Min Data Aggregation Enabled)

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Number of Clients	Service Capability	Performance Collection Capability
	Huawei (supporting SUSE Linux OS)	RH5885H V3 + disk array <ul style="list-style-type: none">● CPU: 4 x Xeon 18-core 2.2 GHz● Memory: 128 GB● Hard disk: 2 x 600 GB disk array: 48 GB memory, 12 x 600 GB or 16 GB memory, 12 x 600 GB			<ul style="list-style-type: none">● BULK collection (Max Equivalent Statistics Record/15 Minutes): 500,000● Qx collection (Max Equivalent Statistics Record/15 Minutes): 100,000

Management Capabilities (Compatible Models in the Access Domain)

Table 11-8 Management capabilities of the U2000 on different hardware platforms

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain NMSs	Number of Clients	Performance Collection Capability
Common-scale network: less than 2000 equivalent NEs	IBM (supporting Windows or SUSE Linux OS)	X3650 M3(2 x 2.66GHZ/ 8G/ 6 x 300G)	No	16	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 5,000 (Without Max/Min Data Aggregation Enabled) - 3,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 66,000
	IBM (supporting Windows or SUSE Linux OS)	X3650 M3(2 x 2.66GHZ/ 16G/ 6 x 300G)	No	32	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 20,000 (Without Max/Min Data Aggregation Enabled) - 13,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 266,000
	SUN (supporting solaris OS)	Netra SPARC T4-1 <ul style="list-style-type: none"> ● CPU: 1 CPU (4-core) x 2.85 GHz ● Memory: 32 GB ● Hard disk: 4 x 600 GB 	Yes		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSS	Number of Clients	Performance Collection Capability
Medium-scale network: 2000-6000 equivalent NEs	IBM (supporting Windows or SUSE Linux OS)	X3650 M4(2 x 2.5GHZ/32 G/8 x 300G)	Yes NOTE For multi-domain case, only 2000 equivalent NEs and 32 clients can be managed.	64	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 60,000 (Without Max/Min Data Aggregation Enabled) - 40,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 800,000
	IBM (supporting Windows or SUSE Linux OS)	X3650 M3(2 x 2.66GHZ/ 32G/ 6 x 300G)	Yes NOTE For multi-domain case, only 2000 equivalent NEs and 32 clients can be managed.		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSs	Number of Clients	Performance Collection Capability
	SUN (supporting solaris OS)	<p>Netra SPARC T4-1</p> <ul style="list-style-type: none"> ● CPU: 1 CPU (4-core) x 2.85 GHz ● Memory: 32 GB ● Hard disk: 4 x 600 GB 	Yes		
	Huawei (supporting Windows or SUSE Linux OS)	<p>Tecal RH2288H V2</p> <ul style="list-style-type: none"> ● CPU: 2 x Xeon 6-core 2.6 GHz ● Memory: 32 GB ● Hard disk: 8 x 300 GB 	<p>Yes</p> <p>NOTE For multi-domain case, only 2000 equivalent NEs and 32 clients can be managed.</p>		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSS	Number of Clients	Performance Collection Capability
Large-scale network: 6000-15000 equivalent NEs	IBM (supporting SUSE Linux OS)	X3850 X5(4 x 2.0GHZ/32 G/8 x 300G)	Yes NOTE For multi-domain case, only 6000 equivalent NEs and 64 clients can be managed.	100	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data Aggregation Enabled) - 100,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 2,000,000
	IBM (supporting SUSE Linux OS)	X3850 X5(4 x 2.0GHZ/ 32G/ 6 x 300G)	Yes NOTE For multi-domain case, only 6000 equivalent NEs and 64 clients can be managed.		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSS	Number of Clients	Performance Collection Capability
	IBM (supporting SUSE Linux OS)	X3850 X5(4 x 2.66GHZ/ 32G/ 6 x 300G)	Yes NOTE For multi-domain case, only 6000 equivalent NEs and 64 clients can be managed.		
	Huawei (supporting Windows or SUSE Linux OS)	RH5885H V3(E7 V2+DDR3) <ul style="list-style-type: none"> ● CPU: 4 x Xeon 8-core 2.0 GHz ● Memory: 32 GB ● Hard disk: 8 x 300 GB 	Yes NOTE For multi-domain case, only 6000 equivalent NEs and 64 clients can be managed.		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSSs	Number of Clients	Performance Collection Capability
	Huawei (supporting SUSE Linux OS)	RH5885HV3 <ul style="list-style-type: none">● CPU: 4 x Xeon 8-core 2.0 GHz● Memory: 64 GB● Hard disk: 8 x 300 GB	Yes NOTE For multi-domain case, only 6000 equivalent NEs and 64 clients can be managed.		
	SUN (supporting solaris OS)	M4000(4 x 2.66GHz/ 32G/ 2 x 300G) + disk array (16 GB memory, 12 x 600 GB)	Yes NOTE For multi-domain case, only 8000 equivalent NEs can be managed.		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSSs	Number of Clients	Performance Collection Capability
	SUN (supporting solaris OS)	M4000(4 x 2.53GHz/ 32G/ 2 x 300G) + disk array (16 GB memory, 12 x 600 GB)	Yes NOTE For multi-domain case, only 8000 equivalent NEs can be managed.		
	SUN (supporting solaris OS)	Oracle SPARC T4-1 + disk array <ul style="list-style-type: none"> ● CPU: 1 CPU (8-core) x 2.85 GHz ● Memory: 64 GB ● Hard disk: 2 x 600 GB disk array: 16 GB memory, 12 x 600 GB	Yes		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSS	Number of Clients	Performance Collection Capability
Super-large-scale network: 15000-20000 equivalent NEs	IBM (supporting SUSE Linux OS)	X3850 X5 (4 x 2.0GHZ/64 G/2 x 300G) + disk array (16 GB memory, 12 x 600 GB)	Yes NOTE For multi-domain case, only 15000 equivalent NEs and 100 clients can be managed.	300	<ul style="list-style-type: none"> ● SNMP collection (Max Equivalent Statistics Record/15 Minutes): <ul style="list-style-type: none"> - 150,000 (Without Max/Min Data Aggregation Enabled) - 100,000 (With Max/Min Data Aggregation Enabled) ● BULK collection (Max Equivalent Statistics Record/15 Minutes): 2,000,000
	Huawei (supporting SUSE Linux OS)	RH5885H V3 + disk array <ul style="list-style-type: none"> ● CPU: 4 x Xeon 8-core 2.0 GHz ● Memory: 64 GB ● Hard disk: 2 x 300 GB disk array: 16 GB memory, 12 x 600 GB	Yes NOTE For multi-domain case, only 15000 equivalent NEs and 100 clients can be managed.		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSs	Number of Clients	Performance Collection Capability
	Huawei (supporting SUSE Linux OS)	RH5885H V3+disk array <ul style="list-style-type: none">● CPU: 4 x Xeon 8-core 2.0 GHz● Memory: 128 GB● Hard disk: 2 x 300 GB disk array: 48 GB memory, 12 x 600 GB or 16 GB memory, 12 x 600 GB	Yes NOTE For multi-domain case, only 15000 equivalent NEs and 100 clients can be managed.		
	Huawei (supporting SUSE Linux OS)	RH5885H V3 + disk array <ul style="list-style-type: none">● CPU: 4 x Xeon 12-core 3.0 GHz● Memory: 128 GB● Hard disk: 2 x 600 GB disk array: 48 GB memory, 12 x 600 GB or 16 GB memory, 12 x 600 GB	Yes NOTE For multi-domain case, only 100 clients can be managed.		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSs	Number of Clients	Performance Collection Capability
	Huawei (supporting SUSE Linux OS)	RH5885H V3 + disk array <ul style="list-style-type: none">● CPU: 4 x Xeon 18-core 2.2 GHz● Memory: 128 GB● Hard disk: 2 x 600 GB disk array: 48 GB memory, 12 x 600 GB or 16 GB memory, 12 x 600 GB	Yes NOTE For multi-domain case, only 100 clients can be managed.		
	SUN (supporting solaris OS)	M5000(8 x 2.66GHz/ 64G/ 2 x 300G) + disk array (16 GB memory, 12 x 600 GB)	Yes NOTE For multi-domain case, only 100 clients can be managed.		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSs	Number of Clients	Performance Collection Capability
	SUN (supporting solaris OS)	M5000(8 x 2.53GHz/ 64G/ 2 x 300G) + disk array (16 GB memory, 12 x 600 GB)	Yes NOTE For multi-domain case, only 100 clients can be managed.		
	SUN (supporting solaris OS)	Netra SPARC T4-2 + disk array <ul style="list-style-type: none"> ● CPU: 2 CPU (8-core) x 2.85 GHz ● Memory: 128 GB ● Hard disk: 2 x 600 GB disk array: 16 GB memory, 12 x 600 GB	Yes NOTE For multi-domain case, only 100 clients can be managed.		

Management Capability (Number of Equivalent NEs)	Software Platform of the Server	Hardware Configuration of the Server	Whether to Support Multi-Domain in NMSs	Number of Clients	Performance Collection Capability
	SUN (supporting solaris OS)	<p>Oracle SPARC T4-2 + disk array</p> <ul style="list-style-type: none"> ● CPU: 2 CPU (8-core) x 2.85 GHz ● Memory: 128 GB ● Hard disk: 2 x 600 GB <p>disk array: 16 GB memory, 12 x 600 GB</p>	<p>Yes</p> <p>NOTE For multi-domain case, only 100 clients can be managed.</p>		

12 Manageable NE

About This Chapter

This topic describes information about the NEs that the U2000 can manage. For the NEs to be managed, deployment instances need to be installed based on domains on the U2000, and the license for managing the NEs must be obtained.

For details about software that the U2000 can manage, click and see the following chapters.

Transport equipment:

- [MSTP Series Equipment](#)
- [WDM Series Equipment](#)
- [WDM \(NA\) Series Equipment](#)
- [Submarine Line Equipment](#)
- [RTN Series Equipment](#)
- [PTN Series Equipment \(Transport\)](#)

Access equipment:

- [FTTx Series Equipment](#)
- [D-CCAP Series Equipment](#)
- [MSAN Series Equipment](#)
- [DSLAM Series Equipment](#)
- [BITS/iSite/EDFA Series Equipment](#)

IP equipment:

- [PTN 6900 Equipment](#)
- [NE/ATN/CX/Multi-service gateways Series Equipment](#)
- [R/AR Series Equipment](#)
- [RM9000 Series Equipment](#)
- [Switch Equipment](#)
- [VoIP Gateway Equipment](#)
- [Security Series Equipment](#)

- **iCache Series Equipment**

12.1 MSTP Series Equipment

The following table lists the MSTP series NE supported.

Table 12-1 MSTP series equipment

Category	Equipment	Software Version	First U2000 Version Supported
OSN series	OptiX OSN 9560	5.51.05.20 (V100R002C00)	Earlier than U2000 V100R009C00
		5.51.06.10 (V100R005C00)	
		5.51.07.10 (V100R006C00)	
		5.51.07.30-5.51.07.59 (V100R006C01)	
		5.51.08.10 (V100R007C00)	
	OptiX OSN 9500	5.15.01.10	Earlier than U2000 V100R009C00
		5.15.01.20	
		5.15.01.30	
		5.15.02.10	
		5.15.02.11	
		5.15.02.20	
		5.15.03.20	
		5.15.03.26	
		5.15.03.30	
		5.15.04.10	
	OptiX OSN 7500 II	5.15.05.10	Earlier than U2000 V100R009C00
		5.15.06.10 (V100R006C00)	
		5.15.06.30 (V100R006C03)	
		5.15.06.50 (V100R006C05SPC200)	

Category	Equipment	Software Version	First U2000 Version Supported
		5.21.32.50 (V200R012C01)	
		5.21.33.10 (V200R013C00)	U2000 V100R009C00
		5.21.33.30 (V200R013C10)	U2000 V200R001C00
		5.21.33.50 (V200R013C20)	U2000 V200R014C50
		5.21.33.70 (V200R013C30)	U2000 V200R014C60
		5.21.34.10 (V200R015C00)	U2000 V200R015C50
		5.21.34.30 (V200R015C10)	U2000 V200R015C60
		5.21.34.60 (V200R015C20)	U2000 V200R016C50
	OptiX OSN 7500	5.21.13.40	Earlier than U2000 V100R009C00
		5.21.14.10	
		5.21.14.30-5.21.14.49	
		5.21.15.10-5.21.15.99	
		5.21.16.10	
		5.21.17.10	
		5.21.18.10 (V100R008C01)	
		5.21.18.40 (V100R008C02)	
		5.21.19.10 (V100R009C01)	
		5.21.19.40 (V100R009C02)	
		5.21.31.10 (V100R009C05)	
		5.21.20.10 (V100R010C00)	
		5.21.20.40 (V100R010C02)	
		5.21.20.50 (V100R010C03)	
		5.21.31.30 (V200R011C00)	
		5.21.31.50 (V200R011C01)	
		5.21.31.60 (V200R011C02)	
		5.21.31.70 (V200R011C03)	
		5.21.32.10 (V200R012C00)	
		5.21.32.50 (V200R012C01)	
		5.21.33.10 (V200R013C00)	U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
		5.21.33.30 (V200R013C10)	U2000 V200R001C00
		5.21.33.50 (V200R013C20)	U2000 V200R014C50
		5.21.33.70 (V200R013C30)	U2000 V200R014C60
		5.21.34.10 (V200R015C00)	U2000 V200R015C50
		5.21.34.30 (V200R015C10)	U2000 V200R015C60
		5.21.34.60 (V200R015C20)	U2000 V200R016C50
	OptiX OSN 3500	5.21.01.10	Earlier than U2000 V100R009C00
		5.21.12.10	
		5.21.12.40	
		5.21.13.40	
		5.21.14.10	
		5.21.14.30-5.21.14.49	
		5.21.15.10-5.21.15.99	
		5.21.16.10	
		5.21.17.10	
		5.21.18.10 (V100R008C01)	
		5.21.18.40 (V100R008C02)	
		5.21.18.44	
		5.21.19.10 (V100R009C01)	
		5.21.19.40 (V100R009C02)	
		5.21.30.10 (V100R009C03)	
		5.21.31.10 (V100R009C05)	
		5.21.20.10 (V100R010C00)	
		5.21.20.40 (V100R010C02)	
		5.21.20.50 (V100R010C03)	
		5.21.31.30 (V200R011C00)	
		5.21.31.50 (V200R011C01)	
		5.21.31.60 (V200R011C02)	
		5.21.31.70 (V200R011C03)	

Category	Equipment	Software Version	First U2000 Version Supported
	OptiX OSN 3580	5.21.32.10 (V200R012C00)	
		5.21.32.50 (V200R012C01)	
		5.21.33.10 (V200R013C00)	U2000 V100R009C00
		5.21.33.30 (V200R013C10)	U2000 V200R001C00
		5.21.33.50 (V200R013C20)	U2000 V200R014C50
		5.21.33.70 (V200R013C30)	U2000 V200R014C60
		5.21.34.10 (V200R015C00)	U2000 V200R015C50
		5.21.34.30 (V200R015C10)	U2000 V200R015C60
		5.21.34.60 (V200R015C20)	U2000 V200R016C50
		5.21.33.10 (V200R013C00)	U2000 V100R009C00
	OptiX OSN 2500	5.21.33.30 (V200R013C10)	U2000 V200R001C00
		5.21.33.50 (V200R013C20)	U2000 V200R014C50
		5.21.33.70 (V200R013C30)	U2000 V200R014C60
		5.21.34.10 (V200R015C00)	U2000 V200R015C50
		5.21.34.30 (V200R015C10)	U2000 V200R015C60
		5.21.34.60 (V200R015C20)	U2000 V200R016C50
		5.27.01.10	Earlier than U2000 V100R009C00
		5.27.12.10	
		5.36.12.10	
		5.36.12.40	
		5.36.13.40	
		5.36.14.10	
		5.36.14.30-5.36.14.49	
		5.36.15.10-5.36.15.99	
		5.36.16.10	
		5.36.17.10	
		5.36.18.10 (V100R008C01)	
		5.36.18.40 (V100R008C02)	
		5.36.19.10 (V100R009C01)	

Category	Equipment	Software Version	First U2000 Version Supported
		5.36.19.40 (V100R009C02)	
		5.36.20.10 (V100R010C00)	
		5.36.20.40 (V100R010C02)	
		5.36.20.50 (V100R010C03)	
	OptiX OSN 1500	5.36.11.10	Earlier than U2000 V100R009C00
		5.36.12.10	
		5.36.12.40	
		5.36.13.40	
		5.36.14.10	
		5.36.14.30-5.36.14.49	
		5.36.15.10-5.36.15.99	
		5.36.16.10	
		5.36.17.10	
		5.36.18.10 (V100R008C01)	
		5.36.18.40 (V100R008C02)	
		5.36.19.10 (V100R009C01)	
		5.36.19.40 (V100R009C02)	
		5.36.30.10 (V100R009C03)	
		5.36.20.10 (V100R010C00)	
		5.36.20.40 (V100R010C02)	
		5.36.20.50 (V100R010C03)	
		5.36.31.30 (V200R011C00)	
		5.36.31.50 (V200R011C01)	
		5.36.31.60 (V200R011C02)	
		5.36.31.70 (V200R011C03)	
		5.36.32.10 (V200R012C00)	
		5.36.32.50 (V200R012C01)	
		5.36.33.10 (V200R013C00)	U2000 V100R009C00
		5.36.33.30 (V200R013C10)	U2000 V200R001C00

Category	Equipment	Software Version	First U2000 Version Supported
OptiX OSN 2000	OptiX OSN 2000	5.36.33.50 (V200R013C20)	U2000 V200R014C50
		5.36.33.70 (V200R013C30)	U2000 V200R014C60
		5.36.34.10 (V200R015C00)	U2000 V200R015C50
		5.36.34.30 (V200R015C10)	U2000 V200R015C60
		5.36.34.60 (V200R015C20)	U2000 V200R016C50
	OptiX OSN 550	5.50.01.10	Earlier than U2000 V100R009C00
		5.50.02.10	
		5.50.02.20 (V100R002)	
		5.50.03.10 (V100R003)	
	OptiX OSN 550	5.81.03.10 (V100R003C00)	Earlier than U2000 V100R009C00
		5.81.05.10 (V100R005C00)	
		5.81.05.20 (V100R005C01)	
		5.81.05.30 (V100R005C02)	
		5.81.06.10 (V100R006C00)	
		5.81.06.20 (V100R006C01)	
		5.81.07.10 (V100R007C00)	
		5.81.07.20 (V100R007C10)	
		5.81.07.30 (V100R007C20)	
		5.81.07.40 (V100R007C30)	
		5.81.08.10 (V100R008C00)	
	OptiX OSN 500	5.81.08.20 (V100R008C10)	Earlier than U2000 V100R009C00
		5.81.08.30 (V100R008C20)	
		5.62.01.10	
		5.62.02.10	
		5.62.03.10 (V100R003C00)	
		5.62.05.10 (V100R005C00)	
		5.62.05.30 (V100R005C02)	
		5.62.06.10 (V100R006C00)	
		5.62.06.20 (V100R006C01)	

Category	Equipment	Software Version	First U2000 Version Supported
	OptiX OSN 2500REG	5.62.07.10 (V100R007C00)	U2000 V100R009C00
		5.62.07.20 (V100R007C10)	U2000 V200R001C00
		5.62.07.30 (V100R007C20)	U2000 V200R014C50
		5.62.07.40 (V100R007C30)	U2000 V200R014C60
		5.62.08.10 (V100R008C00)	U2000 V200R015C50
		5.62.08.20 (V100R008C10)	U2000 V200R015C60
		5.62.08.30 (V100R008C20)	U2000 V200R016C50
	OptiX OSN 50	5.43.13.10	Earlier than U2000 V100R009C00
		5.36.13.40	
		5.36.18.40	
	OptiX OSN 80	5.119.05.10 (V100R005C00)	Earlier than U2000 V100R009C00
	OptiX OSN 580	5.120.03.10 (V100R003C00)	Earlier than U2000 V100R009C00
		5.125.07.20 (V100R007C10)	U2000 V200R001C00
		5.125.07.30 (V100R007C20)	U2000 V200R014C50
		5.125.07.40 (V100R007C30)	U2000 V200R014C60
		5.125.08.10 (V100R008C00)	U2000 V200R015C50
		5.125.08.20 (V100R008C10)	U2000 V200R015C60
		5.125.08.30 (V100R008C20)	U2000 V200R016C50
SDH series	OptiX 155S	4.02.88.10	Earlier than U2000 V100R009C00
		4.02.88.20	
	OptiX 155C	4.04.00.08	Earlier than U2000 V100R009C00
		4.04.02.04	
	OptiX 155/622 (Metro 2050), OptiX 2500, OptiX 155/622B, OptiX 2500REG	4.01.16.20	Earlier than U2000 V100R009C00
		4.01.16.21	
		4.01.16.22	
		4.01.17.01	
		4.01.17.02	
		4.01.17.03	

Category	Equipment	Software Version	First U2000 Version Supported
		4.01.17.04	
		4.01.18.10	
	OptiX 155/622H, OptiX 155/622H (Metro 1000), OptiX 155A	4.02.05.04	Earlier than U2000 V100R009C00
		4.02.05.05	
		4.02.05.06	
		4.02.06.03	
		4.02.06.04	
		4.02.06.06	
		4.02.06.07	
		4.02.06.10	
		4.02.06.20	
		4.02.06.30	
		4.02.06.31	
		4.02.06.40	
		4.02.06.41	
		4.02.06.50	
		4.02.06.53	
		4.02.06.60	
	OptiX 2500+, OptiX 2500+ (Metro 3000)	4.05.03.02	Earlier than U2000 V100R009C00
		4.05.03.10	
		4.05.03.20	
		4.05.03.33	
		4.05.03.36	
		4.05.03.40	
		4.05.04.15	
		4.05.04.16	
		4.05.05.10	
		4.05.06.10	
		4.05.06.15	

Category	Equipment	Software Version	First U2000 Version Supported
		4.05.06.30	
		4.05.06.40	
		4.05.06.41	
		4.05.07.10	
		4.05.08.10	
		4.05.09.10	
		4.05.10.10	
	OptiX 10G MADM (Metro5000)	5.10.01.01	Earlier than U2000 V100R009C00
		5.10.01.10	
		5.10.01.20	
		5.10.02.10	
		5.10.03.10	
		5.10.04.10	
		5.10.04.30	
		5.10.04.35	
		5.10.04.40	
		5.10.05.10	
		5.10.05.20	
		5.10.06.10	
		5.10.06.30	
		5.10.06.40	
MSTP series	OptiX Metro 100	5.42.01.10	Earlier than U2000 V100R009C00
		5.42.01.20	
		5.42.01.30	
		5.42.02.10	
		5.42.03.10	
		5.42.03.20	
		5.42.05.10 (V100R005C00)	
	OptiX Metro 200	5.24.01.10	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
OptiX Metro 500		5.24.02.20	Earlier than U2000 V100R009C00
		5.24.03.10	
		5.24.04.10	
		5.24.04.20	
		5.17.01.10	
		5.17.01.20	
		5.24.02.20	
		5.24.03.10	
	OptiX Metro 1000V3	5.24.04.10	
		5.24.04.20	
		5.24.05.10	
		5.24.04.30	
	OptiX Metro 1050	5.37.01.10	Earlier than U2000 V100R009C00
		5.37.02.10	
		5.37.02.20	
		5.37.02.30	
		5.37.03.10 (V300R003)	
		5.37.04.10 (V300R004)	
		5.37.05.10 (V300R005)	
		5.37.06.10 (V300R006)	
		5.37.07.10 (V300R007C00)	
		5.37.07.20 (V300R007C01)	
		5.37.07.30 (V300R007C02)	

Category	Equipment	Software Version	First U2000 Version Supported
OptiX Metro 1100	OptiX Metro 1100	5.19.04.30	
		5.13.01.10	Earlier than U2000 V100R009C00
		5.13.01.11	
		5.13.02.20	
		5.13.02.30	
	OptiX Metro 3100	4.12.02.01	Earlier than U2000 V100R009C00
		4.12.02.02	
		4.12.02.10	
		4.12.02.15	
		4.12.02.20	
		4.12.03.10	
		4.12.03.20	

 **NOTE**

Mapping principle:

1. If the mapping table provides only the information that a.bb.cc.20 is supported by version A of the U2000, a.bb.cc.2x is supported by version A of the U2000.
2. If the mapping table provides only the information that a.bb.cc is supported by version A of the U2000, a.bb.cc.xx is supported by version A of the U2000.

Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product.

12.2 WDM Series Equipment

The following table lists the WDM series equipment supported.

Table 12-2 WDM Series Equipment

Category	Equipment	Software Version	First U2000 Version Supported
NG WDM series	OptiX OSN 1800 I/II	5.67.01.10(V100R001)	Earlier than U2000 V100R009C00
		5.67.01.20	
		5.67.02.10 (V100R002C00)	
		5.67.03.10 (V100R003C00)	

Category	Equipment	Software Version	First U2000 Version Supported
		5.67.03.20 (V100R003C01)	
		5.67.03.30 (V100R003C02)	
		5.67.03.40 (V100R003C03)	
		5.67.03.50 (V100R003C05)	
		5.67.03.20~5.67.03.90(V100R005C00)	U2000 V200R001C00
		5.67.03.20~5.67.03.90(F1SC C) (V100R005C20)	U2000 V200R014C60
		5.141.05.11(F3SCC) (V100R005C20)	
		5.67.03.20~5.67.03.90(F1SC C) (V100R006C00)	U2000 V200R015C50
		5.141.06.11(F3SCC) (V100R006C00)	
		5.67.03.86~5.67.03.87(F1SC C) (V100R006C10)	U2000 V200R015C60
		5.141.06.21(F3SCC) (V100R006C10)	
		5.67.03.88~5.67.03.89(F1SC C) (V100R006C20)	U2000 V200R016C50
		5.141.06.31(F3SCC) (V100R006C20)	
		5.153.07.11(F1SCC) (V100R007C00)	U2000 V200R016C60
		5.141.07.11(F3SCC) (V100R007C00)	
	HUAWEI OSN902	5.169.1.10(V100R001C00)	U2000 V200R016C60
	Optix OSN 1800 II(Packet)	5.67.03.91 (V100R003C05)	Earlier than U2000 V100R009C00
		5.67.05.11 (V100R005C00)	U2000 V200R001C00
		5.67.05.20 (V100R005C10)	U2000 V200R014C50
		5.67.05.30 (V100R005C20)	U2000 V200R014C60
		5.67.06.11 (V100R006C00)	U2000 V200R015C50
		5.67.06.21 (V100R006C10)	U2000 V200R015C60

Category	Equipment	Software Version	First U2000 Version Supported
OptiX OSN 1800V		5.67.06.31 (V100R006C20)	U2000 V200R016C50
		5.67.07.11 (V100R007C00)	U2000 V200R016C60
		5.67.03.60 (V100R003C05)	U2000 V100R009C00
		5.67.05.11 (V100R005C00)	U2000 V200R001C00
		5.67.05.20 (V100R005C10)	U2000 V200R014C50
		5.67.05.30 (V100R005C20)	U2000 V200R014C60
		5.67.06.11 (V100R006C00)	U2000 V200R015C50
		5.67.06.21 (V100R006C10)	U2000 V200R015C60
		5.67.06.31 (V100R006C20)	U2000 V200R016C50
		5.67.07.11 (V100R007C00)	U2000 V200R016C60
		5.67.03.60 (V100R003C05)	U2000 V100R009C00
		5.67.05.11 (V100R005C00)	U2000 V200R001C00
		5.67.05.20 (V100R005C10)	U2000 V200R014C50
		5.67.05.30 (V100R005C20)	U2000 V200R014C60
		5.67.06.11 (V100R006C00)	U2000 V200R015C50
		5.67.06.21 (V100R006C10)	U2000 V200R015C60
		5.67.06.31 (V100R006C20)	U2000 V200R016C50
		5.67.07.11 (V100R007C00)	U2000 V200R016C60
OptiX OSN 1832 X8		5.67.03.91 (V100R003C05)	U2000 V100R009C00
		5.67.05.11 (V100R005C00)	U2000 V200R001C00
		5.67.05.20 (V100R005C10)	U2000 V200R014C50
		5.67.05.30 (V100R005C20)	U2000 V200R014C60
		5.67.06.11 (V100R006C00)	U2000 V200R015C50
		5.67.06.21 (V100R006C10)	U2000 V200R015C60
		5.67.06.31 (V100R006C20)	U2000 V200R016C50
		5.67.07.11 (V100R007C00)	U2000 V200R016C60
	OptiX OSN 1832	5.51.08.10 (V100R007C00)	Earlier than U2000 V100R009C00
		5.51.08.30 (V100R007C02)	
		5.51.09.10 (V100R008C00)	U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
		5.51.09.30 (V100R008C10)	U2000 V200R014C50
		5.51.10.10 (V100R009C00)	U2000 V200R014C60
		5.51.10.30 (V100R009C10)	U2000 V200R014C60
		5.51.11.10 (V100R010C00)	U2000 V200R015C50
		5.51.11.30 (V100R010C10)	U2000 V200R015C60
		5.51.12.10 (V100R011C00)	U2000 V200R016C50
		5.51.12.30 (V100R011C10)	U2000 V200R016C60
	OptiX OSN 3800	5.52.01.10	Earlier than U2000 V100R009C00
		5.52.02.10	
		5.52.03.20	
		5.52.04.10	
		5.52.04.20 (V100R004C02)	
		5.52.04.30 (V100R004C03)	
		5.52.05.20 (V100R004C04)	
		5.51.06.10 (V100R005C00)	
		5.51.07.10 (V100R006C00)	
		5.51.07.30 (V100R006C01)	
		5.51.07.60 (V100R006C03)	
		5.51.08.10 (V100R007C00)	
		5.51.08.30 (V100R007C02)	
		5.51.09.10 (V100R008C00)	U2000 V100R009C00
		5.51.09.30 (V100R008C10)	U2000 V200R014C50
		5.51.10.10 (V100R009C00)	U2000 V200R014C60
		5.51.10.30 (V100R009C10)	
		5.51.11.10 (V100R010C00)	U2000 V200R015C50
		5.51.11.30 (V100R010C10)	U2000 V200R015C60
		5.51.12.10 (V100R011C00)	U2000 V200R016C50
		5.51.12.30 (V100R011C10)	U2000 V200R016C60
	OptiX OSN 6800	5.51.01.10	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
		5.51.02.10	
		5.51.03.20	
		5.51.04.10	
		5.51.04.20 (V100R004C02)	
		5.52.04.30 (V100R004C03)	
		5.51.05.20 (V100R004C04)	
		5.51.06.10 (V100R005C00)	
		5.51.07.10 (V100R006C00)	
		5.51.07.30 (V100R006C01)	
		5.51.07.60 (V100R006C03)	
		5.51.08.10 (V100R007C00)	
		5.51.08.30 (V100R007C02)	
		5.51.09.10 (V100R008C00)	U2000 V100R009C00
		5.51.09.30 (V100R008C10)	U2000 V200R014C50
		5.51.10.10 (V100R009C00)	U2000 V200R014C60
		5.51.10.30 (V100R009C10)	
		5.51.11.10 (V100R010C00)	U2000 V200R015C50
		5.51.11.30 (V100R010C10)	U2000 V200R015C60
		5.51.12.10 (V100R011C00)	U2000 V200R016C50
		5.51.12.30 (V100R011C10)	U2000 V200R016C60
	OptiX OSN 8800 T16	5.51.07.10 (V100R006C00)	Earlier than U2000 V100R009C00
		5.51.07.30 (V100R006C01)	
		5.51.07.60 (V100R006C03)	
		5.51.08.10 (V100R007C00)	
		5.51.08.30 (V100R007C02)	
		5.51.09.10 (V100R008C00)	U2000 V100R009C00
		5.51.09.30 (V100R008C10)	U2000 V200R014C50
		5.51.10.10 (V100R009C00)	U2000 V200R014C60
		5.51.10.30 (V100R009C10)	

Category	Equipment	Software Version	First U2000 Version Supported
		5.51.11.10 (V100R010C00)	U2000 V200R015C50
		5.51.11.30 (V100R010C10)	U2000 V200R015C60
		5.51.12.10 (V100R011C00)	U2000 V200R016C50
		5.51.12.30 (V100R011C10)	U2000 V200R016C60
	OptiX OSN 8800 T32	5.51.04.20 (V100R001C01)	Earlier than U2000 V100R009C00
		5.51.04.30 (V100R001C02)	
		5.51.05.20 (V100R002C00)	
		5.51.05.21 (V100R002C02)	
		5.51.06.10 (V100R005C00)	
		5.51.07.10 (V100R006C00)	
		5.51.07.30 (V100R006C01)	
		5.51.07.60 (V100R006C03)	
		5.51.08.10 (V100R007C00)	
		5.51.08.30 (V100R007C02)	
		5.51.09.10 (V100R008C00)	U2000 V100R009C00
		5.51.09.30 (V100R008C10)	U2000 V200R014C50
		5.51.10.10 (V100R009C00)	U2000 V200R014C60
		5.51.10.30 (V100R009C10)	
		5.51.11.10 (V100R010C00)	U2000 V200R015C50
		5.51.11.30 (V100R010C10)	U2000 V200R015C60
		5.51.12.10 (V100R011C00)	U2000 V200R016C50
		5.51.12.30 (V100R011C10)	U2000 V200R016C60
	OptiX OSN 8800 T64	5.51.05.20 (V100R002C00)	Earlier than U2000 V100R009C00
		5.51.05.21 (V100R002C02)	
		5.51.06.10 (V100R005C00)	
		5.51.07.10 (V100R006C00)	
		5.51.07.30 (V100R006C01)	
		5.51.07.60 (V100R006C03)	
		5.51.08.10 (V100R007C00)	

Category	Equipment	Software Version	First U2000 Version Supported
		5.51.08.30 (V100R007C02)	
		5.51.09.10 (V100R008C00)	U2000 V100R009C00
		5.51.09.30 (V100R008C10)	U2000 V200R014C50
		5.51.10.10 (V100R009C00)	U2000 V200R014C60
		5.51.10.30 (V100R009C10)	
		5.51.11.10 (V100R010C00)	U2000 V200R015C50
		5.51.11.30 (V100R010C10)	U2000 V200R015C60
		5.51.12.10 (V100R011C00)	U2000 V200R016C50
		5.51.12.30 (V100R011C10)	U2000 V200R016C60
		5.51.08.10 (V100R007C00)	Earlier than U2000 V100R009C00
	OptiX OSN 8800	5.51.08.30 (V100R007C02)	
		5.51.09.10 (V100R008C00)	U2000 V100R009C00
		5.51.09.30 (V100R008C10)	U2000 V200R014C50
		5.51.10.10 (V100R009C00)	U2000 V200R014C60
		5.51.10.30 (V100R009C10)	
		5.51.11.10 (V100R010C00)	U2000 V200R015C50
		5.51.11.30 (V100R010C10)	U2000 V200R015C60
		5.51.12.10 (V100R011C00)	U2000 V200R016C50
		5.51.12.30 (V100R011C10)	U2000 V200R016C60
		5.51.08.15 (V100R001C00)	U2000 V100R009C00
	OptiX OSN 9600	5.51.09.17 (V100R001C01)	U2000 V200R014C50
		5.51.09.33 (V100R001C20)	U2000 V200R014C60
		5.51.10.13 (V100R001C30)	
		5.51.11.13 (V100R002C10)	U2000 V200R015C50
		5.51.11.31 (V100R003C00)	U2000 V200R015C60
		5.51.12.11 (V100R003C10)	U2000 V200R016C50
		5.51.12.17 (V100R005C00)	U2000 V200R016C60
		5.111.01.80 (V100R001C30)	U2000 V200R014C60
	OptiX OSN 9600 U16	5.111.02.30 (V100R002C10)	U2000 V200R015C50

Category	Equipment	Software Version	First U2000 Version Supported
OptiX OSN 9600	OptiX OSN 9600 U32	5.111.03.10 (V100R003C00)	U2000 V200R015C60
		5.111.03.30 (V100R003C10)	U2000 V200R016C50
		5.111.05.10 (V100R005C00)	U2000 V200R016C60
	OptiX OSN 9600 U64	5.111.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
		5.111.01.30 (V100R001C01)	U2000 V100R009C00
		5.111.01.60 (V100R001C20)	U2000 V200R001C00
		5.111.01.80 (V100R001C30)	U2000 V200R014C60
		5.111.02.30 (V100R002C10)	U2000 V200R015C50
		5.111.03.10 (V100R003C00)	U2000 V200R015C60
		5.111.03.30 (V100R003C10)	U2000 V200R016C50
		5.111.05.10 (V100R005C00)	U2000 V200R016C60
		5.111.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
OptiX OSN 9800	OptiX OSN 9800	5.111.01.30 (V100R001C01)	U2000 V100R009C00
		5.111.01.60 (V100R001C20)	U2000 V200R001C00
		5.111.01.80 (V100R001C30)	U2000 V200R014C60
		5.111.02.30 (V100R002C10)	U2000 V200R015C50
		5.111.03.10 (V100R003C00)	U2000 V200R015C60
		5.111.03.30 (V100R003C10)	U2000 V200R016C50
		5.111.05.10 (V100R005C00)	U2000 V200R016C60
		5.51.08.15 (V100R001C00)	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
OptiX OSN 9800	OptiX OSN 9800 U16	5.111.01.80 (V100R001C30)	U2000 V200R014C60
		5.111.02.30 (V100R002C10)	U2000 V200R015C50
		5.111.03.10 (V100R003C00)	U2000 V200R015C60
		5.111.03.30 (V100R003C10)	U2000 V200R016C50
		5.111.05.10 (V100R005C00)	U2000 V200R016C60
	OptiX OSN 9800 U32	5.111.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
		5.111.01.30 (V100R001C01)	U2000 V100R009C00
		5.111.01.60 (V100R001C20)	U2000 V200R001C00
		5.111.01.80 (V100R001C30)	U2000 V200R014C60
		5.111.02.30 (V100R002C10)	U2000 V200R015C50
		5.111.03.10 (V100R003C00)	U2000 V200R015C60
		5.111.03.30 (V100R003C10)	U2000 V200R016C50
		5.111.05.10 (V100R005C00)	U2000 V200R016C60
	OptiX OSN 9800 U64	5.111.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
		5.111.01.30 (V100R001C01)	U2000 V100R009C00
		5.111.01.60 (V100R001C20)	U2000 V200R001C00
		5.111.01.80 (V100R001C30)	U2000 V200R014C60
		5.111.02.30 (V100R002C10)	U2000 V200R015C50
		5.111.03.10 (V100R003C00)	U2000 V200R015C60
		5.111.03.30 (V100R003C10)	U2000 V200R016C50
		5.111.05.10 (V100R005C00)	U2000 V200R016C60
Metro WDM series & LH WDM series	OptiX BWS 320G (OAS/OCI/OIS)	4.08.04.04	Earlier than U2000 V100R009C00
		4.08.04.05	
		4.08.04.10	
		4.08.04.20	
	OptiX BWS 320GV3	5.08.01.30	Earlier than U2000 V100R009C00
		5.08.02.10	
		5.08.02.20	

Category	Equipment	Software Version	First U2000 Version Supported
		5.08.03.10	
	OptiX BWS 1600G	5.08.01.20	Earlier than U2000 V100R009C00
		5.08.01.30	
		5.08.02.20	
		5.08.02.21	
		5.08.02.22	
		5.08.02.23	
		5.08.03.10	
		5.08.03.11	
		5.08.04.10	
		5.08.03.70-5.08.03.99(V100R003GA')	
		5.08.05.10(V100R005)	
		5.08.06.10(V100R006)	
		5.08.06.20	
		5.08.06.40	
		5.08.07.10 (V100R007C01)	
		5.08.07.20 (V100R007C02)	
		5.08.07.30 (V100R007C03)	
	OptiX BWS 1600G OLA	5.08.04.10	Earlier than U2000 V100R009C00
		5.08.05.10	
		5.08.06.10	
		5.08.06.40	
		5.08.07.10 (V100R007C01)	
		5.08.07.20 (V100R007C02)	
		5.08.07.30 (V100R007C03)	
	OptiX OTU40000	V2.0	Earlier than U2000 V100R009C00
	OptiX Metro 6020	5.04.01.03	Earlier than U2000 V100R009C00

Categor y	Equipment	Software Version	First U2000 Version Supported
	OptiX Metro 6040	5.18.01.10 5.18.01.20	Earlier than U2000 V100R009C00
	OptiX Metro 6040V2	5.26.01.10 5.26.01.20 5.26.01.30 5.39.01.30 5.39.01.40 5.39.01.42 5.39.02.10 (V100R006) 5.39.02.20 (V100R006C02) 5.39.03.10 (V100R007C01) 5.39.03.20 (V100R007C02) 5.39.03.33 (V100R007C03) 5.39.03.61 5.39.04.10 (V100R008C01)	Earlier than U2000 V100R009C00
	OptiX Metro 6100	4.09.02.03 4.09.02.05	Earlier than U2000 V100R009C00
	OptiX Metro 6100V1	5.08.01.40 5.08.02.10 5.08.02.20 5.08.02.21 5.08.02.22 5.08.03.10	Earlier than U2000 V100R009C00
	OptiX Metro 6100V1E	5.39.01.10 5.39.01.20 5.39.01.40 5.39.01.42 5.39.02.10 (V100R006) 5.39.02.20 (V100R006C02)	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
		5.39.03.10 (V100R007C01)	
		5.39.03.20 (V100R007C02)	
		5.39.03.33 (V100R007C03)	
		5.39.03.61	
		5.39.04.10 (V100R008C01)	
		5.39.05.10 (V100R008C04)	
	OptiX OSN 900A	5.53.01.10	Earlier than U2000 V100R009C00

NOTE

- Different from OptiX OSN 8800 T32 and other devices, OptiX OSN 8800 is a platform-based device.
- Different from OptiX OSN 9600 U32 and other devices, OptiX OSN 9600 is a platform-based device.
- Different from OptiX OSN 9800 U32 and other devices, OptiX OSN 9800 is a platform-based device.
- The distributed U2000 System does not support OptiX OSN 9600/9800 series.
- The OptiX BWS 1600G OLA is an independent power supply subrack. It is supported by the OptiX BWS 1600G backbone DWDM optical transmission system V100R004 and later versions.
- Mapping principle:
 1. If the mapping table provides only the information that a.bb.cc.20 is supported by version A of the U2000, a.bb.cc.2x is supported by version A of the U2000.
 2. If the mapping table provides only the information that a.bb.cc is supported by version A of the U2000, a.bb.cc.xx is supported by version A of the U2000.

Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product.

12.3 WDM (NA) Series Equipment

The following table lists the WDM (NA) series equipment supported.

NOTE

For the OptiX OSN 8800 (NA) series equipment, the version mapping is the same as the OptiX OSN 8800 series equipment. Refer to [12.2 WDM Series Equipment](#).

Table 12-3 LH WDM series

Category	Equipment	Latest Version
LH WDM series	OptiX BWS 1600A	5.44.01.10

Category	Equipment	Latest Version
		5.44.02.10
		5.44.03.10
		5.44.03.20 (V100R003C02)
	OptiX BWS 1600G (NA)	5.44.01.10
		5.44.02.10
		5.44.03.10
		5.44.03.20 (V100R003C02)

Table 12-4 NA WDM series

Category	Equipment	Latest Version
NA WDM series	OptiX OSN 1800 (NA)	5.66.01.10 (V100R001C01)
		5.67.02.10 (V100R002C00)
		5.67.03.10 (V100R003C00)
		5.67.03.20 (V100R003C01)
		5.67.03.30 (V100R003C02)
		5.67.03.40 (V100R003C03)
		5.67.03.50 (V100R003C05)
		5.67.03.20~5.67.03.90 (V100R005C00)
	OptiX OSN 3800A	5.70.01.19 (V100R001C01)
		5.70.01.20 (V100R001C01)
		5.70.01.40 (V100R001C02)
		5.51.06.10 (V100R005C00)
		5.51.07.10 (V100R006C00)
		5.51.07.30 (V100R006C01)
		5.51.07.60 (V100R006C03)
		5.51.08.10 (V100R007C00)
		5.51.08.30 (V100R007C02)
		5.51.09.10 (V100R008C00)
		5.51.09.30 (V100R008C10)

Category	Equipment	Latest Version
		5.51.10.10 (V100R009C00)
		5.51.10.30 (V100R009C10)
	OptiX OSN 6800A	5.71.01.19 (V100R001C01)
		5.71.01.20 (V100R001C01)
		5.71.01.40 (V100R001C02)
		5.51.06.10 (V100R005C00)
		5.51.07.10 (V100R006C00)
		5.51.07.30 (V100R006C01)
		5.51.07.60 (V100R006C03)
		5.51.08.10 (V100R007C00)
		5.51.08.30 (V100R007C02)
		5.51.09.10 (V100R008C00)
		5.51.09.30 (V100R008C10)
		5.51.10.10 (V100R009C00)
		5.51.10.30 (V100R009C10)

NOTE

Mapping principle:

1. If the mapping table provides only the information that a.bb.cc.20 is supported by version A of the U2000, a.bb.cc.2x is supported by version A of the U2000.
2. If the mapping table provides only the information that a.bb.cc is supported by version A of the U2000, a.bb.cc.xx is supported by version A of the U2000.

Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product.

12.4 Submarine Line Equipment

The following table lists the submarine line equipment supported.

Table 12-5 Submarine line equipment

Equipment	Software Version	First U2000 Version Supported
OptiX BWS 1600S	5.56.01.10	Earlier than U2000 V100R009C00

Equipment	Software Version	First U2000 Version Supported
	5.56.02.10	
	5.56.03.10 (V100R003)	
	5.56.05.10-5.56.05.15 (V100R005C00)	
	5.56.05.16 (V100R005C01)	
	5.56.06.10 (V100R006C00)	
	5.56.07.11 (V100R007C00)	U2000 V200R014C50
OptiX BWS 1600S T16	5.51.08.10 (V100R006C00)	U2000 V200R001C00
	5.51.09.31 (V100R007C00)	U2000 V200R014C50
	5.51.11.10 (V100R008C00)	U2000 V200R015C50
	5.51.11.20 (V100R008C10)	U2000 V200R015C60
SLM 1630	5.61.01.10	Earlier than U2000 V100R009C00
	5.61.01.20 (V100R001C02)	
	5.61.02.10 (V100R002C00)	
	5.61.02.20 (V100R002C00)	
	5.61.03.10 (V100R003C00)	
SLM 1630 P16	5.181.03.01 (V100R003C00)	U2000 V200R016C60
PFE 1670	5.72.01.17 (V100R001C01)	U2000 V200R014C60

NOTE

Mapping principle:

1. If the mapping table provides only the information that a.bb.cc.20 is supported by version A of the U2000, a.bb.cc.2x is supported by version A of the U2000.
2. If the mapping table provides only the information that a.bb.cc is supported by version A of the U2000, a.bb.cc.xx is supported by version A of the U2000.

Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product.

12.5 RTN Series Equipment

The following table lists the RTN series equipment supported.

Table 12-6 RTN series equipment

Category	Equipment	Software Version	First U2000 Version Supported
RTN series	OptiX RTN 605	5.60.01.10 (V100R001)	Earlier than U2000 V100R009C00
		5.60.03.10 (V100R003)	
		5.60.05.10 (V100R005)	
		5.60.03.30 (V100R003C02)	U2000 V100R009C00
	OptiX RTN 610	5.54.01.10	Earlier than U2000 V100R009C00
		5.54.01.20	
		5.54.02.10	
		5.54.03.10 (V100R003)	
	OptiX RTN 620	5.54.01.10	Earlier than U2000 V100R009C00
		5.54.01.20	
		5.54.02.10	
		5.54.03.10 (V100R003)	
		5.54.05.10 (V100R005)	
		5.54.05.20 (V100R005C01)	
		5.54.05.30 (V100R005C02)	U2000 V100R009C00
	OptiX RTN 905	5.95.05.10 (V100R005C00)	Earlier than U2000 V100R009C00
		5.95.05.20 (V100R005C01)	
		5.95.06.10 (V100R006C00)	U2000 V100R009C00
		5.95.06.20 (V100R006C10)	U2000 V200R001C00
		5.95.07.10 (V100R007C00)	U2000 V200R014C50

Category	Equipment	Software Version	First U2000 Version Supported
		5.95.07.20 (V100R007C10)	U2000 V200R014C60
		5.95.08.10 (V100R008C00)	U2000 V200R015C50
		5.95.08.20 (V100R008C10)	U2000 V200R015C60
		5.95.09.10 (V100R009C00)	U2000 V200R016C50
		5.95.09.20 (V100R009C10)	U2000 V200R016C60
	OptiX RTN 905e	5.183.09.20 (V100R009C10)	U2000 V200R016C60
	OptiX RTN 910	5.76.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
		5.76.01.20 (V100R001C01)	
		5.76.01.30 (V100R001C02)	
		5.76.01.40 (V100R001C03)	
		5.76.02.10 (V100R002C00)	
		5.76.02.20 (V100R002C01)	
		5.76.03.10 (V100R003C00)	
		5.76.03.20 (V100R003C01)	
		5.76.03.30 (V100R003C02)	
		5.76.03.40 (V100R003C03)	
		5.76.05.10 (V100R005C00)	
		5.76.05.20 (V100R005C01)	

Category	Equipment	Software Version	First U2000 Version Supported
		5.76.06.10 (V100R006C00)	U2000 V100R009C00
	OptiX RTN 910A	5.152.08.10 (V100R008C00)	U2000 V200R015C50
		5.152.08.20 (V100R008C10)	U2000 V200R015C60
		5.152.09.10 (V100R009C00)	U2000 V200R016C50
		5.152.09.20 (V100R009C10)	U2000 V200R016C60
	OptiX RTN 950	5.76.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
		5.76.01.20 (V100R001C01)	
		5.76.01.30 (V100R001C02)	
		5.76.01.40 (V100R001C03)	
		5.76.02.10 (V100R002C00)	
		5.76.02.20 (V100R002C01)	
		5.76.03.10 (V100R003C00)	
		5.76.03.20 (V100R003C01)	
		5.76.03.30 (V100R003C02)	
		5.76.03.40 (V100R003C03)	
		5.76.05.10 (V100R005C00)	
		5.76.05.20 (V100R005C01)	
		5.76.06.10 (V100R006C00)	U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
		5.76.06.20 (V100R006C10)	U2000 V200R001C00
		5.76.07.10 (V100R007C00)	U2000 V200R014C50
		5.76.07.20 (V100R007C10)	U2000 V200R014C60
		5.76.08.10 (V100R008C00)	U2000 V200R015C50
		5.76.08.20 (V100R008C10)	U2000 V200R015C60
		5.76.09.10 (V100R009C00)	U2000 V200R016C50
		5.76.09.20 (V100R009C10)	U2000 V200R016C60
	OptiX RTN 950A	5.114.05.20 (V100R005C01)	Earlier than U2000 V100R009C00
		5.114.06.10 (V100R006C00)	U2000 V100R009C00
		5.114.06.20 (V100R006C10)	U2000 V200R001C00
		5.114.07.10 (V100R007C00)	U2000 V200R014C50
		5.114.07.20 (V100R007C10)	U2000 V200R014C60
		5.114.08.10 (V100R008C00)	U2000 V200R015C50
		5.114.08.20 (V100R008C10)	U2000 V200R015C60
	OptiX RTN 980	5.114.09.10 (V100R009C00)	U2000 V200R016C50
		5.114.09.20 (V100R009C10)	U2000 V200R016C60

Category	Equipment	Software Version	First U2000 Version Supported
		5.83.03.40 (V100R003C03)	
		5.83.05.10 (V100R005C00)	
		5.83.05.20 (V100R005C01)	
		5.83.06.10 (V100R006C00)	U2000 V100R009C00
		5.83.06.20 (V100R006C10)	U2000 V200R001C00
		5.83.07.10 (V100R007C00)	U2000 V200R014C50
		5.83.07.20 (V100R007C10)	U2000 V200R014C60
		5.83.08.10 (V100R008C00)	U2000 V200R015C50
		5.83.08.20 (V100R008C10)	U2000 V200R015C60
		5.83.09.10 (V100R009C00)	U2000 V200R016C50
		5.83.09.20 (V100R009C10)	U2000 V200R016C60
		5.178.09.20(CSHNU)(V100R009C10)	U2000 V200R016C60
	OptiX RTN 980L	5.140.07.10 (V100R007C00)	U2000 V200R014C50
		5.140.07.20 (V100R007C10)	U2000 V200R014C60
		5.140.08.10 (V100R008C00)	U2000 V200R015C50
		5.140.08.20 (V100R008C10)	U2000 V200R015C60
		5.140.09.10 (V100R009C00)	U2000 V200R016C50
		5.140.09.20 (V100R009C10)	U2000 V200R016C60

Category	Equipment	Software Version	First U2000 Version Supported
		5.179.09.20(CSHLU)(V100R009C10)	U2000 V200R016C60
	OptiX RTN 310	5.92.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
		5.92.01.20 (V100R001C01)	
		5.92.03.10 (V100R003C00)	U2000 V200R014C60
		5.92.05.10 (V100R005C00)	U2000 V200R015C50
		5.92.06.10 (V100R006C00)	U2000 V200R015C60
		5.92.07.10 (V100R007C00)	U2000 V200R016C50
		5.92.07.20 (V100R007C10)	U2000 V200R016C60
	OptiX RTN 320	5.151.05.10 (V100R005C00)	U2000 V200R015C50
		5.151.06.10 (V100R006C00)	U2000 V200R015C60
		5.151.07.10 (V100R007C00)	U2000 V200R016C50
		5.151.07.20 (V100R007C10)	U2000 V200R016C60
	OptiX RTN 360	5.138.01.10 (V100R001C00)	U2000 V200R014C50
		5.138.03.10 (V100R003C00)	U2000 V200R014C60
		5.138.05.10 (V100R005C00)	U2000 V200R015C50
		5.138.06.10 (V100R006C00)	U2000 V200R015C60
		5.138.07.10 (V100R007C00)	U2000 V200R016C50
		5.138.07.20 (V100R007C10)	U2000 V200R016C60

Category	Equipment	Software Version	First U2000 Version Supported
	OptiX RTN 380	5.115.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
		5.115.01.20 (V100R001C10)	U2000 V200R001C00
		5.115.02.10 (V100R002C00)	U2000 V200R014C50
		5.115.03.10 (V100R003C00)	U2000 V200R014C60
		5.115.05.10 (V100R005C00)	U2000 V200R015C50
		5.115.06.10 (V100R006C00)	U2000 V200R015C60
		5.115.07.10 (V100R007C00)	U2000 V200R016C50
	OptiX RTN 380e	5.115.07.20 (V100R007C10)	U2000 V200R016C60
		5.180.07.20 (V100R007C10)	U2000 V200R016C60
		5.160.06.10 (V100R006C00)	U2000 V200R015C60
	OptiX RTN 380H	5.160.07.10 (V100R007C00)	U2000 V200R016C50
		5.160.07.20 (V100R007C10)	U2000 V200R016C60
		V1	U2000 V100R009C00
	NEC 5000S	V2.1	Earlier than U2000 V100R009C00
	OptiX RTN FlexPort80	V1	Earlier than U2000 V100R009C00
	PTP 250	V1	Earlier than U2000 V100R009C00
	PTP 500	V1	Earlier than U2000 V100R009C00
	PTP 650	V1	U2000 V200R014C50
	PMP 450	V1	U2000 V200R015C50

Category	Equipment	Software Version	First U2000 Version Supported
	X-1200	V1	U2000 V200R015C50

Table 12-7 RTN (NA) series equipment

Category	Equipment	Software Version
RTN(NA)	OptiX RTN 910 (NA)	5.76.03.20 (V100R003C01)
	OptiX RTN 950 (NA)	5.76.03.20 (V100R003C01)

NOTE

Mapping principle:

1. If the mapping table provides only the information that a.bb.cc.20 is supported by version A of the U2000, a.bb.cc.2x is supported by version A of the U2000.
2. If the mapping table provides only the information that a.bb.cc is supported by version A of the U2000, a.bb.cc.xx is supported by version A of the U2000.

Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product.

12.6 PTN Series Equipment

The following table lists the PTN series equipment supported.

Table 12-8 PTN series equipment

Category	Equipment	Software Version	First U2000 Version Supported
PTN series	OptiX PTN 1900	5.58.01.10 (V100R001C01)	Earlier than U2000 V100R009C00
		5.58.01.30 (V100R001C02)	
		5.58.01.50 (V100R001C03)	
		5.58.02.10 (V100R002C00)	
		5.58.02.30 (V100R002C01)	
		5.58.02.50 (V100R002C02)	
		5.58.02.60 (V100R002C03)	

Category	Equipment	Software Version	First U2000 Version Supported
		5.58.02.90 (V100R002C02SPC600)	
		5.58.03.20 (V100R003C01)	
		5.58.03.30 (V100R003C02)	
		5.58.05.10 (V100R005C00)	
		5.58.05.30 (V100R005C01)	
		5.58.06.30 (V100R006C10)	V200R014C60
		5.58.07.10 (V100R007C00)	V200R015C50
		5.58.07.30 (V100R007C10)	V200R015C60
		5.58.08.20 (V100R008C10)	V200R016C60
	OptiX PTN 3900-8	5.78.02.50 (V100R002C02)	Earlier than U2000 V100R009C00
		5.78.02.60 (V100R002C03)	
		5.78.02.70 (V100R002C05)	
		5.78.02.90 (V100R002C02SPC600)	
		5.78.03.20 (V100R003C01)	
		5.78.03.30 (V100R003C02)	
		5.78.05.10 (V100R005C00)	
		5.78.05.30 (V100R005C01)	
		5.78.06.30 (V100R006C10)	V200R014C60
		5.78.07.10 (V100R007C00)	V200R015C50
		5.78.07.30 (V100R007C10)	V200R015C60
		5.78.08.20 (V100R008C10)	V200R016C60
	OptiX PTN 3900	5.59.01.10 (V100R001C01)	Earlier than U2000 V100R009C00
		5.59.01.30 (V100R001C02)	
		5.59.01.50 (V100R001C03)	
		5.59.02.10 (V100R002C00)	
		5.59.02.30 (V100R002C01)	
		5.59.02.50 (V100R002C02)	
		5.59.02.60 (V100R002C03)	

Category	Equipment	Software Version	First U2000 Version Supported
		5.59.02.70 (V100R002C05)	
		5.59.02.90 (V100R002C02SPC600)	
		5.59.03.20 (V100R003C01)	
		5.59.03.30 (V100R003C02)	
		5.59.05.10 (V100R005C00)	
		5.59.05.30 (V100R005C01)	
		5.59.06.30 (V100R006C10)	V200R014C60
		5.59.07.10 (V100R007C00)	V200R015C50
		5.59.07.30 (V100R007C10)	V200R015C60
		5.59.08.20 (V100R008C10)	V200R016C60
	OptiX PTN 912	5.63.01.10 (V100R001C01)	Earlier than U2000 V100R009C00
		5.63.01.50 (V100R001C02)	
	OptiX PTN 910	5.64.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
		5.64.01.50 (V100R001C01)	
		5.64.02.10 (V100R002C00)	
		5.64.02.50 (V100R002C01)	
		5.64.02.60 (V100R002C03)	
		5.64.02.70 (V100R002C05)	
		5.64.02.80 (V100R002C01SPC800)	
		5.64.02.90 (V100R002C01SPC600)	
		5.64.03.20 (V100R003C01)	
		5.64.03.30 (V100R003C02)	
		5.64.05.10 (V100R005C00)	
		5.64.05.30 (V100R005C01)	
		5.64.06.30(V100R006C10)	V200R014C60
		5.64.07.10 (V100R007C00)	V200R015C50
		5.64.07.30 (V100R007C10)	V200R015C60
		5.64.08.20 (V100R008C10)	V200R016C60

Category	Equipment	Software Version	First U2000 Version Supported
OptiX PTN 950	OptiX PTN 950	5.65.01.10 (V100R001C00)	Earlier than U2000 V100R009C00
		5.65.01.50 (V100R001C01)	
		5.65.02.10 (V100R002C00)	
		5.65.02.50 (V100R002C01)	
		5.65.02.60 (V100R002C03)	
		5.65.02.70 (V100R002C05)	
		5.65.02.80 (V100R002C01SPC800)	
		5.65.02.90 (V100R002C01SPC600)	
		5.65.03.20 (V100R003C01)	
		5.65.03.30 (V100R003C02)	
		5.65.05.10 (V100R005C00)	
		5.65.05.30 (V100R005C01)	
		5.65.06.30 (V100R006C10)	V200R014C60
		5.65.07.10 (V100R007C00)	V200R015C50
		5.65.07.30 (V100R007C10)	V200R015C60
		5.65.08.20 (V100R008C10)	V200R016C60
OptiX PTN 905	OptiX PTN 905	5.88.02.80 (V100R002C05)	Earlier than U2000 V100R009C00
	OptiX PTN 910-F	5.91.03.30 (V100R003C02)	Earlier than U2000 V100R009C00
		5.91.05.10 (V100R005C00)	
		5.91.05.30 (V100R005C01)	
		5.91.06.30 (V100R006C10)	V200R014C60
		5.91.07.10 (V100R007C00)	V200R015C50
		5.91.07.30 (V100R007C10)	V200R015C60
		5.91.08.20 (V100R008C10)	V200R016C60
OptiX PTN 960	OptiX PTN 960	5.94.03.40 (V100R003C03)	Earlier than U2000 V100R009C00
		5.94.05.10 (V100R005C00)	
		5.94.05.30 (V100R005C01)	
		5.94.06.30 (V100R006C10)	
		V200R014C60	

Category	Equipment	Software Version	First U2000 Version Supported
		5.94.07.10 (V100R007C00)	V200R015C50
		5.94.07.30 (V100R007C10)	V200R015C60
		5.94.08.20 (V100R008C10)	V200R016C60
OptiX PTN 906A	OptiX PTN 906A	5.145.06.30 (V100R006C10)	V200R014C60
		5.145.07.10 (V100R007C00)	V200R015C50
		5.145.07.30 (V100R007C10)	V200R015C60
		5.145.08.20 (V100R008C10)	V200R016C60
OptiX PTN 906B	OptiX PTN 906B	5.146.07.30 (V100R007C10)	V200R015C60
		5.146.08.20 (V100R008C10)	V200R016C60
OptiX PTN 906AI	OptiX PTN 906AI	5.159.07.10 (V100R007C00)	V200R015C50
		5.159.07.30 (V100R007C10)	V200R015C60
		5.159.08.20 (V100R008C10)	V200R016C60
OptiX PTN 905A	OptiX PTN 905A	5.123.05.30 (V100R005C01)	Earlier than U2000 V100R009C00
		5.123.06.30 (V100R006C10)	V200R014C60
		5.123.07.10 (V100R007C00)	V200R015C50
		5.123.07.30 (V100R007C10)	V200R015C60
		5.123.08.20 (V100R008C10)	V200R016C60
OptiX PTN 905B	OptiX PTN 905B	5.124.05.30 (V100R005C01)	Earlier than U2000 V100R009C00
		5.124.06.30 (V100R006C10)	V200R014C60
		5.124.07.10 (V100R007C00)	V200R015C50
		5.124.07.30 (V100R007C10)	V200R015C60
		5.124.08.20 (V100R008C10)	V200R016C60
	OptiX PTN 905E	8.163.09.10 (V100R009C00)	V200R016C60
	OptiX PTN 970	8.182.08.20 (V100R008C10)	V200R016C60
OptiX PTN 990	OptiX PTN 990	8.150.07.20 (V100R007C10)	V200R015C60
		8.150.08.10 (V100R008C00)	V200R016C50
		8.150.08.20 (V100R008C10)	V200R016C60

Category	Equipment	Software Version	First U2000 Version Supported
PTN7900 series	PTN 7900-12	8.148.07.10(V100R007C00)	V200R015C50
		8.148.07.20(V100R007C10)	V200R015C60
		8.148.08.10(V100R008C00)	V200R016C50
		8.148.08.20(V100R008C10)	V200R016C60
	PTN 7900-24	8.135.06.20(V100R006C10)	V200R001C00
		8.135.06.30(V100R006C20)	V200R014C60
		8.135.07.10(V100R007C00)	V200R015C50
		8.135.07.20(V100R007C10)	V200R015C60
		8.135.08.10(V100R008C00)	V200R016C50
		8.135.08.20(V100R008C10)	V200R016C60
	PTN 7900-32	8.128.06.10(V100R006C00)	V200R001C00
		8.128.06.20(V100R006C10)	V200R001C00
		8.128.06.30(V100R006C20)	V200R014C60
		8.128.07.10(V100R007C00)	V200R015C50
		8.128.07.20(V100R007C10)	V200R015C60
		8.128.08.10(V100R008C00)	V200R016C50
		8.128.08.20(V100R008C10)	V200R016C60

NOTE

Mapping principle:

1. If the mapping table provides only the information that a.bb.cc.20 is supported by version A of the U2000, a.bb.cc.2x is supported by version A of the U2000.
2. If the mapping table provides only the information that a.bb.cc is supported by version A of the U2000, a.bb.cc.xx is supported by version A of the U2000.

Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product.

Table 12-9 PTN 6900 equipment

Category	Equipment	Software Version	First U2000 Version Supported
PTN6900 series	PTN 6900-1/PTN 6900-2/PTN	V600R003C02	Earlier than U2000 V100R009C00
		V600R005C00	

Category	Equipment	Software Version	First U2000 Version Supported
6900-3/PTN 6900-8/PTN 6900-16	V600R006C00		
	V600R007C00		
	V600R008C00		
	V600R008C10		
	V600R008C20	V200R014C60	
	V600R009C00	V200R015C50	
	V600R009C10	V200R015C60	
	V600R009C20	V200R016C50	
	V800R005C01	Earlier than U2000 V100R009C00	
	V800R006C00		
PTN 6900-1- M4/PTN 6900-2- M8/PTN 6900-2- M16	V800R006C10		
	V800R007C00	V200R014C60	
	V800R007C00	V200R014C60	
	V800R007C10	V200R015C50	
	V800R008C00	V200R015C60	
	V800R008C10	V200R016C50	
	V800R008C11	V200R016C60	
	V800R009C00		
	V800R007C00	V200R014C60	
	V800R007C10	V200R015C50	
PTN6900-3/8/16/3A /8A/16A	V800R008C00	V200R015C60	
	V800R008C10	V200R016C50	
	V800R008C11	V200R016C60	
	V800R009C00		
	V800R007C10	V200R015C50	
	V800R008C00	V200R015C60	
	V800R008C10	V200R016C50	
	V800R008C11	V200R016C60	
	V800R009C00		
	V800R007C10	V200R015C50	
PTN6900-1/2/M2E/ M2F	V800R008C00	V200R015C60	
	V800R008C10	V200R016C50	
	V800R008C11	V200R016C60	
	V800R009C00		

Category	Equipment	Software Version	First U2000 Version Supported
	PTN6900-2-M8A/ M16A	V800R008C10	V200R016C50
		V800R008C11	V200R016C60
		V800R009C00	

12.7 FTTx Series Equipment

The following table lists the manageable FTTx series equipment supported.

Table 12-10 FTTx series equipment

Category	Equipment	Software Version	First U2000 Version Supported	
OLT series	SmartAX MA5600T Multi-Service Access Module (MA5600T)	MA5600 V800R006C31 MA5600 V800R006C32 MA5600 V800R006C72 MA5600 V800R006C02 MA5600 V800R006C02SPC100 MA5600 V800R007C00 MA5600 V800R007C01 MA5600 V800R008C00 MA5600 V800R008C01 MA5600 V800R008C02 MA5600 V800R008C03 MA5600 V800R008C05 MA5600 V800R009C00 MA5600 V800R010C00 MA5600 V800R011C00 MA5600 V800R012C00	Earlier than U2000 V100R009C00	
	MA5600 V800R013C00	V100R009C00		
	MA5600 V800R013C10	V200R001C00		
	MA5600 V800R015C00	V200R014C50		

Category	Equipment	Software Version	First U2000 Version Supported
		MA5600 V800R015C10	V200R014C60
		MA5600 V800R016C00	V200R015C50
		MA5600 V800R016C10	V200R015C60
		MA5600 V800R017C00	V200R016C50
		MA5600 V800R017C10	V200R016C60
	SmartAX MA5603T Multi-Service Access Module (MA5603T)	MA5600 V800R006C02 MA5600 V800R006C32 MA5600 V800R006C73 MA5600 V800R006C02SPC100 MA5603 V800R007C00 MA5603 V800R007C01 MA5603 V800R008C00 MA5600 V800R008C01 MA5600 V800R008C02 MA5600 V800R008C03 MA5600 V800R008C05 MA5600 V800R009C00 MA5600 V800R010C00 MA5600 V800R011C00 MA5600 V800R012C00	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
		MA5600 V800R013C00	V100R009C00
		MA5600 V800R013C10	V200R001C00
		MA5600 V800R015C00	V200R014C50
		MA5600 V800R015C10	V200R014C60
		MA5600 V800R016C00	V200R015C50
		MA5600 V800R016C10	V200R015C60
		MA5600 V800R017C00	V200R016C50
		MA5600 V800R017C10	V200R016C60
	SmartAX MA5603U Optical Access Equipment	MA5600 V800R202C00 MA5600 V800R202C01 MA5600 V800R203C00 MA5600 V800R205C00 MA5600 V800R010C00 MA5600 V800R011C00 MA5600 V800R012C00	Earlier than U2000 V100R009C00
		MA5600 V800R013C00	V100R009C00
		MA5600 V800R013C10	V200R001C00
		MA5600 V800R016C00	V200R015C50
		MA5600 V800R016C10	V200R015C60

Category	Equipment	Software Version	First U2000 Version Supported
		MA5600 V800R017C00	V200R016C50
	SmartAX MA5680T Optical Access Equipment (MA5680T)	MA5600 V800R006C31 MA5600 V800R006C32 MA5600 V800R006C72 MA5600 V800R006C02 MA5600 V800R006C02SPC100 MA5600 V800R007C00 MA5600 V800R007C01 MA5600 V800R008C00 MA5600 V800R008C01 MA5600 V800R008C02 MA5600 V800R008C03 MA5600 V800R008C05 MA5600 V800R009C00 MA5600 V800R010C00 MA5600 V800R011C00 MA5600 V800R012C00	Earlier than U2000 V100R009C00
		MA5600 V800R013C00	V100R009C00
		MA5600 V800R013C10	V200R001C00
		MA5600 V800R015C00	V200R014C50

Category	Equipment	Software Version	First U2000 Version Supported
		MA5600 V800R015C10	V200R014C60
		MA5600 V800R016C00	V200R015C50
		MA5600 V800R016C10	V200R015C60
		MA5600 V800R017C00	V200R016C50
		MA5600 V800R017C10	V200R016C60
	SmartAX MA5683T Optical Access Equipment (MA5683T)	MA5600 V800R006C32 MA5600 V800R006C72 MA5600 V800R006C02 MA5600 V800R006C02SPC100 MA5600 V800R007C00 MA5600 V800R007C01 MA5600 V800R008C01 MA5600 V800R008C03 MA5600 V800R008C05 MA5600 V800R009C00 MA5600 V800R010C00 MA5600 V800R011C00 MA5600 V800R012C00	Earlier than U2000 V100R009C00
		MA5600 V800R013C00	V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
		MA5600 V800R013C10	V200R001C00
		MA5600 V800R015C00	V200R014C50
		MA5600 V800R015C10	V200R014C60
		MA5600 V800R016C00	V200R015C50
		MA5600 V800R016C10	V200R015C60
		MA5600 V800R017C00	V200R016C50
		MA5600 V800R017C10	V200R016C60
	SmartAX MA5608T Multi-Service Access Equipment (MA5608T)	MA5600 V800R012C00	Earlier than U2000 V100R009C00
		MA5600 V800R013C00	V100R009C00
		MA5600 V800R013C10	V200R001C00
		MA5600 V800R015C00	V200R014C50
		MA5600 V800R015C10	V200R014C60
		MA5600 V800R016C00	V200R015C50
		MA5600 V800R016C10	V200R015C60
		MA5600 V800R017C00	V200R016C50
		MA5600 V800R017C10	V200R016C60
	SmartAX MA5800-X17 Multi-Service Access Equipment (MA5800-X17)	MA5800 V100R015C00	V200R014C60

Category	Equipment	Software Version	First U2000 Version Supported
		MA5800 V100R016C00	V200R015C50
		MA5800 V100R016C10	V200R015C60
		MA5800 V100R017C00	V200R016C50
		MA5800 V100R017C10	V200R016C60
	SmartAX MA5800-X15 Multi-Service Access Equipment (MA5800-X15)	MA5800 V100R018C00	V200R014C60
		MA5800 V100R017C00	V200R016C50
		MA5800 V100R017C10	V200R016C60
	SmartAX MA5800-X7 Multi-Service Access Equipment (MA5800-X7)	MA5800 V100R016C00	V200R015C50
		MA5800 V100R016C10	V200R015C60
		MA5800 V100R017C00	V200R016C50
		MA5800 V100R017C10	V200R016C60
	SmartAX MA5800-X2 Multi-Service Access Equipment (MA5800-X2)	MA5800 V100R017C10	V200R016C60
MDU series	SmartAX MA5606T Multi-Service Access Equipment (MA5606T)	MA5600 V800R006C21 MA5600 V800R006C22 MA5600 V800R006C62 MA5600 V800R006C02 MA5600 V800R007C00 MA5600 V800R007C01	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
	SmartAX MA5620 Remote Optical Access Unit (MA5620)	MA5620 V800R307C00 MA5620 V800R307C01 MA5620 V800R308C00 MA5620 V800R308C02 MA5620 V800R310C00 MA5620 V800R312C00	Earlier than U2000 V100R009C00
		MA5620 V800R016C10	V200R015C60
	SmartAX MA5626 Remote Optical Access Unit (MA5626)	MA5626 V800R307C00 MA5626 V800R307C01 MA5626 V800R308C00 MA5626 V800R310C00 MA5626 V800R312C00	Earlier than U2000 V100R009C00
		MA5626 V800R016C10	V200R015C60
	SmartAX MA5628 Remote Optical Access Unit (MA5628)	MA5628 V800R308C01 MA5628 V800R309C00 MA5628 V800R310C00	Earlier than U2000 V100R009C00
	SmartAX MA5620E EPON Remote Optical Access Unit (MA5620E)	MA5600 V800R305C01 MA5620E V800R307C00 MA5620E V800R307C01	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
	SmartAX MA5626E EPON Remote Optical Access Unit (MA5626E)	MA5600 V800R305C01 MA5626E V800R307C00 MA5626E V800R307C01	Earlier than U2000 V100R009C00
	SmartAX MA5620G GPON Remote Optical Access Unit (MA5620G)	MA5600 V800R305C01 MA5620G V800R307C00 MA5620G V800R307C01	Earlier than U2000 V100R009C00
	SmartAX MA5626G GPON Remote Optical Access Unit (MA5626G)	MA5600 V800R305C01 MA5626G V800R307C00 MA5626G V800R307C01	Earlier than U2000 V100R009C00
	SmartAX MA5610 Multi-Service Access Module (MA5610)	MA5610 V800R306C01 MA5610 V800R307C01	Earlier than U2000 V100R009C00
	SmartAX MA5612 Multi-Service Access Module (MA5612)	MA5612 V800R307C01 MA5612 V800R308C00 MA5612 V800R308C01 MA5612 V800R308C03 MA5612 V800R310C00 MA5612 V800R311C00 MA5612 V800R312C00	Earlier than U2000 V100R009C00
		MA5612 V800R015C00	V200R014C50
		MA5612 V800R017C00	V200R016C50

Category	Equipment	Software Version	First U2000 Version Supported
	SmartAX MA5612A Multi-Service Access Module (MA5612A)	MA5612 V800R308C01 MA5612 V800R310C00 MA5612 V800R311C00 MA5612 V800R312C00	Earlier than U2000 V100R009C00
		MA5612 V800R015C00	V200R014C50
	SmartAX MA5616 Multi-Service Access Module (MA5616)	MA5616 V800R306C01 MA5616 V800R307C00 MA5616 V800R307C01 MA5616 V800R307C02 MA5616 V800R308C00 MA5616 V800R308C01 MA5616 V800R308C02 MA5616 V800R308C03 MA5616 V800R309C00 MA5616 V800R310C00 MA5616 V800R311C00 MA5616 V800R312C00	Earlier than U2000 V100R009C00
		MA5616 V800R313C00	V100R009C00
		MA5616 V800R313C10	V200R001C00
		MA5616 V800R015C00	V200R014C50

Category	Equipment	Software Version	First U2000 Version Supported
		MA5616 V800R015C10	V200R014C60
		MA5616 V800R016C00	V200R015C50
		MA5616 V800R016C10	V200R015C60
		MA5616 V800R017C00	V200R016C50
		MA5616 V800R017C10	V200R016C60
	SmartAX MA5651 Remote Optical Access Unit (MA5651)	MA5600 V800R305C03	Earlier than U2000 V100R009C00
	SmartAX MA5652 Remote Optical Access Unit (MA5652)	MA5652 V800R309C00 MA5652 V800R310C00	Earlier than U2000 V100R009C00
	SmartAX MA5652G GPON Remote Optical Access Unit (MA5652G)	MA5652G V800R306C01 MA5652G V800R307C00 MA5652G V800R308C02	Earlier than U2000 V100R009C00
	SmartAX MA5662 Multi-Service Access Module (MA5662)	MA5600 V800R202C00 MA5600 V800R202C01 MA5600 V800R203C00 MA5600 V800R205C00 MA5662 V800R309C00	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
	SmartAX MA5621 Multi-Service Access Module (MA5621)	MA5621 V800R309C00 MA5621 V800R310C00 MA5621 V800R312C00	Earlier than U2000 V100R009C00
		MA5621 V800R017C00	V200R016C50
	SmartAX MA5621A Multi-Service Access Module (MA5621A)	MA5621 V800R311C00 MA5621 V800R312C00	Earlier than U2000 V100R009C00
		MA5621 V800R016C00	V200R015C50
	SmartAX MA5622A Multi-Service Access Module (MA5622A)	MA5622 V800R311C00	Earlier than U2000 V100R009C00
		MA5622 V800R313C00	V100R009C00
	SmartAX MA5623 Multi-Service Access Module (MA5623)	MA5623 V800R311C00	Earlier than U2000 V100R009C00
		MA5623 V800R313C00	V100R009C00
	SmartAX MA5623A Multi-Service Access Module (MA5623A)	MA5623 V800R311C01 MA5623 V800R312C00	Earlier than U2000 V100R009C00
		MA5623 V800R313C00	V100R009C00
		MA5623 V800R313C10	V200R001C00
		MA5623 V800R016C00	V200R015C50

Category	Equipment	Software Version	First U2000 Version Supported
	SmartAX MA5631 EoC Head End Device (MA5631)	MA5631 V800R308C02 MA5631 V800R310C00	Earlier than U2000 V100R009C 00
	SmartAX MA5632 EoC Head End Device (MA5632)	MA5632 V800R310C00	Earlier than U2000 V100R009C 00
	SmartAX MA5635 Multi-Service Access Module (MA5635)	MA5635 V800R307C00	Earlier than U2000 V100R009C 00
	SmartAX MA5669 Multi-Service Access Module (MA5669)	MA5669 V800R310C00	Earlier than U2000 V100R009C 00
	SmartAX MA5658 Multi-Service Access Module (MA5658)	MA5658 V800R312C00	Earlier than U2000 V100R009C 00
	SmartAX MA5671 Multiple Dwelling Unit (MA5671)	MA5671 V800R313C00	V100R009C 00
		MA5671 V800R016C00	V200R015C 50
		MA5671 V800R016C10	V200R015C 60
		MA5671 V800R017C00	V200R016C 50
	SmartAX MA5671A Multiple Dwelling Unit (MA5671A)	MA5671A V800R015C10	V200R014C 60
	SmartAX MA5671A-G1 Multiple Dwelling Unit (MA5671A-G1)	MA5671A V800R016C00	V200R015C 50
	SmartAX MA5672M Multiple Dwelling Unit (MA5672M)	MA5672M V800R313C00	V100R009C 00
		MA5672M V800R017C00	V200R016C 50
	SmartAX MA5675M Multiple Dwelling Unit (MA5675M)	MA5675M V800R313C00	V100R009C 00

Category	Equipment	Software Version	First U2000 Version Supported
		MA5675M V800R016C00	V200R015C50
		MA5675M V800R017C00	V200R016C50
	SmartAX MA5673 Multiple Dwelling Unit (MA5673)	MA5673 V800R313C00	V100R009C00
	SmartAX MA5675 Multiple Dwelling Unit (MA5675)	MA5675 V800R313C00	V100R009C00
		MA5675 V800R016C00	V200R015C50
		MA5675 V800R017C00	V200R016C50
	SmartAX MA5675-G1F1 Multiple Dwelling Unit (MA5675-G1F1)	MA5675 V800R016C00	V200R015C50
	SmartAX MA5675-G1F1P1 Multiple Dwelling Unit (MA5675-G1F1P1)	MA5675 V800R016C00	V200R015C50
		MA5675 V800R017C00	V200R016C50
	SmartAX MA5676-G1F1 Multiple Dwelling Unit (MA5676-G1F1)	MA5676 V800R016C00	V200R015C50
	SmartAX MA5676 Multiple Dwelling Unit (MA5676)	MA5676 V800R016C10	V200R015C60
	SmartAX MA5694 Multi-Service Access Module (MA5694)	MA5694 V800R313C00	V100R009C00
		MA5694 V800R015C00	V200R014C50
		MA5694 V800R016C00	V200R015C50
	SmartAX MA5698 Multi-Service Access Module (MA5698)	MA5698 V800R313C00	V100R009C00
		MA5698 V800R015C00	V200R014C50
	SmartAX MA5821 Multiple Dwelling Unit (MA5821)	MA5821 V800R313C00	V100R009C00
		MA5821 V800R313C10	V200R001C00

Category	Equipment	Software Version	First U2000 Version Supported
SmartAX MA5822 Multiple Dwelling Unit (MA5822)		MA5821 V800R017C00	V200R016C50
		MA5821 V800R017C10	V200R016C60
	SmartAX MA5818 Multi-Service Access Module (MA5818)	MA5822 V800R313C00	V100R009C00
		MA5822 V800R017C00	V200R016C50
		MA5818 V800R313C00	V100R009C00
		MA5818 V800R015C00	V200R014C50
		MA5818 V800R015C10	V200R014C60
		MA5818 V800R016C00	V200R015C50
		MA5818 V800R017C00	V200R016C50
		MA5818 V800R017C10	V200R016C60
SmartAX MA5611S Multi-Service Access Module (MA5611S)		MA5611S V800R313C00	V100R009C00
		MA5611S V800R313C10	V200R001C00
		MA5611S V800R015C00	V200R014C50
		MA5611S V800R015C10	V200R014C60
		MA5611S V800R017C10	V200R016C60
SmartAX MA5811S Multi-Service Access Module (MA5811S)		MA5811S V800R016C00	V200R015C50
		MA5811S V800R016C10	V200R015C60
		MA5811S V800R017C00	V200R016C50

Category	Equipment	Software Version	First U2000 Version Supported
	MA5811S V800R017C10	MA5811S V800R017C10	V200R016C60
	SmartAX MA5871-G4 Multiple Dwelling Unit (MA5871-G4)	MA5871 V800R016C00	V200R015C50
	SmartAX MA5878 Multi-Service Access Module (MA5878)	MA5878 V800R017C00	V200R016C50
	SmartAX MA5694S Multi-Service Access Module (MA5694S)	MA5694S V800R313C10	V200R001C00
		MA5694S V800R015C00	V200R014C50
	SmartAX MA5898 Multi-Service Access Module (MA5898)	MA5898 V800R313C00	V100R009C00
		MA5898 V800R015C00	V200R014C50
		MA5898 V800R017C10	V200R016C60
	SmartAX MA5651S Multiple Dwelling Unit (MA5651S)	MA5651S V800R313C10	V200R001C00
		MA5651S V800R016C10	V200R015C60
		MA5651S V800R017C00	V200R016C50
		MA5651S V800R017C10	V200R016C60
	SmartAX MA5652S Multiple Dwelling Unit (MA5652S)	MA5652S V800R313C10	V200R001C00
		MA5652S V800R017C00	V200R016C50
		MA5652S V800R017C10	V200R016C60
	SmartAX MA5672-8 Multiple Dwelling Unit (MA5672-8)	MMA5672 V800R016C00	V200R015C50
	SmartAX MA5672-16 Multiple Dwelling Unit (MA5672-16)	MMA5672 V800R016C00	V200R015C50
	SmartAX MA5672-24 Multiple Dwelling Unit (MA5672-24)	MMA5672 V800R016C00	V200R015C50

12.8 D-CCAP Series Equipment

The following table lists the manageable D-CCAP series equipment supported.

Table 12-11 D-CCAP series equipment

Category	Equipment	Software Version	First U2000 Version Supported
OLT series	SmartAX MA5600T Multi-Service Access Module (MA5600T)	MA5600V800R012 C00	V100R008C00
		MA5600V800R013 C00	V100R009C00
		MA5600V800R013 C10	V200R001C00
		MA5600V800R015 C00	V200R014C50
		MA5600V800R015 C10	V200R014C60
		MA5600V800R016 C00	V200R015C50
		MA5600V800R016 C10	V200R015C60
		MA5600V800R017 C00	V200R016C50
	SmartAX MA5800-X17 Multi-Service Access Equipment (MA5800-X17)	MA5800V100R017 C10	V200R016C60
		MA5800V100R015 C00	V200R014C60
		MA5800V100R016 C00	V200R015C50
		MA5800V100R016 C10	V200R015C60
		MA5800V100R017 C00	V200R016C50

Category	Equipment	Software Version	First U2000 Version Supported
	SmartAX MA5800-X15 Multi-Service Access Equipment (MA5800-X15)	MA5800V100R016 C10	V200R014C60
		MA5800V100R017 C00	V200R016C50
		MA5800V100R017 C10	V200R016C60
		MA5800V100R018 C00	V200R016C60
	SmartAX MA5800-X7 Multi-Service Access Equipment (MA5800-X7)	MA5800V100R016 C00	V200R015C50
		MA5800V100R016 C10	V200R015C60
		MA5800V100R017 C00	V200R016C50
		MA5800V100R017 C10	V200R016C60
		MA5800V100R018 C00	V200R016C60
	SmartAX MA5800-X2 Multi-Service Access Equipment (MA5800-X2)	MA5800V100R017 C10	V200R016C60
		MA5800V100R018 C00	V200R016C60
D-CCAP series	SmartAX MA5633 Distributed-CMTS Head End (MA5633)	MA5633V800R312 C00	V100R008C00
		MA5633V800R313 C00	V100R009C00
		MA5633V800R313 C10	V200R001C00
		MA5633V800R015 C00	V200R014C50
		MA5633V800R015 C10	V200R014C60
		MA5633V800R016 C00	V200R015C50
		MA5633V800R016 C10	V200R015C60

Category	Equipment	Software Version	First U2000 Version Supported
		MA5633V800R017 C00	V200R016C50
		MA5633V800R017 C10	V200R016C60
		MA5633V800R018 C00	V200R016C60

12.9 MSAN Series Equipment

The following table lists the MSAN series equipment supported.

Table 12-12 MSAN series equipment

Category	Equipment	Software Version	First U2000 Version Supported
UA5000 series	UA5000 Universal Access Unit (UA5000(IPMB))	UA5000IPMB V100R015C02	Earlier than U2000 V100R009C00
		UA5000IPMB V100R017C02	

Category	Equipment	Software Version	First U2000 Version Supported
	UA5000 Universal Access Unit (UA5000(PVMV1))	UA5000PVM V100R017C01 UA5000PVM V100R017C02 UA5000PVM V100R017C03 UA5000PVM V100R019C00 UA5000PVM V100R019C01 UA5000PVM V100R019C02 UA5000PVM V100R019C06 UA5000PVM V100R019C07	Earlier than U2000 V100R009C00

12.10 DSLAM Series Equipment

The following table lists the DSLAM series equipment supported.

Table 12-13 DSLAM series equipment

Category	Equipment	Software Version	First U2000 Version Supported
MA5600 series	SmartAX MA5600 Multi-service Access Module (MA5600V3)	MA5600 V300R003C05 MA5600 V300R003C06 MA5600 V300R003C07	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported	
MA5600V8 series	SmartAX MA5600T Multi-service Access Module (MA5600T)	MA5600 V800R006C31 MA5600 V800R006C32 MA5600 V800R006C72 MA5600 V800R006C02 MA5600 V800R006C02SPC10 0 MA5600 V800R007C00 MA5600 V800R007C01 MA5600 V800R008C00 MA5600 V800R008C01 MA5600 V800R008C02 MA5600 V800R008C03 MA5600 V800R008C05 MA5600 V800R009C00 MA5600 V800R010C00 MA5600 V800R011C00 MA5600 V800R012C00	Earlier than U2000 V100R009C00	
	MA5600 V800R013C00	V100R009C00		
	MA5600 V800R013C10	V200R001C00		
	MA5600 V800R015C00	V200R014C50		
	MA5600 V800R015C10	V200R014C60		

Category	Equipment	Software Version	First U2000 Version Supported
		MA5600 V800R016C00	V200R015C50
		MA5600 V800R016C10	V200R015C60
		MA5600 V800R017C00	V200R016C50
		MA5600 V800R017C10	V200R016C60
	SmartAX MA5603T Multi-service Access Module (MA5603T)	MA5600 V800R006C02 MA5600 V800R006C32 MA5600 V800R006C73 MA5600 V800R006C02SPC10 0 MA5603 V800R007C00 MA5603 V800R007C01 MA5603 V800R008C00 MA5600 V800R008C01 MA5600 V800R008C02 MA5600 V800R008C03 MA5600 V800R008C05 MA5600 V800R009C00 MA5600 V800R010C00 MA5600 V800R011C00 MA5600 V800R012C00	Earlier than U2000 V100R009C00
		MA5600 V800R013C00	V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
		MA5600 V800R013C10	V200R001C00
		MA5600 V800R015C00	V200R014C50
		MA5600 V800R015C10	V200R014C60
		MA5600 V800R016C00	V200R015C50
		MA5600 V800R016C10	V200R015C60
		MA5600 V800R017C00	V200R016C50
		MA5600 V800R017C10	V200R016C60
	SmartAX MA5662 Multi-service Access Module (MA5662)	MA5600 V800R202C00 MA5600 V800R202C01 MA5600 V800R203C00 MA5600 V800R205C00 MA5662 V800R309C00	Earlier than U2000 V100R009C00
	SmartAX MA5606T Multi-service Access Module (MA5606T)	MA5600 V800R006C21 MA5600 V800R006C22 MA5600 V800R006C62 MA5600 V800R006C02 MA5600 V800R007C00 MA5600 V800R007C01	Earlier than U2000 V100R009C00
	SmartAX MA5608T Multi-service Access Module (MA5608T)	MA5600 V800R012C00	Earlier than U2000 V100R009C00
		MA5600 V800R013C00	V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
		MA5600 V800R013C10	V200R001C00
		MA5600 V800R015C00	V200R014C50
		MA5600 V800R015C10	V200R014C60
		MA5600 V800R016C00	V200R015C50
		MA5600 V800R016C10	V200R015C60
		MA5600 V800R017C00	V200R016C50
		MA5600 V800R017C10	V200R016C60

12.11 BITS/iSite/EDFA Series Equipment

The following table lists the BITS/iSite/EDFA series equipment supported.

Table 12-14 BITS/iSite/EDFA series equipment

Category	Equipment	Software Version	First U2000 Version Supported
BITS	SYNLOCK V3/V5 Building Integrated Timing Supply System	V3 V5	Earlier than U2000 V100R009C00
	SYNLOCK T6020 IP Network Special Timing System	V6	Earlier than U2000 V100R009C00
iSite	Cabinet Control Unit (CCU)	CCU V100R001C00	V200R014C50
		CCU V200R001C00	V200R015C50
	Remote Power System (RPS)	ETPC1701 V100R001C20 (iSite V300R015C92)	V200R014C60

Category	Equipment	Software Version	First U2000 Version Supported
		ETPC1701 V100R001C20 (iSite V300R016C00)	V200R015C50
		ETPC1701 V100R001C30 (iSite V300R016C10)	V200R015C60
EDFA	EDFA3220-D	EDFA&WDM1r V100R006C00	V200R016C50

12.12 NE/ATN/CX/Multi-service gateways Series Equipment

Manageable NE/ATN/CX/Multi-service gateways series equipment is listed as follows:

Table 12-15 Manageable NE/ATN/CX/Multi-service gateway series equipment

Category	Equipment	Software Version	First U2000 Version Supported
NE series	NE40E-4/8/NE80E	V600R009C20	V200R016C50
		V600R009C10	V200R015C60
		V600R009C00	V200R015C50
		V600R008C20	V200R014C60
		V600R008C10	V200R014C50
		V600R008C00	V200R001C00
		V600R007C00	V100R009C00
	V600R006C00 V600R005C00 V600R003C00	V600R006C00	Earlier than U2000 V100R009C00
		V600R005C00	
		V600R003C00	

Category	Equipment	Software Version	First U2000 Version Supported
NE40E	NE40E-M2	V800R009C00 V800R008C11	V200R016C60
		V800R008C10	V200R016C50
		V800R008C00	V200R015C60
		V800R007C10	V200R015C50
		V800R007C00	V200R014C60
	NE40E-X1/-X2	V800R009C00 V800R008C11	V200R016C60
		V800R008C10 V600R009C20	V200R016C50
		V800R008C00 V600R009C10	V200R015C60
		V800R007C10 V600R009C00	V200R015C50
		V800R007C00 V600R008C20	V200R014C60
	NE40E-X3/X8/X16	V800R006C10 V600R008C10	V200R014C50
		V800R006C00 V600R008C00	V200R001C00
		V800R005C01 V800R005C00 V600R007C00 V600R006C00 V600R005C00 V600R003C01 V600R003C00 V600R002C05 V600R002C03	Earlier than U2000 V100R009C00
		V800R009C00 V800R008C11	V200R016C60
		V600R009C20 V800R008C10	V200R016C50

Category	Equipment	Software Version	First U2000 Version Supported
		V600R009C10 V800R008C00	V200R015C60
		V600R009C00 V800R007C00 V800R007C10	V200R015C50
		V600R008C20	V200R014C60
		V600R008C10	V200R014C50
		V600R008C00	V200R001C00
		V600R007C00 V600R006C00 V600R005C00 V600R003C05 V600R003C01 V600R003C00 V600R002 V600R001	Earlier than U2000 V100R009C00
		V800R009C00 V800R008C11	V200R016C60
		V600R009C20 V800R008C10	V200R016C50
		V600R009C10 V800R008C00	V200R015C60
		V600R009C00 V800R007C00	V200R015C50
	NE40E-X8/X16	V800R006C30	V200R014C60
		V800R006C10	V200R014C50
		V800R006C00	V200R001C00
		V800R009C00	V200R016C60
		V800R008C10	V200R016C50
		V800R009C00	V200R016C60
		V800R008C10	V200R016C50
	NE9000	V800R009C00	V200R016C60
		V800R008C10	V200R016C50
		V800R009C00	V200R016C60
	NE5000E	V800R008C10	V200R016C50
		V800R008C00	V200R015C60
		V800R009C00	V200R015C60

Category	Equipment	Software Version	First U2000 Version Supported
		V800R007C10	V200R015C50
		V800R007C00	V200R014C60
		V800R006C10	V200R014C50
		V800R006C00	V200R001C00
		V800R005C01	V100R009C00
		V800R005C00	Earlier than U2000
		V800R003C00	V100R009C00
		V800R002C01	
		V800R002C00	
		V300R007	
	NE5000E-Multi	V300R005	
		V200R003	
		V200R002	
		V800R009C00 (Multi)	V200R016C60
		V800R008C10 (Multi)	V200R016C50
		V800R008C00 (Multi)	V200R015C60
		V800R007C10 (Multi)	V200R015C50
		V800R007C00 (Multi)	V200R014C60
		V800R006C10 (Multi)	V200R014C50
		V800R006C00 (Multi)	V200R001C00
	NE40	V800R005C01 (Multi)	V100R009C00
		V800R005C00 (Multi)	Earlier than U2000
		V800R003C00 (Multi)	V100R009C00
		V800R002C01 (Multi)	
		V800R002C00 (Multi)	
		V300R007C00 (Multi)	
		V300R006C02 (Multi)	
		V300R005 (Multi)	
		V300R005	
		V300R002	
		V100R002	

Category	Equipment	Software Version	First U2000 Version Supported
	NE80	V300R005 V300R002 V100R002	Earlier than U2000 V100R009C00
	NE16E/NE08E/ NE05	V300R002 V100R007	Earlier than U2000 V100R009C00
	NE20E-8	V200R005 V200R003	Earlier than U2000 V100R009C00
	NE20E-S2	V800R009C00 V800R008C11	V200R016C60
		V800R008C10	V200R016C50
		V800R008C00	V200R015C60
		V800R007C00	V200R014C60
		V800R007C10	V200R015C50
	NE20E-X6	V600R006C00 V600R005C00 V600R003C05 V600R003C00	Earlier than U2000 V100R009C00
	NE20-2/4/8	V200R005 V200R003	Earlier than U2000 V100R009C00
	NE20E-S4/S8/S16	V800R009C00 V800R008C11	V200R016C60
		V800R008C10	V200R016C50
		V800R008C00	V200R015C60
		V800R007C00	V200R014C60
		V800R006C10	V200R014C50
		V800R005C01	V200R001C00
		V800R005C00	Earlier than U2000 V100R009C00
	NE16EX	V200R005C30	V200R014C60
		V200R005C20 V200R005C10	Earlier than U2000 V100R009C00
	NE16/NE08	V100R007	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
	NE05E/NE08E	V300R002C00	V200R016C60
		V200R006C20	
		V200R006C10	V200R016C50
		V300R001C10	V200R016C50
		V200R006C00	V200R015C60
	ATN series	V200R005C10	V200R015C50
		ATN905	V200R006C20
		V200R006C10	V200R016C50
		V200R006C00	V200R015C60
		V200R005C10	V200R015C50
		V200R005C00	V200R014C60
		V200R003C20	V200R014C50
		V200R003C10	
	ATN910I	V200R003C00	V200R001C00
		V200R002C01	V100R009C00
		V200R002C00	
		ATN910	V200R006C20
		V200R006C10	V200R016C50
		V200R006C00	V200R015C60
		V200R005C10	V200R015C50
		V200R005C00	V200R014C60
		V200R003C20	V200R014C50
		V200R003C10	
		V200R003C00	V200R001C00
		V200R002C01	V100R009C00
		V200R002C00	

Category	Equipment	Software Version	First U2000 Version Supported
		V200R003C20	V200R014C50
		V200R003C10	
		V200R003C00	V200R001C00
		V200R002C01	V100R009C00
		V200R002C00	
		V200R001C02	Earlier than U2000
		V200R001C01	V100R009C00
		V200R001C00	
		V200R006C20	V200R016C60
		V200R006C10	V200R016C50
	ATN910B	V200R006C00	V200R015C60
		V200R005C10	V200R015C50
		V200R005C00	V200R014C60
		V200R003C20	V200R014C50
		V200R003C10	
		V200R003C00	V200R001C00
		V200R005C00	V200R014C60
	ATN950	V200R003C10	V200R014C50
		V200R003C00	V200R001C00
		V200R002C01	V100R009C00
		V200R002C00	
		V200R001C02	
		V200R001C01	
		V200R001C00	
		V200R006C20	V200R016C60
		V200R006C10	V200R016C50
		V200R006C00	V200R015C60
	ATN950B	V200R005C10	V200R015C50
		V200R005C00	V200R014C60
		V200R003C20	V200R014C50
		V200R003C10	
		V200R003C00	V200R001C00

Category	Equipment	Software Version	First U2000 Version Supported
		V200R002C01 V200R002C00 V200R001C02	V100R009C00
		ATN980	V600R006C00 V600R005C00 V600R003C01 V600R003C00 V600R002C05 V600R002C03 V200R001C02
		ATN980B	V300R002C00 V300R001C10 V300R001C00
	ATN990	V200R016C60	V200R016C50
		V200R015C60	V200R015C50
		V600R006C00 V600R005C00 V600R003C01 V600R003C00 V600R002C05 V600R002C03 V200R001C02	Earlier than U2000 V100R009C00
	ATN910C	V200R016C60	V200R016C50
		V200R016C50	V200R016C60
	ATN950C	V200R016C60	V200R016C50
		V200R016C50	V200R016C60
ETN series	ETN500-A/B/C	V200R006C20	V200R016C60
		V200R006C10	V200R016C50
		V200R006C00	V200R015C60
		V200R005C10	V200R015C50
	ETN550-A	V200R006C20	V200R016C60
		V200R006C10	V200R016C50
		V200R006C00	V200R015C60
CX series	CX600-X3/X8/X16	V800R009C00 V800R008C11	V200R016C60

Category	Equipment	Software Version	First U2000 Version Supported
		V600R009C20 V800R008C10	V200R016C50
		V600R009C10 V800R008C00	V200R015C60
		V600R009C00 V800R007C00	V200R015C50
		V600R008C20	V200R014C60
		V600R008C10	V200R014C50
		V600R008C00	V200R001C00
		V600R007C00	V100R009C00
		V600R006C00 V600R005C00 V600R003C05 V600R003C01 V600R003C00 V600R002 V600R001	Earlier than U2000 V100R009C00
		V800R009C00 V800R008C11	V200R016C60
		V600R009C20 V800R008C10	V200R016C50
	CX600-X8/X16	V600R009C10 V800R008C00	V200R015C60
		V600R009C00 V800R007C00	V200R015C50
		V800R006C30	V200R014C60
		V800R006C10 V800R006C00	Earlier than U2000 V100R009C00
		V300R006 V200R002 V200R001 V100R001	Earlier than U2000 V100R009C00
	CX600-4/8/16		

Category	Equipment	Software Version	First U2000 Version Supported
CX600	CX600-M2	V800R009C00 V800R008C11	V200R016C60
		V800R008C10	V200R016C50
		V800R008C00	V200R015C60
		V800R007C10	V200R015C50
		V800R007C00	V200R014C60
	CX600-X1/X2	V800R009C00 V800R008C11	V200R016C60
		V600R009C20 V800R008C10	V200R016C50
		V600R009C10 V800R008C00	V200R015C60
		V600R009C00 V800R007C10	V200R015C50
		V800R007C00 V600R008C20	V200R014C60
	CX200	V800R006C10 V600R008C10	V200R014C50
		V800R006C00 V600R008C00	V200R001C00
		V800R005C01 V600R007C00	V100R009C00
		V800R005C00 V600R006C00 V600R005C00 V600R003C05 V600R003C01 V600R003C00 V600R002C05 V600R002C03	Earlier than U2000 V100R009C00
		V100R005 V100R002	Earlier than U2000 V100R009C00
	CX200C	V100R005	Earlier than U2000 V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
Multi-service gateways	ME60	V800R009C00	V200R016C60
		V800R008C11	
		V600R009C20	V200R016C50
		V800R008C10	
		V600R009C10	V200R015C60
		V600R009C00	V200R015C50
		V600R008C20	V200R014C60
		V600R008C10	V200R014C50
		V600R008C00	V200R001C00
		V600R007C00	V100R009C00
		V600R006C00	Earlier than U2000
		V600R005C00	V100R009C00
		V600R003C01	
		V600R003C00	
		V600R002C02	
		V600R002C00	
		V100R006C05	
		V100R006	
		V100R005	
		V100R003	
		V100R002	
	BGW9916	V100R002C20	V200R016C50
		V100R002C10	V200R015C60
		V100R001C10	V200R014C60
		V100R001C00	V200R014C50
	MA5200G	V300R003	Earlier than U2000
		V300R002	V100R009C00
		V200R003	
	MA5200E/F	V100R007	Earlier than U2000 V100R009C00
VNE series	VNE1000	V100R002C00	V200R015C60
		V100R001C00	V200R015C60
	VNE9000	V100R003C00	V200R016C50

Category	Equipment	Software Version	First U2000 Version Supported
	VSIG9800	V100R003C00	V200R016C50

12.13 R/AR Series Equipment

The following table lists the R/AR series equipment supported.

Table 12-16 Manageable R/AR series equipment

Equipment	Software Version	First U2000 Version Supported
R1600	V100R001	Earlier than U2000 V100R009C00
	V200R007	Earlier than U2000 V100R009C00
R2500	V100R001	Earlier than U2000 V100R009C00
R2600	V200R007	Earlier than U2000 V100R009C00
AR18	V100R001 V100R002 V200R007	Earlier than U2000 V100R009C00
AR28	V200R007 V300R003	Earlier than U2000 V100R009C00
AR150	V200R007C00	V200R015C60
	V200R006C10	V200R015C50
	V200R005C30	V200R014C60
	V200R005C20	V200R014C50
	V200R005C10	V200R001C00
	V200R005C00	V100R009C00
	V200R003C00 V200R002C02 V200R002C01 V200R002C00	Earlier than U2000 V100R009C00
AR200	V200R007C00	V200R015C60
	V200R006C10	V200R015C50

Equipment	Software Version	First U2000 Version Supported
	V200R005C70	V200R014C60
	V200R005C30	
	V200R005C20	V200R014C50
	V200R005C10	V200R001C00
	V200R005C00	V100R009C00
	V200R003C00	Earlier than U2000
	V200R002C02	V100R009C00
	V200R002C01	
	V200R002C00	
AR1200	V200R007C00	V200R015C60
	V200R006C10	V200R015C50
	V200R005C30	V200R014C60
	V200R005C20	V200R014C50
	V200R005C10	V200R001C00
	V200R005C00	V100R009C00
	V200R001C00	Earlier than U2000
AR2200	V200R001C01	V100R009C00
	V200R001C02	
	V200R007C00	V200R015C60
	V200R006C10	V200R015C50
	V200R005C30	V200R014C60
	V200R005C20	V200R014C50
	V200R005C10	V200R001C00
AR3200	V200R005C00	V100R009C00
	V200R001C00	Earlier than U2000
	V200R001C01	V100R009C00
	V200R001C02	
	V200R006C10	V200R015C50
	V200R005C30	V200R014C60
	V200R005C20	V200R014C50
	V200R005C10	V200R001C00

Equipment	Software Version	First U2000 Version Supported
	V200R005C00	V100R009C00
	V200R001C00 V200R001C01 V200R001C02	Earlier than U2000 V100R009C00
AR3600	V200R006C10	V200R015C50
AR46	V300R003	Earlier than U2000 V100R009C00
AR19	V200R007	Earlier than U2000 V100R009C00
AR29	V300R003	Earlier than U2000 V100R009C00
AR49	V300R003	Earlier than U2000 V100R009C00
SRG1300	V200R002C02	Earlier than U2000 V100R009C00
	V200R003C00	Earlier than U2000 V100R009C00
	V200R005C00	V200R014C50
	V200R005C10	V200R014C50
	V200R005C20	V200R014C50
	V200R005C30	V200R014C60
SRG2300	V200R002C02	Earlier than U2000 V100R009C00
	V200R003C00	Earlier than U2000 V100R009C00
	V200R005C00	V200R014C50
	V200R005C10	V200R014C50
	V200R005C20	V200R014C50
	V200R005C30	V200R014C60
SRG3300	V200R002C02	Earlier than U2000 V100R009C00
	V200R003C00	Earlier than U2000 V100R009C00
	V200R005C00	V200R014C50

Equipment	Software Version	First U2000 Version Supported
	V200R005C10	V200R014C50
	V200R005C20	V200R014C50
	V200R005C30	V200R014C60

12.14 RM9000 Series Equipment

The following table lists the RM9000 series equipment supported.

Table 12-17 RM9000 series equipment

Category	Equipment	Software Version
RM9000	RM9000	V200R003C05

12.15 Switch Series Equipment

The following table lists the switch equipment supported.

Table 12-18 Manageable switch series equipment

Category	Equipment	Software Version	First U2000 Version Supported
S series	Quidway S2300	V200R008C00	V200R015C60
		V200R007C00	V200R014C60
		V200R006C00	Earlier than U2000
		V200R005C00	V100R009C00
		V200R003C00	
		V100R006C05	
		V100R006	
		V100R005	
		V100R003	
		V100R002	
	Quidway S3300	V100R006C05	Earlier than U2000
	V100R006	V100R009C00	
	V100R005		
	V100R003		
	V100R002		

Category	Equipment	Software Version	First U2000 Version Supported
Quidway S5300	Quidway S5300	V200R010C00	V200R016C60
		V200R009C00	V200R016C50
		V200R008C10	V200R016C50
		V200R008C00	V200R015C60
		V200R007C00	V200R014C60
		V200R006C00	Earlier than U2000 V100R009C00
		V200R005C00	
		V200R003C02	
		V200R003C00	
		V200R002C00	
Quidway S9300	Quidway S9300	V200R001C00	
		V100R006	
		V100R005	
		V100R003	
		V100R002	
		V200R010C00	V200R016C60
		V200R009C00	V200R016C50
		V200R008C10	V200R016C50
		V200R008C00	V200R015C60
		V200R007C00	V200R014C60
Quidway S2700	Quidway S2700	V200R006C00	Earlier than U2000 V100R009C00
		V200R005C00	
		V200R003C00	
		V200R002C00	

Category	Equipment	Software Version	First U2000 Version Supported
		V200R006C00 V200R005C00 V200R003C00 V100R006 V100R005	Earlier than U2000 V100R009C00
	Quidway S3700	V200R003C00 V200R002C00 V200R001C00 V100R006 V100R005	Earlier than U2000 V100R009C00
	Quidway S5700	V200R010C00 V200R009C00 V200R008C00 V200R007C00	V200R016C60 V200R016C50 V200R015C60 V200R014C60
		V200R006C00 V200R005C00 V200R003C00 V200R002C00 V200R001C00 V100R006 V100R005	Earlier than U2000 V100R009C00
	Quidway S7700	V200R010C00 V200R009C00 V200R008C00 V200R007C00	V200R016C60 V200R016C50 V200R015C60 V200R014C60
		V200R006C00 V200R005C00 V200R003C00 V200R002C00 V200R001C00 V100R006 V100R003	Earlier than U2000 V100R009C00
	Quidway S6700	V200R010C00 V200R009C00	V200R016C60 V200R016C50

Category	Equipment	Software Version	First U2000 Version Supported
		V200R008C00	V200R015C60
		V200R007C00	V200R014C60
		V200R006C00	Earlier than U2000
		V200R005C00	V100R009C00
		V200R003C00	
		V200R002C00	
		V200R001C00	
		V100R006	
	Quidway S9700	V200R010C00	V200R016C60
		V200R009C00	V200R016C50
		V200R008C00	V200R015C60
		V200R007C00	V200R014C60
		V200R006C00	Earlier than U2000
		V200R005C00	V100R009C00
		V200R003C00	
		V200R002C00	
		V200R001C00	
	Quidway S12700	V200R010C00	V200R016C60
		V200R009C00	V200R016C50
		V200R008C00	V200R015C60
		V200R007C00	V200R014C60
		V200R006C00	Earlier than U2000
		V200R005C00	V100R009C00
	Quidway S6300	V200R010C00	V200R016C60
		V200R009C00	V200R016C50
		V200R008C00	V200R015C60
		V200R007C00	V200R014C60
		V200R006C00	Earlier than U2000
		V200R005C00	V100R009C00
		V200R003C00	
		V200R002C00	
		V200R001C00	
		V100R006	

Category	Equipment	Software Version	First U2000 Version Supported
	Quidway E652	V200R010C00	V200R016C60
		V200R009C00	V200R016C50
		V200R008C00	V200R015C60
	Quidway E628	V200R010C00	V200R016C60
		V200R009C00	V200R016C50
		V200R008C00	V200R015C60
	S8500	V100R006	Earlier than U2000 V100R009C00
	S6500	V200R005	Earlier than U2000 V100R009C00
	S5600	V100R002 V100R001	Earlier than U2000 V100R009C00
	S5500	V100R002	Earlier than U2000 V100R009C00
	S5000	V100R001	Earlier than U2000 V100R009C00
	S3900	V100R002 V100R001	Earlier than U2000 V100R009C00
	S3500	V200R001 V100R003 V100R002 V100R001	Earlier than U2000 V100R009C00
	S3000	V200R001 V100R001	Earlier than U2000 V100R009C00
	S2000	V300R001 V200R005 V200R003 V100R001	Earlier than U2000 V100R009C00
CX200D series	Quidway CX200D	V200R003C00 V200R002C02	Earlier than U2000 V100R009C00
	CE series	V200R001C00	V200R016C50
		V100R006C00	V200R015C60

Category	Equipment	Software Version	First U2000 Version Supported
		V100R005C00	V200R015C50
		V100R005C10	
		V100R003C00	V200R014C60
		V100R002C00	Earlier than U2000
		V100R001C00	V100R009C00
	CE6800	V200R001C00	V200R016C50
		V100R006C00	V200R015C60
		V100R005C00	V200R015C50
		V100R005C10	
		V100R003C00	V200R014C60
		V100R002C00	Earlier than U2000
		V100R001C00	V100R009C00
		V100R003C00	V200R014C60
	CE7800	V200R001C00	V200R016C50
		V100R006C00	V200R015C60
		V100R005C00	V200R015C50
		V100R005C10	
		V100R003C00	V200R014C60
	CE8800	V200R001C00	V200R016C50
		V100R006C00	V200R015C60
	CE12800	V200R001C00	V200R016C50
		V100R006C00	V200R015C60
		V100R005C00	V200R015C50
		V100R005C10	
		V100R003C00	V200R014C60
		V100R002C00	Earlier than U2000
		V100R001C00	V100R009C00

12.16 VoIP Gateway Equipment

The following table lists the VoIP gateway equipment supported.

Table 12-19 VoIP gateway equipment

Category	Equipment	Software Version
VoIP gateway	VG10	Earlier than U2000 V100R009C00
	VG20	Earlier than U2000 V100R009C00
	VG80	Earlier than U2000 V100R009C00
	XE series	Earlier than U2000 V100R009C00

12.17 Security Series Equipment

For positioning of U2000 mapping security NEs, see [here](#).

The following table lists the security series equipment supported.

Table 12-20 Security series equipment

Category	Equipment	Software Version	First U2000 Version Supported
Eudemon	Eudemon 8040	V300R001C05	Earlier than V100R009C00
		V300R001C06	
	Eudemon 8080	V300R001C05	Earlier than V100R009C00
		V300R001C06	
	Eudemon 1000	V200R006C02	Earlier than V100R009C00
	Eudemon 500	V200R006C02	Earlier than V100R009C00
	Eudemon 300	V200R006C02	Earlier than V100R009C00
	Eudemon 8080E	V500R001C00	V200R015C50
		V100R001C01	Earlier than V100R009C00
		V100R001C05	
		V100R002C00	
		V100R003C00	
		V200R001C00	
		V200R001C01	
Eudemon	8160E	V500R001C00	V200R015C50
		V100R001C01	Earlier than V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
Eudemon 8000E-X		V100R001C05	
		V100R002C00	
		V100R003C00	
		V200R001C00	
		V200R001C01	
	Eudemon 8000E-X	V500R001C00	V200R015C50
		V200R001C00	Earlier than V100R009C00
		V200R001C01	
		V300R001C00	
	Eudemon 6080E	V100R001C00	Earlier than V100R009C00
Eudemon 1000E	Eudemon 1000E	V100R002C01	Earlier than V100R009C00
		V100R003C01	
		V100R005C00	
		V200R001C00	
	Eudemon 100E	V200R007C01	Earlier than V100R009C00
	Eudemon 200S	V200R007C01	Earlier than V100R009C00
	Eudemon 200E-B	V100R002C00	Earlier than V100R009C00
		V100R005C00	
		V300R001C00	
Eudemon 200E-C	Eudemon 200E-C	V100R002C00	Earlier than V100R009C00
		V100R005C00	
		V300R001C00	
	Eudemon 200E-F	V100R002C00	Earlier than V100R009C00
		V100R005C00	
		V300R001C00	
	Eudemon 200E-BW	V100R005C00	Earlier than V100R009C00
		V300R001C00	

Category	Equipment	Software Version	First U2000 Version Supported
NGFW	Eudemon 200E-F-D	V100R002C00	Earlier than V100R009C00
		V100R005C00	
		V300R001C00	
	Eudemon 200E-X	V100R005C00	Earlier than V100R009C00
		V300R001C00	
	Eudemon 1000E-N	V100R001C00	V200R015C50
	Eudemon 1000E-X	V200R001C00	Earlier than V100R009C00
		V200R002C00	
		V300R001C00	
	Eudemon 1000E-V	V500R001C10	V200R015C60
	vRouter 6000V	V500R001C10	V200R015C60
USG	Eudemon 200E-N	V100R001C10	V200R001C00
		V100R001C20	V200R014C60
		V500R001C00	V200R015C50
	Eudemon 1000E-N	V100R001C10	V200R001C00
		V100R001C20	V200R014C60
		V500R001C00	V200R015C50
	LE1D2FW0 OS01	V100R001C10	V200R001C00
		V100R001C20	V200R014C60
		V500R001C00	V200R015C50
	USG9100	V100R001C00	Earlier than V100R009C00
	USG9300	V500R001C00	V200R015C50
		V100R001C01	Earlier than V100R009C00
		V100R001C05	
		V100R002C00	
		V100R003C00	
		V200R001C00	
		V200R001C01	

Category	Equipment	Software Version	First U2000 Version Supported
	USG9500	V500R001C00	V200R015C50
		V200R001C00	Earlier than V100R009C00
		V200R001C01	
		V300R001C00	
	USG5100	V100R003C01	Earlier than V100R009C00
		V100R005C00	
		V300R001C00	
	USG5300	V100R001C00	Earlier than V100R009C00
		V100R002C01	
		V100R003C01	
		V100R005C00	
		V200R001C00	
	USG5500	V200R001C00	Earlier than V100R009C00
		V200R002C00	
		V300R001C00	
	USG6600	V100R001C00	V100R009C00
	USG5520S	V300R001C00	Earlier than V100R009C00
	USG2100	V100R001C03	V100R009C00
		V100R002C01	Earlier than V100R009C00
		V100R003C01	
		V100R003C03	
		V100R005C00	
		V300R001C00	
	USG3000	V100R001C03	Earlier than V100R009C00
	USG2200	V100R002C01	Earlier than V100R009C00
		V100R003C01	
		V100R005C00	
		V300R001C00	
	USG50	V100R001C03	Earlier than V100R009C00

Category	Equipment	Software Version	First U2000 Version Supported
SRG	SRG2200	V100R001C01	Earlier than V100R009C00
		V100R002C01	
		V100R002C02	
	SRG20-10	V100R001C03	Earlier than V100R009C00
	SRG20-12 W	V100R002C01	Earlier than V100R009C00
		V100R003C01	
		V100R005C00	
	SRG20-15 W	V100R002C01	Earlier than V100R009C00
		V100R003C01	
		V100R005C00	
	SRG20-11	V100R002C01	Earlier than V100R009C00
		V100R003C01	
		V100R005C00	
	SRG20-12	V100R002C01	Earlier than V100R009C00
		V100R003C01	
		V100R005C00	
	SRG20-15	V100R002C01	Earlier than V100R009C00
		V100R003C01	
		V100R005C00	
	SRG20-20	V100R005C00	Earlier than V100R009C00
		V200R002C01	
	SRG20-21	V200R002C01	Earlier than V100R009C00
		V100R005C00	
	SRG20-30	V200R002C01	Earlier than V100R009C00
		V100R005C00	
	SRG20-31	V200R002C01	Earlier than V100R009C00
		V100R005C00	
	SRG20-31-D	V200R002C01	Earlier than V100R009C00
		V100R005C00	

Category	Equipment	Software Version	First U2000 Version Supported
	SRG1200	V100R001C01	Earlier than V100R009C00
		V100R002C01	
		V100R002C02	
	SRG3200	V100R002C01	Earlier than V100R009C00
		V100R002C02	
ASG	ASG2100	V100R001C00	Earlier than V100R009C00
	ASG2200	V100R001C00	
	ASG2600	V100R001C00	
	ASG2800	V100R001C00	
EGW	EGW2100	V100R001C02	Earlier than V100R009C00
		V100R001C20	
	EGW2200	V100R001C02	
		V100R001C20	
	EGW3200	V100R001C02	
		V100R001C20	
SIG	SIG9800	V200R002C01	Earlier than V100R009C00
		V200R002C02	
		V200R003C00	
		V300R001C00	
		V300R003C00	
		V300R005C00	
		V300R006C00	
		V300R006C10	
		V300R006C20	
	SIG9800-X3	V300R001C00	Earlier than V100R009C00
		V300R003C00	
		V300R005C00	
		V300R006C00	
		V300R006C10	
		V300R006C20	

Category	Equipment	Software Version	First U2000 Version Supported
SIG9800-X8	V300R001C00	Earlier than V100R009C00	
	V300R003C00	V200R014C60	
	V300R005C00	V200R015C50	
	V300R006C00	V200R015C60	
	V300R006C10	V200R016C50	
	V300R006C20	V200R016C60	
	V300R001C00	Earlier than V100R009C00	
	V300R003C00	V200R014C60	
	V300R005C00	V200R015C50	
	V300R006C00	V200R015C60	
	V300R006C10	V200R016C50	
	V300R006C20	V200R016C60	
SIG Server	V200R002C01	Earlier than V100R009C00	
	V200R002C02		
	V200R003C00		
	V300R001C00		
	V300R003C00	V200R014C60	
	V300R005C00	V200R015C50	
	V300R006C00	V200R015C60	
	V300R006C10	V200R016C50	
	V300R006C20	V200R016C60	
	V200R002C02	Earlier than V100R009C00	
RADIUS Proxy	V200R003C00	V200R014C60	
	V300R001C00	V200R015C50	
	V300R003C00	V200R015C60	
	V300R005C00	V200R016C50	
	V300R006C00	V200R016C60	
	V300R006C10	V200R016C50	
	V300R006C20	V200R016C60	

Category	Equipment	Software Version	First U2000 Version Supported
	URL Classify Server	V100R001C00	Earlier than V100R009C00
		V100R002C01	
		V300R001C00	
		V300R003C00	V200R014C60
		V300R005C00	V200R015C50
		V300R006C00	V200R015C60
	NE40E/80E-FW	V300R006C10	V200R016C50
		V300R006C20	V200R016C60
		V500R008C00	Earlier than V100R009C00
		V500R008C01	
	NE80E-FW	V500R008C02	
		V500R008C03	
		V500R008C00	
		V500R008C01	
	OP-Bypass	V500R008C02	Earlier than V100R009C00
		V500R008C03	
	OP-Bypass	V100R001C00	Earlier than V100R009C00
	SVN	SVN3000	Earlier than V100R009C00
		V100R002C02	
		SVN2200	
		V200R001C00SPC300	
		V200R001C01	
		SVN5300	
	SVN5500	V200R001C00SPC300	V200R014C60
		V200R001C01	
		SVN5600	
	SVN5800	V200R003C00	V200R014C60
		V200R003C00	V200R014C60

Category	Equipment	Software Version	First U2000 Version Supported
NIP	NIP6610-AC NIP6320-AC NIP6320D-AC NIP6330-AC NIP6330D-AC NIP6620-AC NIP6620D-AC NIP6650-AC NIP6650-DC NIP6650D-AC NIP6650D-DC NIP6680-AC NIP6680-DC NIP6830-BASE-AC NIP6830-BASE-DC	V500R001C00	V200R015C50
CE	CE-FWA CE-IPSA	V500R001C00	V200R015C50
SeMG9811	SeMG9811-X3 SeMG9811-X8 SeMG9811-X16	V300R001C01 V300R001C00	V200R015C50

12.18 iCache Series Equipment

The following table lists the iCache series equipment supported.

Table 12-21 iCache series equipment

Category	Equipment	Software Version
iCache	iCache9200 RSS	V100R002C00
		V200R001C00
	iCache9200 DSS	V100R002C00
		V200R001C00
	iCache9200 MSS	V100R002C00
		V200R001C00
	iCache9200 CSS	V100R002C00
		V200R001C00

13 Distributed U2000 System

About This Chapter

Different from the traditional centralized U2000 system, the distributed system is composed of independent sets of U2000, which can manage ultra-large-scale networks that contain 50,000 equivalent NEs. A maximum of 80,000 equivalent NEs can be managed when the U2000 manages only PTN networks.

13.1 Solution Overview

Driven by the constant expansion of networks, the single-server U2000 system has hit a bottleneck in management capacity. To help customers manage extra-large networks, Huawei launches the distributed U2000 system.

13.2 Network Structure

This topic describes the network scheme and software of a U2000 distributed system.

13.3 Configuration Requirements

This topic describes the hardware and software configurations required for the U2000 server in a distributed system. The standard hardware delivery configurations for the virtual machine solution are E9000 blade servers. The U2000 also supports a decoupling solution, that is, users provide a virtualization environment and Huawei provides a U2000 installation solution.

13.4 NBI Capabilities

In a distributed system, the U2000 NBI provides rich interface management functions to meet different OSS integration requirements.

13.5 Introduction to the Reliability and Protection Solution

Reliability design ensures that the product will be in service for many years because measures have been taken to prevent potential risks.

13.6 Reliability Indicator

This topic describes the indicators of the reliability design.

13.7 Management Capability

This topic describes the management capability of the U2000 in a distributed system.

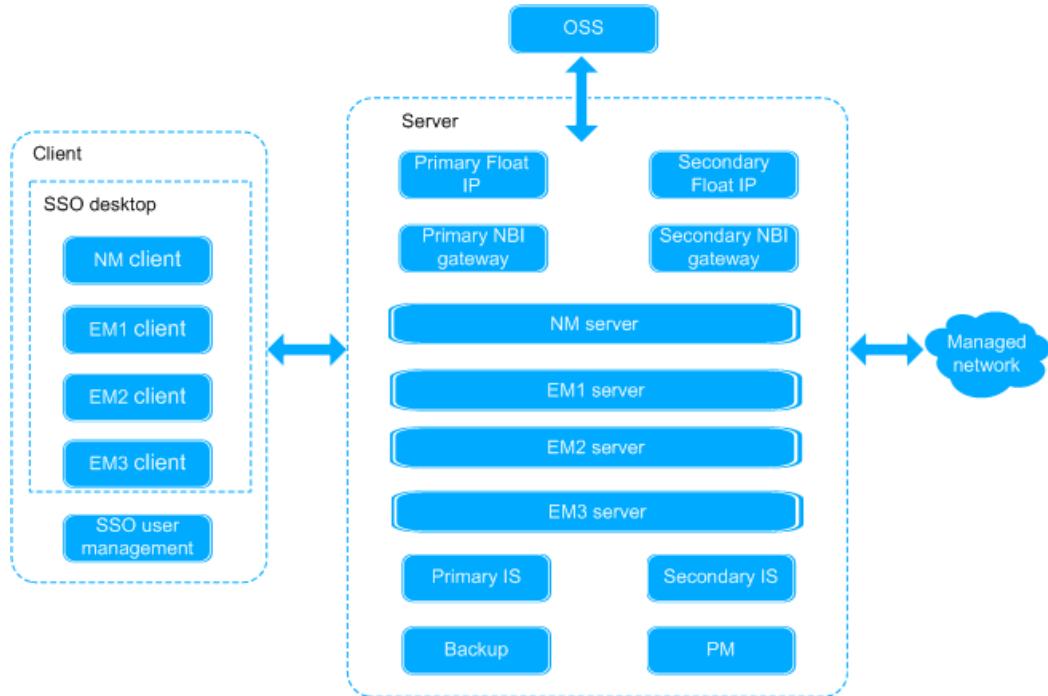
13.8 Performance Indicators

This topic describes the performance indicators of the U2000.

13.1 Solution Overview

Driven by the constant expansion of networks, the single-server U2000 system has hit a bottleneck in management capacity. To help customers manage extra-large networks, Huawei launches the distributed U2000 system.

Figure 13-1 Components of a U2000 distributed system



Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. The U2000 distributed system involves various nodes, each of which runs on a separate operating system.

Table 13-1 Functions of server nodes involved in the U2000 distributed deployment mode

Node Type	Quantity	Function
NBI Gateway	2	NBI gateway node that can achieve dual-system hot backup for some high availability sites.
NM	1	Centralized network management node that implements unified network management by providing functions, such as alarm monitoring, NE upgrade task monitoring, physical topology, cross-EM fiber/cable, service template, E2E service, and performance (except transport NEs) management, and a few inventory report functions.

Node Type	Quantity	Function
EM	1..n	NE management node that manages a subnet by providing NE configuration, alarm/topology/security/inventory/NE software management, NE batch operation, and transport NE performance management functions. If an EM system is installed on a four-CPU blade server, the EM system manages a maximum of 16,000 equivalent NEs. A maximum of five EM systems can be deployed in a distributed system.
IS	2	Integration server that is used for account management, SSO, and server address management. The two nodes protect each other by means of dual-system hot backup.
Backup	1	Data backup node that stores backup U2000 data, such as NE and U2000 database data.
Float IP	2	Optional nodes that map two NBI gateways to a single floating IP address so that the gateway nodes use the same IP address. If the two nodes are not deployed, the OSS determines the NBI gateway to be connected to by itself.
PM	1	Performance management node, as performance data acquisition and storage performance, including real-time performance of mining, historical performance data collection, data aggregation, and TCA alarms view, and export performance of NBI file.

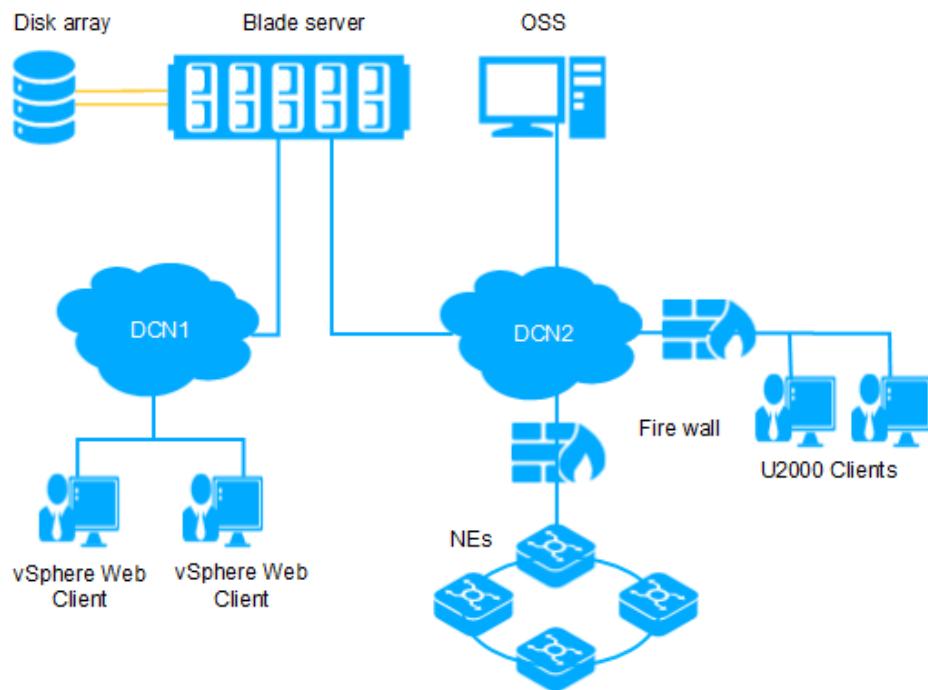
13.2 Network Structure

This topic describes the network scheme and software of a U2000 distributed system.

VMware Virtualization Platform

A U2000 distributed system uses a blade server in hardware, on which all blades have VMware installed. VMware is used for partitioning a blade server into multiple virtual servers whose data is stored in the disk array. VMs use the CPU and memory resources of each blade for computing. Systems such as U2000 element managers (EMs) and U2000 network manager (NM) are independently installed on the virtual machines. [Figure 13-2](#) shows a U2000 distributed network.

Figure 13-2 U2000 distributed system network



Terms

- **Blade server:** Each blade server involves multiple blades (computing nodes), each serving as a computer. A set of VMware ESXi is installed on a blade, which functions as a virtual server.
- **vCenter Server Appliance (VCSA):** VCSA indicates the VMware virtualization management software installed in the VM. The VM with the VCSA software installed is a VCSA VM.
- **vSphere Web Client:** Indicates the web application installed on the VCSA. You can visit the VCSA through the vSphere Web Client to operate ESXi hosts and VMs.

13.3 Configuration Requirements

This topic describes the hardware and software configurations required for the U2000 server in a distributed system. The standard hardware delivery configurations for the virtual machine solution are E9000 blade servers. The U2000 also supports a decoupling solution, that is, users provide a virtualization environment and Huawei provides a U2000 installation solution.

Hardware Configurations (VMware, E9000 Blade Server)

- A distributed U2000 deploy on the VMware platform.
- **Table 13-2** list the hardware configurations required for the U2000 server in a distributed system.
- The switch board on a blade server provides 10GE interfaces and can be interconnected only with gigabit or 10 gigabit network interfaces. Ensure that each of the two switches connected to the switch board on the blade server has at least two gigabit network interfaces.

- The disk array must be configured. **Table 13-3** list the disk array configurations required for the U2000 server in a distributed system.

Table 13-2 Hardware configurations

Network Scale	E9000 Blade Configurations	H242 V3 Blade Configurations
< 50,000 equivalent NEs	Eight CH242 V3 blades	<ul style="list-style-type: none"> CPU: 4 x 14-core 2.0 GHz CPUs Memory: 192 GB Hard disk: 2 x 600 GB
50,000-80,000 equivalent NEs (only supported in PTN networks)		

The network scale depends on the number of EMs deployed. Four, and five EMs are used in deploying 50000, and 80,000 equivalent NEs, respectively. When 80,000 equivalent NEs are deployed, the VCSA and EM5 nodes are configured on the same blade.

Figure 13-3 VM configurations when 50,000 equivalent NEs are deployed

backup blade	VM	EM_1	IS_1	NBI_GW_1	Float_IP_1	EM_2	IS_2	NBI_GW_2	Float_IP_2	EM_3	Backup	EM_4	PM	VCSA	Win2008
	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM
ESXi	ESXi		ESXi			ESXi		ESXi		ESXi		ESXi		ESXi	
blade8	blade7		blade6			blade5		blade4		blade3		blade2		blade1	
E9000															

Figure 13-4 VM configurations when 50,000-80,000 equivalent NEs are deployed

backup blade	VM	EM_1	IS_1	NBI_GW_1	Float_IP_1	EM_2	IS_2	NBI_GW_2	Float_IP_2	EM_3	Backup	EM_4	PM	EM_5	VCSA	Win2008
	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	VM	
ESXi	ESXi		ESXi			ESXi		ESXi		ESXi		ESXi		ESXi		
blade8	blade7		blade6			blade5		blade4		blade3		blade2		blade1		
E9000																

Table 13-3 Configurations of the disk array

Hardware Configuration Item	Disk Array Hardware Version	Capacity
Delivered: OceanStor 5500 V3	-	48 GB memory, 24 x 900 GB
Compatible: OceanStor S3900 NOTE An M200 controller enclosure is delivered with disk arrays.	V100R005C02 V100R002C00	16 GB memory, 24 x 900 GB

Hardware Configurations of Virtual Machines

Table 13-4 lists the VM configurations required for the U2000 in a distributed system.

Table 13-4 VM configurations

Item	Configuration
Backup	<ul style="list-style-type: none"> ● Number of virtual CPUs per VM: 8 ● Virtual memory per VM: 8 GB ● Virtual disk space per VM: 1600 GB ● Virtual disk format: Thin Provision ● Physical disk's reserved space per VM: 3840 GB <p>NOTE</p> <p>Physical disk's reserved space = Virtual disk space + Space reserved for cloning (virtual disk space x 1.2) + Space reserved for snapshots (virtual disk space x 0.2)</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 750

Item	Configuration
IS	<ul style="list-style-type: none"> ● Number of virtual CPUs per VM: 4 ● Virtual memory per VM: 8 GB ● Virtual disk space per VM: 100 GB ● Virtual disk format: Thick Provision Lazy Zeroed ● Physical disk's reserved space per VM: 240 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for cloning (virtual disk space} \times 1.2) + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 200
Float IP	<ul style="list-style-type: none"> ● Number of virtual CPUs per VM: 2 ● Virtual memory per VM: 8 GB ● Virtual disk space per VM: 25 GB ● Virtual disk format: Thick Provision Lazy Zeroed ● Physical disk's reserved space per VM: 60 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for cloning (virtual disk space} \times 1.2) + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 200
NBI_GW	<ul style="list-style-type: none"> ● Number of virtual CPUs per VM: 8 ● Virtual memory per VM: 8 GB ● Virtual disk space per VM: 50 GB ● Virtual disk format: Thick Provision Lazy Zeroed ● Physical disk's reserved space per VM: 120 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for cloning (virtual disk space} \times 1.2) + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 200

Item	Configuration
NM	<ul style="list-style-type: none"> ● Number of virtual CPUs per VM: 32 ● Virtual memory per VM: <ul style="list-style-type: none"> - 50,000 equivalent NEs: 48 GB - 80,000 equivalent NEs: 64 GB ● Virtual disk space per VM: 500 GB ● Virtual disk format: Thick Provision Lazy Zeroed ● Physical disk's reserved space per VM: 1200 GB <p>NOTE Physical disk's reserved space = Virtual disk space + Space reserved for cloning (virtual disk space x 1.2) + Space reserved for snapshots (virtual disk space x 0.2)</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 1600
EM	<ul style="list-style-type: none"> ● Number of virtual CPUs per VM: 32 ● Virtual memory per VM: <ul style="list-style-type: none"> - 50,000 equivalent NEs: 48 GB - 80,000 equivalent NEs: 64 GB ● Virtual disk space per VM: 400 GB ● Virtual disk format: Thick Provision Lazy Zeroed ● Physical disk's reserved space per VM: 960 GB <p>NOTE Physical disk's reserved space = Virtual disk space + Space reserved for cloning (virtual disk space x 1.2) + Space reserved for snapshots (virtual disk space x 0.2)</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 1600

Item	Configuration
PM	<ul style="list-style-type: none"> ● Number of virtual CPUs per VM: 32 ● Virtual memory per VM: 40 GB ● Virtual disk space per VM: 500 GB ● Virtual disk format: Thick Provision Lazy Zeroed ● Physical disk's reserved space per VM: 1200 GB <p>NOTE $\text{Physical disk's reserved space} = \text{Virtual disk space} + \text{Space reserved for cloning (virtual disk space} \times 1.2) + \text{Space reserved for snapshots (virtual disk space} \times 0.2)$</p> <ul style="list-style-type: none"> ● Disk IOPS (Input/Output Operations Per Second): 1600

NOTE

- The CPU virtualization ratio must be disabled, that is, the number of virtual CPUs (vCPUs) that can be allocated on a physical host cannot exceed the number of physical CPUs on the host. Otherwise, the U2000 performance will be downgraded.

The CPU virtualization ratio is a proportion of **physical CPUs** to **vCPUs**. For example, if 32 physical CPUs are available and the virtualization ratio is 1:5, the number of vCPUs that can be allocated is 160 (32×5). At this moment, the vCPU performance will be downgraded.

- The memory virtualization ratio must be disabled, that is, the size of virtual memory that can be allocated on a physical host cannot exceed the size of physical memory on the host. Otherwise, the U2000 performance will be downgraded.

The memory virtualization ratio is a proportion of **physical memory size** to **virtual memory size**. For example, if 32 GB physical memory is available and the virtualization ratio is 1:5, the size of virtual memory that can be allocated is 160 GB ($32 \text{ GB} \times 5$). At this moment, the virtual memory performance will be downgraded.

Software Configurations of Virtual Machines

Table 13-5 lists the software configurations required for the U2000 server in a distributed system.

Table 13-5 Software configurations

Item	Configuration
Virtual machine server version	<ul style="list-style-type: none"> ● Recommended: VMware vSphere ESXi 6.5 ● Compatible: VMware vSphere ESXi 5.5
OS	SUSE Linux Enterprise Server 11 SP3
Database	SYBASE 15.7 with EBF26397 + SP138

Software configurations of the vSphere Web Client

Table 13-6 Software configurations of the vSphere Web Client

OS	Browser
Windows	<ul style="list-style-type: none">● Mozilla Firefox 34 to 49● Google Chrome 39 to 53
Mac OS	<ul style="list-style-type: none">● Mozilla Firefox 34 to 49● Google Chrome 39 to 53

Configurations for the U2000 client

Table 13-7 shows the hardware and software configuration for the U2000 client.

Table 13-7 Software and hardware configurations for the U2000 client

Platform	Hardware Configuration	Software Configuration	Browser Version
Windows	Minimal configuration requirements: Intel E2140: (dual-core) (1.6 GHz or greater); memory (4 GB or greater)	Recommended OS: <ul style="list-style-type: none">● Windows 10 Professional (64-bit version)● Windows 10 Professional (32-bit version)● Windows 7 Professional (64-bit version)● Windows 7 Professional (32-bit version) Compatible OS: <ul style="list-style-type: none">● Windows Server 2008 R2 Standard (64-bit version)● Windows Server 2012 R2 Standard (64-bit version)	<ul style="list-style-type: none">● Firefox17.X ESR, Firefox24.X ESR or Firefox31.X ESR● IE11(32-bit version)● IE10(32-bit version)● IE9(32-bit version)

13.4 NBI Capabilities

In a distributed system, the U2000 NBI provides rich interface management functions to meet different OSS integration requirements.

NOTE

In a distributed system, the XML NBI does not support the following functions.

- IP NE test cases, test suites, PW/LSP/VRF ping result queries, and Ethernet LB test result queries
- Traffic policy profile for access equipment.

The following tables show the NBI functions that the equipment in different domains supports.

Table 13-8 NBI functions supported by transport equipment

Interface	Feature	MSTP	Hybrid MSTP	WDM	OTN	Hybrid RTN (TDM)	TDM RTN	Packet RTN	PTN	Marine
XML (MTOSI)	Alarm	√	√	√	√	√	√	√	√	×
	Performance	√	√	√	√	√	√	√	√	×
	Inventory	√	√	√	√	√	√	√	√	×
	Configuration	√	√	√	√	√	√	√	√	×
CORBA	Alarm	√	√	√	√	√	√	√	√	√
	Performance	√	√	√	√	√	√	√	√	√
	Inventory	√	√	√	√	√	√	√	√	√
	Configuration	√	√	√	√	√	√	√	√	×
SNMP	Alarm	√	√	√	√	√	√	√	√	×
Performance NBI	Performance	√	√	√	√	√	√	√	√	×

Table 13-9 NBI functions supported by access equipment

Interface	Feature	MSAN/DSLAM			FTTx	
		Narrowband Port	Broadband Port	FTTH	FTTB/C	
XML (MTOSI)	Alarm	√	√	√	√	√
	Performance	√	×	√	√	√
	Inventory	√	√	√	√	√

Interface	Feature	MSAN/DSLAM		FTTx	
		Narrowband Port	Broadband Port	FTTH	FTTB/C
	Service provisioning	×	√	√	√
CORBA	Alarm	√	√	√	√
SNMP	Alarm	√	√	√	√
Performance text NBI	Performance	√	√	√	√
TL1	Diagnosis	√	√	√	√
	Inventory	√	√	√	√
	Service provisioning	√	√	√	√

Table 13-10 NBI functions supported by IP equipment

Interface	Feature	NE Series	CX Series	Switch	BRAS	ATN	Security Series	PTN
XML (MTOSI)	Alarm	√	√	√	√	√	×	√
	Performance	√	√	×	×	√	×	√
	Inventory	√	√	√	√	√	×	√
	Configuration	√	√	√	√	√	×	√
CORBA	Alarm	√	√	√	√	√	×	√
SNMP	Alarm	√	√	√	√	√	√	√
Performance text NBI	Performance	√	√	√	√	√	×	√

Supported	√
Not supported	×

13.5 Introduction to the Reliability and Protection Solution

Reliability design ensures that the product will be in service for many years because measures have been taken to prevent potential risks.

Table 13-11 shows the U2000 distributed system protection solutions under the Huawei delivery scenario in detail.

Table 13-11 Usage scenarios for the U2000 protection

Protection Type	Protection Solution	Usage Scenario
Hardware protection	Hardware redundancy protection	The U2000 enhances reliability by providing redundancy protection for hardware such as the power supply, fan, switch board, and network adapter.
	Hard disk redundancy backup	A hardware disk group (logical) is composed of multiple hard disks (physical) to provide higher storage performance and data redundancy protection.
	Hot standby protection of key nodes	When a node fails, protection is automatically implemented. For example, when the IS, NBI gateway, or Float IP node fails, hot standby protection takes effect.
	vSphere HA cluster-based protection	By installing the VMware management software, you can define multiple blades as a cluster. When a blade server is damaged, the VMs on the blade will be automatically switched to the failover host for proper running. After the damaged blade is restored to be the same as the previous configuration, the VMs on the failover host are switched back to the repaired blade.
Software protection	Backup	Data backup improves the reliability of the important U2000 data. When a fault occurs on the data, for example, the U2000 or database reports an error, you can use the backup data to restore the data.
	Snapshot protection of virtual machines (VMs)	A VM snapshot is an image of a VM disk file at a specific time point and is used to back up the current system status. When VM system upgrade or patch installation fails and cannot be recovered, you can restore the VM to the previous status using snapshots.

Protection Type	Protection Solution	Usage Scenario
	Process protection	When the U2000 detects unexpected process termination or faults, it automatically handles the problem or notifies users of the problem.
Remote disaster recovery protection	SRM (Recommended)	<p>Configure two sets of U2000 as the protected site and recovery site separately. Based on the VMware Site Recovery Manager (SRM) technology, the U2000 supports vSphere replication (VR) and Array-based replication (ABR) solutions. When the protected site fails or a disaster causing data unrecoverable occurs, you need to manually start the recovery plan in the SRM recovery page to quickly recover the U2000.</p> <p>NOTICE Customers need to purchase the compatible SRM + VR solution from the VMware company by themselves.</p>
	Cold Backup System	Two sets of U2000 are configured as primary and secondary sites. The primary site periodically backs up the U2000 database file, and the secondary site periodically obtains the U2000 database file from the primary site for restoration. The secondary site is ready to take over the live network upon primary site failure.
System security	OS hardening and anti-virus	The U2000 provides hardening tools and anti-virus solutions for the OS to fix vulnerabilities and prevent risks.
	Communication security	Reliable communication protocols and encryption policies are adopted to ensure communication security between network nodes. In addition, DCN protection also improves the reliability of the communication connection between the U2000 and devices.
	U2000 operation security	The U2000 leverages user access control, centralized authentication, audit tracing, and security events and alarms to ensure operation security of the application layer.

Hardware Redundancy

- It is advisable to set up a U2000 distributed system environment with the hardware that supports redundancy.
- Hardware redundancy is provided by blade server hardware and disk arrays. Specific hardware redundancy types include power supply redundancy, fan redundancy, switch board 1+1 redundancy, and management module redundancy for the blade server. The redundancy types available to disk arrays include controller redundancy, power supply

redundancy and so on. When this hardware is damaged, protection is automatically implemented.

- Redundancy involves instant protection switching without impact on the U2000.

Hard Disk Redundancy Backup

The hard disk redundancy backup function helps to improve the reliability of disk data on the U2000 server.

RAID Technologies Used by the U2000

Redundant array of independent disks (RAID) is a technology that is used to form a logical hard disk group by combining multiple independent physical hard disks in different modes. In this way, RAID provides a storage capability higher than that of a single hard disk and implements the data redundancy protection. The different modes of forming hard disk groups are called RAID levels.

- RAID 0: consists of more than two hard disks by summing up their capacities. In a disk array group, these hard disks are concurrently processed. During data access, data is read and written respectively in each hard disk at the same time. This greatly improves the efficiency of accessing and writing data.
- RAID 1: RAID 1, also called disk mirroring, mirrors the data of one hard disk to another hard disk. Without affecting performance, disk mirroring ensures the reliability and restorability of the system to the greatest extent. This provides a strong capability of data redundancy. RAID 1 requires at least two hard disks.
- RAID 10: a combination of RAID 0 and RAID 1. Two hard disks are used to configure RAID 1 and two hard disk groups for RAID 1 are used to configure RAID 0. RAID 10 features the advantages of both RAID 0 and RAID 1. Four hard disks are required to configure a RAID 10.

Principles of Planning the Hard Disk Redundancy Backup

With reference to [Table 13-12](#), plan the hard disk redundancy backup according to the server hardware and the number of hard disks in the U2000 server.

Table 13-12 Recommended RAID level

Server Hardware	Configuration Principle
E9000 server	Add the two hard disks of each compute node to RAID 1 using the LSI SAS3108 RAID controller card installed on the E9000.
Disk array	<ul style="list-style-type: none">● OceanStor 5500 V3 (24 x 900GB): The disk array is configured with 24 hard disks. Configure disk domains whose hot standby policy priority is high and then configure the storage pool to RAID 10.● OceanStor S3900: The RAID 10 and hot spare disk are recommended for the disk array where 12 hard disks are configured. Specifically, configure RAID 10 by using any 10 hard disks and use the remaining 2 as hot spare disks.

Hot standby protection of key nodes

- The IS, NBI gateway and Float IP nodes support HSB. That is, two identical nodes can stay online at the same time. If one of them fails, the other node takes over services, ensuring service continuity.
- The deployment of two online IS nodes ensures that when either IS node fails, users can still log in to the client after switching the IP address manually. After either IS node fails, NEs cannot be created or deleted, and NE names, IP addresses, and communication parameters and parameters of the northbound interface connecting to the U2000 cannot be modified.
- The deployment of two NBI gateway nodes ensures that when either NBI gateway fails, the OSS can automatically switch to the IP address of the other NBI gateway. HSB for NBI gateways involves no protection switching time. The switching is controlled by the OSS.
- The floating IP address capability (sold separately) enables the U2000 to present only one interworking IP address to the OSS. Every NBI gateway failure is similar to a transient network disconnection (for seconds). The OSS only needs to initiate reconnection, but not switching. The floating IP address capability helps load balance (connections from the OSS) between the two NBI gateway nodes.
- When deploying VMs, deploy the nodes of same type to different blades. If they are deployed on the same blade, the working and protection nodes will both fail upon a hardware failure on the blade.

Hardware Protection based on vSphere HA

The vSphere HA cluster is a protection solution provided by VMware. This solution can be configured only when the U2000 is installed and runs on the VM VMware.

Hardware Protection based on vSphere HA supports local blade protection. When a blade server is damaged, the VMs on the blade will be automatically switched to the failover host for proper running. After the damaged blade is restored to be the same as the previous configuration, the VMs on the failover host are automatically switched back to the repaired blade.

Backup and Restoration

1. Data Backup

- In the U2000 distributed system, data backup needs to be performed separately on each node. If data is backed up while modification is in progress, the backup data may be inconsistent across nodes. Therefore, be sure to back up data on the U2000 distributed system when no one changes configuration data (add or delete NEs, add or delete fibers/cables, provision services, and upload NE data). In addition, the backup must start at the same time on all nodes. Alarm reporting, and performance data collection do not affect the backup.
- After the U2000 is deployed, configure scheduled backup policies on the IS, NM, EM, NBI_GW, Backup and PM nodes, including the backup time, number of data copies reserved, and address of the backup server.
- Data on the two IS nodes needs to be backed up separately. To back up data on the IS nodes, users can run the backup commands or configure a scheduled backup task. Data can be backed up to a remote server.
- Do not store much backup data on the NM or EM nodes because these nodes have limited disk space and it is not reliable enough to store backup data locally. The

U2000 distributed system has a Backup node for storing backup data transferred from all the other nodes. (The SFTP transfer mode is supported.) To restore data from an earlier backup, download the backup from the Backup node. If the IP address of the Backup node is changed, data backup must be re-configured.

2. Data Restoration

- Data needs to be restored in the following situations:
 - The database on a certain node crashes. In this situation, users only need to restore data on that node.
 - Due to user misoperations or disasters, data is lost on multiple nodes. In this situation, users need to restore data for the entire system.
- After database restoration, data on the U2000 is not the latest and tends to be inconsistent with data on the live network. For example, the number of NEs, fiber connections, and NE configurations will be inconsistent between the U2000 and the live network. To prevent the data inconsistency causing service interruption, users must synchronize data immediately from the live network after restoring the database. Uploading backup data to restore data is a best-effort measure, which only restores configurations that have been provisioned to NEs. After the last backup, configurations by the NMS that have not been provisioned to NEs will be lost.

Snapshot protection of VMs

A VM snapshot is a copy of the status and data of a VM at a specified time. When system upgrade or patch installation fails and cannot be recovered, you can perform a rollback using the stored snapshots.

- Generating snapshots: VM snapshots need to be generated before system upgrade or patch installation.
- Managing snapshots: It is recommended that the number of snapshots on a VM be no more than two and the stored time of each snapshot be no more than three days, to avoid occupying the storage space and affecting performance of VMs and hosts.
- Restoring snapshots: When system upgrade or patch installation fails and cannot be recovered, you need to restore the VM using snapshots. Only the status and data of the VM when the snapshots are created can be restored. After restoration, the current VM data is unavailable.

Process Protection

- When the U2000 detects that a process stops abnormally or is faulty, it records system logs. Then, the system restarts the process automatically and ensures that the process is running properly. The system can also generate an alarm that urges a user to manually resolve the problem.
- In the case of an HA system, when the active server is faulty (for example, software applications fail or the database quits unexpectedly), switchover is performed between the active server and the standby server and then the standby server starts to monitor networks.

SRM

You can deploy the same distributed system on the backup site as that on the primary site and use Site Recovery Manager (SRM) to deliver a remote HA protection.

SRM is a disaster recovery solution developed by the VMware. This solution uses virtual machines to achieve policy-based storage and copy. In addition, storage requirements can be automatically allocated and implemented based on policies.

The SRM remote DR solution and the cold backup HA solution cannot be used simultaneously.

Cold Backup System

On the secondary site, you can establish a U2000 Distributed System that is the same as that on the primary site. The Centralized Maintenance Management Tool helps configure the two systems as a remote cold standby HA system, which automatically synchronizes data of the Backup node on the primary site to the Backup node on the remote secondary site in a scheduled manner to implement data synchronization. If the primary site encounters a fault or disaster, the HA system switches services from the primary site to the secondary site to ensure that the U2000 Distributed System runs properly.

OS Hardening and Anti-virus

- The U2000 VMs run the SUSE Linux OS. Generally, the default OS configurations cannot meet security requirements of telecom management systems. For example, by default the OS runs services and opens external communication ports that are redundant or unnecessary for the U2000, and uses Transmission Control Protocol/Internet Protocol (TCP/IP) parameters that make the U2000 vulnerable. Therefore, the OS easily becomes a weakness in the security of the U2000. To ensure that the U2000 runs securely and stably, Huawei releases the U2000 with OS security hardening software and provides default security hardening policies. Security hardening takes effect after you manually import the policy file into the system. For the SUSE Linux OS, the U2000 VMs provide the system hardening tool SetSUSE.
- The OS is vulnerable to viruses, leading to abnormal U2000 running or even system crash.

A virus scan using Symantec, OfficeScan, Mcafee, Avira AntiVir and Kaspersky software is run before the U2000 is released. The U2000 has also passed the OfficeScan compatibility test. The U2000 software package includes OfficeScan to protect the system against viruses. OfficeScan is only applied to the Windows.

Communication Security

- Information is transmitted on networks at the risk of being eavesdropped, tampered, or copied and resent. The U2000 and gateway device adopt the TCP/IP protocol for communication, and the communication channel uses the standard SNMPv3, SSL, SSH, SFTP, or HTTPS protocol for encryption to ensure security.
- You can use a data communication network (DCN) to connect the U2000 to a standby gateway NE (GNE). This improves the reliability of the communication connection between the U2000 and equipment. Only the MSTP, WDM, RTN, PTN, and router series NEs support DCN protection.

The communication between non-GNEs and the U2000 is forwarded by the GNE. In the U2000, you can set the active GNE and standby GNE for NEs in advance. When the communication between the active GNE and the U2000 is interrupted, the U2000 automatically switches to the standby GNE for communication, so that the communication between the U2000 and NEs is not interrupted. When the communication between the U2000 and the active GNE recovers, the U2000 determines whether to use the active GNE again according to the preset revertive mode.

 **NOTE**

For Transport Domain, the recommended number of non-gateway NEs (including non-gateway NEs that connects to the GNE by using the extended ECC) that connect to each GNE is fewer than 50. Once the limit is exceeded, the number of GNEs should be increased.

U2000 Operation Security

- User Access Control: Access control includes user management, automatic lock-out policy, online user monitoring, and user permission division.
- Centralized Authentication: The U2000 provides three user authentication modes: local authentication, Remote Authentication Dial-In User Service (RADIUS) authentication, and Lightweight Directory Access Protocol (LDAP) authentication. Local authentication: The U2000 server implements user management, login authentication, and security policies in a unified manner. Local authentication is the default user authentication management mode provided by the U2000. RADIUS authentication: During user login, the U2000 verifies and authenticates users' login requests through the RADIUS server and authorizes login users based on the permissions of the belonging user group. LDAP authentication: During user login, the U2000 verifies and authenticates users' login requests through the LDAP server and authorizes login users based on the permissions of the belonging user group. LDAP authentication is similar to RADIUS authentication, but the protocols used are different.
- Audit Tracing: The U2000 provides complete log information about running status, security events, and operations and configurations for query and audit, real-time check, analysis, and protection. With the log information, proper measures can be taken if services on live networks are affected by users' operations. Logs of each NE can also be managed by the U2000 in a uniform manner. Based on log impacts on the U2000, logs are divided into security log, operation log, and system log. Logs can be forwarded to a third-party server.
- Security Event Alarms: After the system detects an event or behavior that is against the configured security policies or the event or behavior will bring security risks to the system, the system reports information about the security event to the security alarm management platform (such as the U2000) so that administrators can immediately handle the event or behavior to eliminate security risks.

13.6 Reliability Indicator

This topic describes the indicators of the reliability design.

Table 13-13 lists the reliability indicators of the U2000.

Table 13-13 Reliability indicators of the U2000

Item	Indicator
MTBF	The average fault interval is larger than 6 months.
MTTR	≤ 15 minutes (vSphere HA switching time, including the fault detection time)
Remote disaster recovery time	≤ 4 hours

13.7 Management Capability

This topic describes the management capability of the U2000 in a distributed system.

Table 13-14 shows the management capability of a single U2000.

Table 13-14 U2000 management capability

Item	Subitem	Indicator
Management capability	Number of managed EMs	Maximum: 4 A maximum of 5 EMs can be supported when the U2000 manages only PTN networks.
	Number of managed equivalent NEs	Maximum: 50,000 equivalent NEs A maximum of 80,000 equivalent NEs can be managed when the U2000 manages only PTN networks.
	Number of managed clients	Maximum: 300 NM or EM clients (by deploying multiple desktop service instances) NOTE The U2000 supports a maximum of 300 online clients and concurrent service provisioning on 32 of them. The U2000 supports concurrent service provisioning on 50 clients when the U2000 manages only PTN networks.
Number of managed physical nodes		Maximum: 50,000 physical NEs <ul style="list-style-type: none">● A maximum of 80,000 physical NEs can be managed when the U2000 manages only PTN networks.● The maximum of managed MDUs in access networks is 100,000. The maximum of managed DSLAM/MSAN is 7,000,000 lines.● There is no limit to the number of subnets. The maximum of physical nodes in each subnet is recommended to be 500; 200 is optimal. The maximum of subnet nests is recommended to be 6.
Service capability	PTN O&M	The maximum values are as follows: <ul style="list-style-type: none">● Number of NEs: 80,000 equivalent NEs, no more than 80,000 physical NEs● Number of links: 120,000 Layer 2 links● Number of tunnels: 600,000● Number of APS protection groups: 150,000● Number of PWE3 services: 300,000● Number of VPLS services: 1000 (VSI: 15,000)● Number of L3VPN services: 1000 (VRF: 20,000)

Item	Subitem	Indicator
	SDH+OTN O&M	<p>The maximum values are as follows:</p> <ul style="list-style-type: none"> ● Number of NEs: 50,000 equivalent NEs, no more than 50,000 physical NEs ● Number of SDH trails: 1,000,000 ● Number of OTN trails: 300,000 ● Number of EOS trails: 50,000
	Access network management	<p>The maximum values are as follows:</p> <ul style="list-style-type: none"> ● Network scale: 50,000 equivalent NEs, 6,000,000 lines of FTTx equipment ● Number of concurrent NBI processes of each EM: 30 ● Number of connections to the northbound gateway NE: 200 ● Number of managed ONTs: 7,500,000

13.8 Performance Indicators

This topic describes the performance indicators of the U2000.

Performance indicators

Table 13-15 Performance indicators

Item	Subitem	Indicator
NMS startup and shutdown	NMS start time (70% of the management capacity)	≤ 10 minutes
	NMS shutdown time (70% of the management capacity)	≤ 10 minutes
Database restoration time		≤ 60 minutes
Storage capacity	Capacity of current alarms	Maximum: 300,000
	Capacity of historical alarms	Maximum: 10,000,000 Storage period in the database: 180 days
	Capacity of logs, including operation logs and system logs	Maximum: 1,000,000 Storage period in the database: 90 days

Item	Subitem	Indicator
Resources occupied	CPU usage	Equal to or less than 10%
Link capacity	Number of manageable links in the topology	Maximum: 120,000
Processing capability	Response speed of handling an alarm	Usually equal to or less than 15 seconds. Response speed of handling an alarm indicates the interval from the time at which an alarm is generated on the equipment to the time at which the alarm is displayed on the U2000.
	Performance collection capability	<p>Maximum performance collection capability in each collection mode:</p> <ul style="list-style-type: none"> ● SNMP collection: 500,000 equivalent statistics records/15 minutes ● BULK collection: <ul style="list-style-type: none"> - IP equipment: 1,500,000 equivalent statistics records/15 minutes - Access equipment: 6,000,000 equivalent statistics records/15 minutes ● Qx collection: 500,000 collection instances/30 minutes <p>NOTE</p> <ul style="list-style-type: none"> ● For details about the performance collection capability in different network scales, see Table 13-17. ● For details about the hard disk space required for storing performance data and the data life cycle, see Performance Storage Capability.
	Alarm handling capability	100 alarms per second on average and 400 alarms per second at the peak
U2000 user management capability	User	Maximum: 700
	User group	Maximum: 300
	Object set	Maximum: 100
	Operation Set	Maximum: 255
Concurrent NE upgrades		Maximum: 60 x Number of EM

Item	Subitem	Indicator
HWECC/IP over DCC networking capacity	Number of manageable GNEs	The maximum number of manageable GNEs for a single EM is 3000, and the NM cannot manage GNE directly. NOTE The U2000 can manage 500 GNEs by a single instance.
	Number of manageable NEs for a GNE	Recommended: <= 50; maximum: <= 60

DCN bandwidth requirements

Table 13-16 DCN bandwidth requirements

Item	Bandwidth
Bandwidth required for communication between a U2000 client and the U2000 server	4 Mbit/s + 2 Mbit/s x Number of EM clients
Bandwidth required for communication between the U2000 server and nodes	2Gbit/s
Bandwidth required for communication between N Equivalent NEs and the U2000 server	A bandwidth of 2 Mbit/s may not meet the bandwidth requirements for certain types of networks. In this case, you can set the (Committed Information Rate) or PIR (Peak Information Rate) by using the following formulas. The bandwidth of the live network should meet the PIR requirement in large bandwidth consuming scenarios, such as network-wide data synchronization, performance data collection, and batch upgrade. CIR: <ul style="list-style-type: none">● $N > 56: 2048 \text{ kbit/s} + (N - 56) \times 0.5 \text{ kbit/s}$● $N \leq 56: 2 \text{ Mbit/s}$ PIR: <ul style="list-style-type: none">● $N > 56: 10240 \text{ kbit/s} + (N - 56) \times 5 \text{ kbit/s}$● $N \leq 56: 10 \text{ Mbit/s}$
Bandwidth required for communication between an OSS and the U2000 server	10 Mbit/s NOTE A minimum of 10 Mbit/s is required.

Performance collection capability

Table 13-17 Performance collection capability

Network Scale	SNMP Collection Capability (Without Max/Min Data Aggregation Enabled, Max Equivalent Statistics Record/15 Minutes)	SNMP Collection Capability (With Max/Min Data Aggregation Enabled, Max Equivalent Statistics Record/15 Minutes)	BULK Collection Capability (Max Equivalent Statistics Record/15 Minutes)	Qx Collection Capability (Max Equivalent Statistics Record/15 Minutes)
< 50,000 equivalent NEs	500,000	330,000	<ul style="list-style-type: none"> ● IP NEs: 1,500,000 ● Access NEs: 6,000,000 	<ul style="list-style-type: none"> ● PTN/RTN900 NEs: 500,000 ● Other transport NEs: 100,000

Performance Storage Capability

The hard disk space for basic data is 100 GB. Every 10,000 15-minute performance instances (for NEs with data aggregation enabled, such as routers) or 30,000 15-minute performance instances (for NEs without data aggregation enabled, such as access and transport NEs) are added, the hard disk space increases 15 GB. The maximum disk space is 850 GB.

Formula

- Required hard disk space (GB) = Hard disk space for basic data + Hard disk space required for added instances x Life cycle = $100 + (15 \times A + 15/3 \times N) \times 4 \times 24 \times L$
- Life cycle (day) = (Total hard disk space - Hard disk space for basic data)/Hard disk space required for daily added instances = $(S - 100)/[(15 \times A + 15/3 \times N) \times 4 \times 24]$

NOTE

- A (10,000): indicates the number of instances collected when the data aggregation function is enabled.
- N (10,000): indicates the number of instances collected when the data aggregation function is disabled.
- L (day): indicates the life cycle of performance data.
- S (GB): indicates the total hard disk space. By default, the maximum space is 850 GB. You can expand the space if needed.

14 Standards and Protocols Compliance

This topic describes the standards and protocols that the U2000 is compliant with.

The U2000 is developed according to the network management system model that the ITU-T TMN series standards define. The information model is constructed based on the object-oriented concept. Complying with multiple standards, the U2000 has good expandability and reusability. The U2000 complies with the following international standards and protocols:

- RFC 793 Telnet/TCP/IP standards
- RFC 1155, RFC 1157, RFC 1212, RFC 1213 and RFC 1215 SNMP V1 series standards
- RFC 1905, RFC 1906, RFC 1907, RFC 1908, RFC 2011, RFC 2012, RFC 2013, RFC 2571, RFC 2572, RFC 2573, RFC 2574, RFC 2576, RFC 2578, RFC 2579, and RFC 2580 SNMP V2 series standards
- RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, and RFC 3418 SNMP V3 series standards
- RFC 3164 Syslog standards
- ISO 8824 and ISO 8825 ASN.1 standards
- ITU-T standards for managing the telecommunications management network: M.3000, M.3010, M.3020, M.3100, and M.3400 (without accounting)
- HTTP, HTTPS, and JAVA interface protocols and standards
- The SNMP NBI complies with the SNMP v1/v2c/v3 standards.
- The performance text NBI complies with the FTP or SFTP protocol.
- The XML NBI complies with the MTOSI standards as follows: TMF 518, TMF 612, and TMF 864
- CORBA 2.5 protocol
- ISO 8824 and ISO 8825 ASN.1 standards
- The CORBA NBI complies with the MTNM standards as follows: TMF 513, TMF 608, TMF 814, and TMF 814A
- The TL1 NBI complies with the Generic Requirements (GR) 831 standard.

Table 14-1 lists the details of the standards and protocols.

Table 14-1 Details of the Standards and Protocols

Standards and Protocols	Description
M.3016.0	Security for the management plane: Overview
M.3016.1	Security for the management plane: Security requirements
M.3016.2	Security for the management plane: Security services
M.3016.3	Security for the management plane: Security mechanism
M.3016.4	Security for the management plane: Profile proforma
M.3703	Common management services - Alarm management - Protocol neutral requirements and analysis
RFC 793	Transmission Control Protocol (Darpa Internet Program Protocol Specification)
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1212	Concise MIB Definitions
RFC 1213	Management Information Base for Network Management of TCP/IP-based Internets: MIB-II
RFC 1215	A Convention for Defining Traps for use with the SNMP
RFC 1905	Protocol Operations for Version 2 of the Simple Network Management Protocol
RFC 1906	Transport Mappings for Version 2 of the Simple Network Management Protocol
RFC 1907	Management Information Base for Version 2 of the Simple Network Management Protocol
RFC 1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC 2011	SNMPv2 Management Information Base for the Internet Protocol using SMIv2
RFC 2012	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC 2013	SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2
RFC 2544	Benchmarking Methodology for Network Interconnect Devices
RFC 2571	An Architecture for Describing SNMP Management Frameworks
RFC 2572	Message Processing and Dispatching for the Simple Network Management Protocol

Standards and Protocols	Description
RFC 2573	SNMP Applications
RFC 2574	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)
RFC 2576	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 2578	Structure of Management Information Version 2 (SMIv2)
RFC 2579	Textual Conventions for SMIv2
RFC 2580	Conformance Statements for SMIv2
RFC 3411	An Architecture for Describing SNMP Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	SNMP Applications
RFC 3414	User-based Security Model (USM) for version 3 of SNMPv3
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 3417	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3164	BSD syslog Protocol
ISO 8824-4-2000	Information Technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications Amendment 1: ASN.1 semantic model
ISO 8825-2-1998	Information Technology - ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER) Second Edition; Technical Corrigendum 1: 12/15/1999; Amendment 1: 12/01/2000
ITU-T M.3000	Overview of TMN recommendations
ITU-T M.3010	Principles for a telecommunications management network
ITU-T M.3013	Considerations for a telecommunications management network
ITU-T M.3017	Framework for the integrated management of hybrid circuit/packet networks

Standards and Protocols	Description
ITU-T M. 3020	TMN interface specification methodology
ITU-T M. 3100	Generic network information model
ITU-T M. 3101	Managed Object Conformance statements for the generic network information model
ITU-T M. 3180	Catalog of TMN management information
ITU-T M. 3200	TMN management services and telecommunications managed areas: overview
ITU-T M. 3300	TMN F interface requirements
ITU-T M. 3400	TMN management functions
ITU-T X. 720	Management information model
ITU-T X. 721	Definition of management information
ITU-T X. 722	Guidelines for the definition of managed objects
ITU-T X. 733	Information technology - Open Systems Interconnection - Systems Management: alarm reporting function
ITU-T X. 735	Information technology - Open Systems Interconnection - Systems Management: log control function
ITU-T X. 903	Information technology - Open distributed processing - Reference Model: architecture
ITU-T G. 707	Network node interface for the synchronous digital hierarchy (SDH)
ITU-T G. 773	Protocol suites for Q-interfaces for management of transmission systems
ITU-T G. 774 (01, 02, 03, 04)	Synchronous digital hierarchy (SDH) - Management information model for the network element view
ITU-T G. 7710	Common equipment management function requirements
ITU-T G. 783	Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

Standards and Protocols	Description
ITU-T G. 784	Synchronous digital hierarchy (SDH) management
ITU-T G. 803	Architecture of transport networks based on the synchronous digital hierarchy (SDH)
ITU-T G. 831	Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)
ITU-T G. 851.1	Management of the transport network - Application of the RM-ODP framework
ITU-T G. 852.1	Enterprise viewpoint for simple subnetwork connection management
ITU-T G. 852.2	Enterprise viewpoint description of transport network resource model
ITU-T G. 852.3	Enterprise viewpoint for topology management
ITU-T G. 852.6	Enterprise viewpoint for trail management
ITU-T G. 853.1	Common elements of the information viewpoint for the management of a transport network
ITU-T G. 853.2	Subnetwork connection management information viewpoint
ITU-T G. 853.3	Information viewpoint for topology management
ITU-T G. 853.6	Information viewpoint for trail management
ITU-T G. 854.1	Computational interfaces for basic transport network model
ITU-T G. 854.3	Computational viewpoint for topology management
ITU-T G. 854.6	Computational viewpoint for trail management
ITU-T Y. 1701	Common equipment management function requirements
MEF 15	Requirements for Management of Metro Ethernet Phase 1 Network Elements
Rational Unified Process 5.5	Rational Unified Process

Standards and Protocols	Description
Sif99025	EML-NML interface models
TMF518	MTOSI Business Agreement
TMF612	MTOSI Information Agreement
TMF864	MTOSI Interface Implementation Specifications
TMF513 V2.0	Multi-Technology Network Management Business Agreement NML-EML Interface Version 2.0
TMF608 V2.0	Multi-Technology Network Management Information Agreement NML-EML Interface Version 2.0
TMF814 V2.0	Multi Technology Network Management Solution Set Conformance Document Version 2.0
TMF814A	MTNM Implementation Statement and Guidelines for MTNM Release 3.5M

A Glossary and Abbreviations

A

Abnormal Resource	When the network management system (NMS) polls device resources on the device management module or the module is refreshed manually, the physical resources of some devices (such as boards, subboards, and ports) cannot be accessed because they have been deleted or have some faults. So, after the NMS polls device resources on the device management module or the module is refreshed manually again, the result of polling the physical resources differ from the first time. The physical resources that cannot be polled in the second time are called the abnormal resource.
AIS	Alarm indication signal. An AIS signal is sent downstream in a digital network if an upstream failure has been detected and persists for a specified amount of time.
AIS Insertion	If there are excessive bit errors in a channel, an AIS can be inserted to indicate that the channel is unavailable. AIS insertion can be enabled or disabled in the following scenarios: a line board when there are excessive B1, B2 or B3 bit errors, a tributary board at the E1 or T1 level when there are excessive BIP-2 bit errors, and a tributary board at the E3 level or higher when there are excessive B3 bit errors.
Alarm Correlation Analysis	In the event that alarm 2 is raised within five seconds after alarm 1 is raised, and alarm 2 complies with the conditions defined in the alarm correlation analysis rule, you can either suppress alarm 2 or raise its severity according to the behavior defined in the alarm correlation rule. Such a process is called alarm correlation analysis.
Alarm Status	Device reports the trap information to the NMS. The NMS displays the received information on the alarm start on the topology view. There are four types of alarm states: urgent alarm, important alarm, subordinate alarm, and prompt alarm.
Auto Discovery	By using ping or Simple Network Management Protocol (SNMP) parameter profiles, the NMS can test remote devices, discover IP devices and devices that supports SNMP, and automatically add discovered devices.
Alarm Reversion	For the port that has already been configured but not actually loaded with services, this function can be used to avoid generating alarm information and prevent alarm interference.

Alarm Severity	The alarm severity identifies the level of an alarm or event. According to ITU-T recommendations, alarms are classified into four severities: critical, major, minor, and warning.
Alarm Suppression	Suppressed alarms of a specific object are not reported. The object here may be network-wide equipment, a specific NE, a specific board, or even a specific function module of a board.
Alarm	A visible or an audible indication of a failure or an emergency.
ALS	Automatic laser shutdown. ALS is turned on when the optical interface board does not carry services or the optical fiber is faulty. Its service life can be prolonged by decreasing the duration during which the laser is on.
APS	Automatic protection switching. APS is the capability of a transmission system to detect a failure on a working facility and to switch to a standby facility to recover the traffic.
ATM Protection Group	Asynchronous transfer mode. An ATM protection group refers to the logically bound ATM virtual path (VP) network or subnetwork connections that share the same physical transmission channel. In the VP group (VPG), a pair of VP connections (working connection and its protective connection) is used for monitoring the automatic protection switching, called monitoring connections (APS VPCs). If the monitoring connections switch over, the whole VPG will switch over to accelerate the ATM protection switching (as quick as the protection switching of the SDH layer).
Attribute	Property of an object.
Automatic Switching	When the active board or path fails, the standby one automatically performs the tasks.

B

Bandwidth	The maximum range of transmission frequencies that a transmission line or channel can carry on a network. The greater the bandwidth, the faster the data transmission rate.
Baseline	Select the test result when the line is in good condition as the line test baseline to provide a basis for comparison and analysis of subsequent line test results.
Baseline Collection Test	One of the methods used to test submarine lines. For deployment or fault restoration, or when updating the baseline is required, collect the baseline to provide reference for comparison tests and alarms.
Binding	In virtual concatenated payload configuration, designating one binding number to identify the VC4s of the same virtual concatenated payload is called "binding". If a fault occurs in one of the bound services, all bound services will switch.
Bit Error Alarm Threshold	When bit errors reach a specific limit, the device will report an alarm. This limit is the bit error alarm threshold. There are two types of thresholds: threshold-crossing threshold and defect threshold.

C

CCU	Cabinet control unit. It manages electronic locks of sites.
------------	---

Comparison Test in Periodic Mode	One of the methods used to test submarine lines. Carry out polling tests for multiple lines on the same location measurement unit (LMU) board periodically, compare the test results with the baseline data in in-service mode, and provide pre-warnings or alarms for lines.
Comparison Test in Single-Test Mode	One of the methods used to test submarine lines. Test lines by using test parameters of the baseline collection test in in-service mode, compare the test result with the baseline data, and provide pre-warnings or alarms for lines.
Check Alarms	Compare one (or more) uncleared alarm on the NMS with that on the NE. If an alarm is included in the current alarms on the NE, it is kept on the NMS. If not, it will be removed from the NMS.
Client	A kind of terminal (PC or workstation) connected to a network that can send instructions to a server and get results through a user interface.
Clock View	The clock view provides a visible platform to enable: NE clock settings, network-wide clock synchronization status query, and clock tracing and search functions.
Configuration Data	A command file which is used to configure hardware for an NE so that the NE can carry specified services and coordinate with other NEs in the entire network. Configuration data is the key factor for the proper operation of the entire network. The typical configurations include board configuration, clock configuration and protection relationship configuration.
Configuration Management	Configuration management enables the inventory query of network configuration resources (such as NMS or SNMS, NEs, subnets, links, SNCs, routes, TPs, edge points, and equipment). Real-time inventory changes will be timely reported to the upper NMS to notify the carrier of the existing network operating status and maintain data consistency with the upper NMS or SNMS. SNMS is short for subnetwork management system.
Configure	To set basic parameters for an object.
Connection Point	A reference point where the output of a trail termination source or a connection is bound to the input of another connection, or where the output of a connection is bound to the input of a trail termination sink or another connection. The connection point is characterized by the information which passes across it. A bidirectional connection point is formed by the association of a contra-directional pair.
Connection	A transport entity which consists of a pair of associated unidirectional connections. The two unidirectional connections can simultaneously transfer information to each other in opposite directions.
CORBA	The Common Object Request Broker Architecture (CORBA) is a distributed and object-oriented application architecture specification. It is an object interoperability model irrelevant to language for heterogeneous computing. To be specific, the CORBA is designed to be independent from platform and language. Therefore, the CORBA can run on any platform, be located at any place of a network, and use any language that has interface definition language (IDL) mapping. Its core technology is a set of standard languages, interfaces, and protocols to support interoperability among heterogeneous distributed application programs and language-independent object reuse.
Current Alarms	Alarms that are not cleared, or is cleared but not acknowledged.

Current Performance Data	The performance data stored during the current register is called current performance data. The current 15-minute or 24-hour register (only one for each) is applied to collect the performance data during the current monitoring period. It changed within the monitor period.
Customer OSS test NBI	The standard NBI provided by the U2000 for connection to the customer OSS, and provides reliable data and reference for troubleshooting.
Change Audit Service	A service that is developed to record the change on the network device, including changes in the information about the device, the configuration, and the mapping of the device. It provides one integrated database. Every application records these changes in the database and ensures that these changes in the database are reflected in other applications.
Cluster	The cluster is an administrative domain composed of a set of switches. It consists of a command switch and multiple member switches. A public IP address manages all the switches within the cluster.
Configuration File	Text file, recording various configurations on devices.

D

DCC	Data communications channel. A DCC uses the D1-D12 bytes in the overhead of an STM-N signal to transmit information. There are two types of DCC channels: the 192 kbit/s DCC-R channel, which is composed of bytes D1-D3; the 576 kbit/s DCC-M channel, which is composed of bytes D4-D12. The DCC-R channel supports communications between all NEs. The DCC-M channel, however, is not the regenerator section overhead and does not support communications between regenerators. It serves a more universal purpose (for example, it supports TMN as a physical channel of ECC).
DNI	Dual node interconnection. The protection mode defined in G. 842 Recommendation for the inter-ring service. In recommended protection modes, the protection of the interconnecting service between two ring networks composed of the devices from different manufacturers and in different protection modes can be realized. Moreover, in the event of a fiber failure or node failure, services can also be protected.
Domain	The domain of the NMS specifies the scope of addresses or functions which are available to each specific user.
DS	A server that obtains service data from the Service Data server and provides data to be displayed on the client.
Dumping	Dumping is a process of exporting alarm data to the customized file from the database where it is then cleared.

E

ECC	Embedded control channel. An ECC provides a logical operations channel between SDH NEs, using a data communications channel (DCC) as its physical layer.
EMU	Environment monitoring unit. An EMU is installed on the top of the OptiX 155/622H equipment rack to monitor the environment variables, such as the power supply and temperature. With external signal input through the relay, the EMU can monitor alarms (such as fire, smog, and burglary alarms). Displayed on the NMS, the changes of environment can be monitored timely and accurately.

Equipment Set	An aggregate of multiple managed equipment. Equipment set facilitates the user authority management on equipment in the management domain of the NMS. If some operation authorities over one equipment set are assigned to a user (user group), these operation authorities for all the equipment in the equipment set are assigned to the user (user group).
----------------------	---

F

Failure	A fault that persists long enough to terminate the required function of an item.
Fault	A fault is the inability of a function to perform a required action. This does not include inability due to preventive maintenance, lack of external resources, or planned actions.
Filter	The filter is used to filter matched logs.
Forced Switch	This function forces the service to switch from the working board to the protection board, regardless of the state of the protection board.
FTP	File Transfer Protocol. A member of the TCP/IP suite of protocols, used to copy files between two computers on the Internet. Both computers must support their respective FTP roles: one must be an FTP client and the other an FTP server.

H

Historical Alarms	Alarms that have cleared and acknowledged.
Historical Performance Data	Historical performance data consists of the performance data stored in the historical register and the auto-report performance data stored on the NMS.

I

Intermediate Office	It refers to the equipment used for optical fiber management in metropolitan areas. It has multiple pairs of interfaces for fiber connections. Every two interfaces in a pair are connected to each other to form a longer physical fiber path. The physical fiber path connecting transport equipment is comprised of two or more fiber sections that connect in serial through the intermediate office. Intermediate office information lists show the information about each fiber section.
In-Service Mode	One of the methods used to test submarine lines. By using the in-service test mode, you can test submarine cables and repeaters without damaging the existing services of the submarine system.
Image (OS)	Binary file, equivalent to the OS of the device and a part of the device version.
IP Address	In the TCP/IP protocol, it is used to uniquely identify the address of the communication port, which consists of four bytes in decimal digits, for example, 129.9.161.55.

J

Jitter	An indication that shows the delay stability of a ping operation (or other test operations). Unit: ms.
---------------	--

L

Label	A mark on a cable, a subrack, or a rack for identification.
Layer	A concept used to allow the transport network functionality to be described hierarchically as successive levels; each layer being solely concerned with the generation and transfer of its characteristic information.
LCT	Local craft terminal. The LCT provides the user with single-layer management network solutions to the transmission network of up to five NEs to realize integrated management of multi-service transmission networks. Usually it uses crossover cables or serial cables to connect one NE for configuring and maintaining a single NE.
License	A permission provided by a vendor to authorize the use of specific functions of a product. Usually the license consists of encrypted codes, and the authorization varies with license levels.
Link	The link is responsible for transmitting data from one station to the next neighbor station.
Lock NE Login	This function prohibits users with lower-level rights from logging in to NEs and forces these logged-in lower-level NE users to log out.

M

Main Topology	The default client interface of the NMS, a basic component of the human-machine interactive interface. The topology view clearly shows the structure of the network, the alarms of different NEs, subnets in the network, the communication status as well as the basic network operating status.
Management Information	The signal passing across an access point.
Manual Switch	A type of protection switching. When the protection path is normal and there is no request for a higher level switching, the service is manually switched from the working path to the protection path in order to test whether the network is still capable of providing this type of protection.
Manual Test	One of the methods used to test submarine lines. You need to set test parameters manually, start the test, and save the test result as the baseline of the in-service mode.
MO	Managed object. The management view of a resource within the telecommunication environment that may be managed by the agent. Examples of SDH MOs are: equipment, receive ports, transmit ports, power supplies, plug-in boards, virtual containers, multiplex sections, and regenerator sections.
MS	Multiplex section. An MS is the trail between and including two multiplex-section trail-termination functions.
MSTP	Multi-service transmission platform. Based on the SDH platform, the MSTP provides unified service management. It can access, process, and transmit TDM, ATM, and Ethernet services.
MSP	Multiplex section protection. The nodes online achieve protection switching through the K1 and K2 bytes in the MS, including linear 1+1 MSP protection switching links, linear 1:N MSP protection switching links, dedicated MSP protection rings, and shared MSP protection rings.

N

NE Database	The three types of databases on NE SCC boards are as follows: (1) DRDB: a dynamic database in a dynamic RAM, powered by battery; (2) SDB: a static database in a power-down RAM; (3) FDB0, FDB1: permanently saved databases in a flash ROM. During proper operation, the NE configuration data is saved in DRDB and SDB at the same time. Backing up an NE database means backing up the NE configuration data from SDB to FDB0 and FDB1. When an NE is restarted after power failure, the NE database is restored by performing the following: As the SDB data is lost due to power failure, the main control restores the data first from DRDB. If the data in DRDB is also lost due to the exhaustion of the battery, the data is restored from FDB0 or FDB1.
NE Explorer	NE Explorer is the main operation interface of the NMS. For easy navigation, the NE Explorer window presents an expandable directory tree (function tree) in the lower left pane. The configuration, management and maintenance of the equipment are accessed here.
NE	network element. An NE contains both the hardware and the software running on it. One NE is at least equipped with one system control and communication (SCC) board which manages and monitors the entire network element. NE software runs on the SCC board.
NOC	Network operation center, which is responsible for the network operation, troubleshooting, and maintenance. It ensures the proper operating of the network.
NMS	Network management system. In the telecommunication management network structure, the NMS is located between the NE level and network level, which can support all functions at the NE level and part of the network level management functions. See also U2000.
NNI	Network node interface. An NNI identifies the interface between the ATM network nodes. See also SDH NNI.
Node	A node, one of the topology objects, is the minimum unit displayed on the topology view. A node icon on the topology view represents a router, a switch, a 3rd-party device, or a virtual node.

O

Online Help	An indexed collection of information on all aspects of the NMS. They can be accessed at any time from the Help menu or by pressing F1 .
Optical Time Domain Reflectometer	OTDR is an optical fault locator and analysis tool for optical fiber networks. The OTDR can measure the fiber length, test the fiber shrink, and test the connection shrink. After coupling modulated optical signals to the fibers to be tested, the OTDR detects features of the fiber links by analyzing the amplitude and time domain of the backscattering lightwave.
Out-of-Service Mode	One of the methods used to test submarine lines. By transmitting detection light with high power, the out-of-service test can detect the fiber status and repeater status, to realize the status detection and fault point location after a fiber cut. In general, when detecting that a line is abnormal during a test in in-service mode, you can carry out a test in out-of-service mode to locate the fault.

OWSP	Optical wavelength shared protection. OWSP is a bidirectional ring, where each node is equipped with an OWSP. There are two channels (λ_1 and λ_2) in the main optical path on the internal and external rings in each span on a ring. The fiber and the OWSP on the main optical path are connected to the optical ports inputting λ_1 and λ_2 on the multiplexer/demultiplexer board (unnecessary to be connected to the OTU); therefore λ_1 and λ_2 can be added and dropped at every node.
P	
Packets Loss Ratio	The packet loss ratio is an indicator that reflects the possibility of packet loss after many ping tests or other tests; expressed in percentage (%).
Path Protection	The working principle of path protection: When the system works in path protection mode, the PDH path is dual-fed and selectively received. Through the tributary unit and cross-connect unit, the tributary signal is sent simultaneously to the east and west lines. Meanwhile, the cross-connect matrix sends the signal dually sent from the opposite end to the tributary board through the active and standby buses, and the hardware of the tributary board will selectively receive the signal from the two groups of buses automatically according to the AIS number of the lower order path.
Path	A trail at a path layer.
Performance Register	A performance register is the memory space for performance event counts, including 15-min current performance registers, 24-hour current performance registers, 15-min historical performance registers, 24-hour historical performance registers, UAT register and CSES registers.
Performance Threshold	Performance events usually have upper and lower thresholds. When the performance event count exceeds the upper threshold, a performance threshold-crossing event is generated; when the performance event count value is below the lower threshold for a period of time, the performance threshold-crossing event will end. In this way, performance jitter caused by some sudden events can be shielded.
PMU	Power monitoring unit. PMU is a type of power and environment monitoring unit.
Poll Status	The NMS polls the device status and other configuration data periodically and displays the polling results on the topology view. The polling status can be displayed as normal, unknown (a device can be pinged to), offline (a device cannot be pinged to), light fault, subordinate fault, important fault and urgent fault.
Private Line	Both communication parties are connected permanently.
Procedure	A generic term for an action.
Process	A generic term for a collection of actions.
Protection Path	A specific path that is part of a protection group and is labeled protection.
Protection Strategy	In case the service route provides multiple service protections, different protection strategies can be selected as required. Protection strategy refers to the protection mode given the priority in use for the trail: protection, no protection, and extra traffic. Of the above, the protection preference is divided into trail protection and sub-network connection protection.

Protection Subnet	On the NES and RWS+ NMS, the protection subnet is an MSP ring or path protection ring. On the U2000, however, the protection subnet is a network which consists of NE equipment and fibers links. The resources that form a protection subnetwork include NEs and fiber cables. The creation of the protection subnet requires that the NEs are created and properly configured, and the fiber connection is correctly created among the NEs.
PTN	Packet transport network.
PNM	Proactive Network Maintenance, that is, to detect fault points on networks before user services are affected. Proactively diagnosing and recovering faults helps minimize service impact, improve carriers' service level agreements (SLAs), and reduce network maintenance costs.
R	
RPS	Remote power system is introduced to FTTC networks as a low-cost and fast-feed solution. On the equipment room side, RPS devices step up voltage from -48 V to above 200 V DC for transport over twisted pairs. On the device side, RPS devices step down voltage to -48 V.
ROADM	Reconfigurable optical add/drop multiplexer. A ROADM helps you to terminate or pass through any wavelength at every node without affecting the existing services. At the same time, ROADM can remotely change wavelengths through the NMS, to adjust wavelengths added or dropped in a quick and convenient manner. In addition, ROADM enables power equalization at path level through a built-in power equalization function, and then adjusts power for pass-through paths in a better way than a band-based dynamic gain equalizer (DGE) does.
Route	The IP route selection is in table driving mode. In each host and each router of the Internet, there is a routing table that contains information about how the service is transmitted from the source to the sink, providing a basis for route selection. Ethernet static routing in ET1 refers to the mapping relationship between the Ethernet port and the bound path. Its routing type includes port routing and VLAN routing. Port routing: It means configuring a route between the Ethernet port and the bound path port, which is usually used for point-to-point networking communication; VLAN routing: It means configuring a route between the Ethernet port and the bound path port based on the VLAN service. It can be used flexibly in point-to-point, point-to-multipoint or multipoint-to-multipoint communication. The implementation divides and converges the data stream according to the VLAN flag of the packet. As a VLAN flag can be added to the Ethernet port, the equipment can be applied more flexibly.
Report	Reports are generated manually in real time.
RTN	Radio transmission node. It is a split microwave transmission system which provides seamless microwave transmission solutions for mobile communication networks and other private networks.
RTT	Round-trip time. RTT is the delay of ping tests.

S

Script File	It is the text file describing the physical information and configuration information of the entire network, including the NE configuration file, port naming file, end-to-end configuration file, NE physical view script file, NMS information file and the script file for service implementation.
Schedule Task	The report on a scheduled task that is generated at an interval along with the periodical running of the schedule tasks.
Script	A list of instructions for performing a specific task or action, written in a scripting language.
SDH NNI	SDH network node interface. It is applied to build communications with the equipment beyond the NMS management area. Usually, the NMS creates an SDH NNI by creating a logical system on the port of an idle line board; the NE must be a TM without protection and fiber connections.
Section	A trail at a section layer.
Settings	Parameters of an operation that can be selected by the user.
Severity	See Alarm Severity.
SNMP	The SNMP (Simple Network Management Protocol) protocol consists of a set of standards for network management and is the most widely used protocol in TCP/IP networks. TCP is short for Transmission Control Protocol and IP is short for Internet Protocol.
Subnet Mask	Also referred to as the network mask-off code, it is used to define network segments, so that only the computers in the same network segment can communicate with one another, which suppresses broadcast storms between different network segments.
Subnet Number	Subnetwork number is used to differentiate the different network sections in the sub-network conference. Actually it is the first couple of digits of the user phone number. An orderwire phone number is composed of the sub-network number and the user number.
Subnet	Sub-network is the logical entity in the transmission network and comprises a group of network management objects. A sub-network can contain NEs and other sub-networks. A sub-network planning can better the organization of a network view.
Support	The frame on the bottom of a rack, when installing the rack on the ESD floor.
Synchronize NE Time	Send the system time of the NMS server to NEs to synchronize all NEs with the server.

T

T2000	The T2000 is a subnetwork management system (SNMS). In the TMN architecture, the T2000 is located between the NE level and network level, which can support all functions of the NE-level and part of the network-level management functions. See also NM.
T2100	The T2100 is a network level management system for the optical transmission network, and is located in the network management layer (NML) in the telecommunication management network (TMN) architecture.

TDA Clock Source	TDA is short for Tone Data Access. For the 2500+ NE equipment, an external TDA board can be installed for which the clock source must be set so that the TDA board can switch according to the set clock source sequence when clock source switching occurs.
TL1	Transaction Language 1.
TMN	Telecommunications management network. A TMN provides the means used to transport and process information related to management functions for the telecommunications network.
Topology	The NMS topology is a basic component of the man-machine interactive interface. The topology view clearly shows the structure of the network, the alarms of different NEs, subnets in the network, the communication status as well as the basic network operating status.
Trail Management Function	A network level management function of the NMS. Through trail management, you can configure end-to-end services, view graphic interface and visual routes of a trail, query detailed information of a trail, filter, search and locate a trail quickly, manage and maintain trails in a centralized manner, manage alarms and performance data by trail, and print a trail report.
Trail	A trail is a type of transport entity, mainly engaged in transferring signal from the input of the trail source to the output of the trail sink, and monitoring the integrity of the transferred signal.
Tributary Loopback	A fault can be located for each service path by performing loopback to each path of the tributary board. There are three types of loopback modes: No loopback, Outloop, and Inloop.
Threshold	The alarm range will be defined after the performance data is collected. Thresholds can be upper and lower thresholds and are relevant to the unit and indicator values set for each specific scenario.

U

U2000	Short for iManager U2000 Unified Network Management System (NMS). The U2000 is future-oriented and provides unified management of All-IP and FMC bearer and access equipment.
UAT	Unavailable time. A UAT event is reported when the monitored object generates 10 consecutive severely errored seconds (SES) and the SESs begin to be included in the unavailable time. The event will end when the bit error ratio per second is better than 10-3 within 10 consecutive seconds.
UNI	User network interface. A UNI is the interface between the user and the ATM network node.
Unprotected	Services transmitted in an ordinary manner that cannot have data restored once a failure or interruption occurs due to a lack of protection mechanisms.
Upload	Report all or part of the configuration data of the NE to the NMS and overwrite the configuration data saved in the NE layer on the NMS.
User Group	User groups refer to a combination of NMS users with the same management and operation rights. The default user groups include security management group, administrator group, maintenance engineer group, operator group, and monitor group. The user group attributes are the name and detailed description of a group.

User The user of the NMS client. The user name and password determine what level of access the user is given to the operation and management of the NMS.

V

VC4 Loopback The fault in each VC4 path on the optical fiber can be located by setting the loopback for each VC4 path of the line. There are three types of loopback modes: No loopback, Outloop, and Inloop.

VC4 Server Trail The path rate of the VC4 server trail is 150.336 Mbit/s. The VC4 server trail provides transparent channels (that is, circuit groups) for circuit-layer network nodes (for example, a switch) in a path-layer network, and acts as the basic unit for inter-office communication paths. When the VC4 server trail is configured, the higher order cross-connection of VC4 is generated only in the intermediate NE, but no cross-connection is generated at the two ends. That is, no service is added/dropped. Therefore, the VC4 server trail is not a traditional service. It is only the basis for VC3 and VC12 trail creation.

VCI The Virtual Channel Identifier occupies 16 bits in both NNI cells or UNI cells. It indicates the virtual channel in the path. The VPI and VCI together indicate a virtual connection.

View Organizes and displays rules and filter conditions of the topology data. Customize the view according to requirements of every product and organize the data in the view displayed by the topology module, such as the layer 2 view, VPN view, and IP view. By default, the platform provides the physical view. The topology view can be planned according to the domain, maintenance relationship, and so on.

Virtual Fiber A virtual fiber is created between SDH equipment that has WDM equipment in between. From the perspective of the SDH equipment, creation of virtual fibers disassociates its fiber connection with WDM equipment and prevents impact on the auto fiber search function, ensuring independence of SDH trail management. From the perspective of the WDM equipment, its service bearer layer is a virtual fiber instead of a real fiber after the virtual fiber is created. Deletion of the real fiber does not affect trail management.

Virtual NE Like a common NE, a virtual NE is also displayed with an icon on a view, but it is only an NE simulated according to the practical situation, which does not represent an actual NE. Therefore, the actual status of this NE cannot be queried and its alarm status cannot be displayed. Usually, when the trail management function is used for the NEs or subnets the NMS cannot manage, or the equipment is interconnected with other vendors NEs for service configuration, the end-to-end service configuration method and the trail management capability are provided.

VLAN ID Namely, it is the virtual LAN identifier. One Ethernet port can support 4K VLAN routes, and one NE can support up to 8K VLAN routes.

VPI Virtual path identifier. A VPI occupies 12 bits in NNI cells and 8 bits in UNI cells.

W

Wavelength Protection Group	The wavelength protection group is important to describe the wavelength protection structure. Its function is similar to that of the protection subnet in the SDH NE. The wavelength path protection can only work with the correct configuration of the wavelength protection group.
WDM Service	The WDM service is accessed at the client side of the OTU board that can access SAN services.
Web LCT	In the TMN architecture, the Web LCT is located in the NE management level, which can manage the RTN series and NG WDM series equipment.
Working Path	A specific path that is part of a protection group and is labeled working.
WTR Time	A period of time that must elapse from when a fault is recovered to the time when a trail/connection can be used again to transport the normal traffic signal and/or to select the normal traffic signal.
WTR	Wait to restore. This command is issued when a working path meets the restoration threshold after an SD or SF condition. It is used to maintain the status of the working path during the WTR period unless it is pre-empted by a higher priority bridge request.
WXCP	Wavelength cross-connection protection. A WXCP service is also known as a GE ADM service. It is a path protection service for ring networks. In this protection mode, services are dual-fed and selectively received. As a result, the services can be switched between the primary and secondary rings through cross-connects.

X

XML	The eXtensible Markup Language (XML) is a general-purpose markup language. It is classified as an extensible language, because it allows its users to define their own tags. Its primary purpose is to facilitate the sharing of structured data across different information systems, particularly through internet. It is used both to encode documents and serialize data.
------------	---