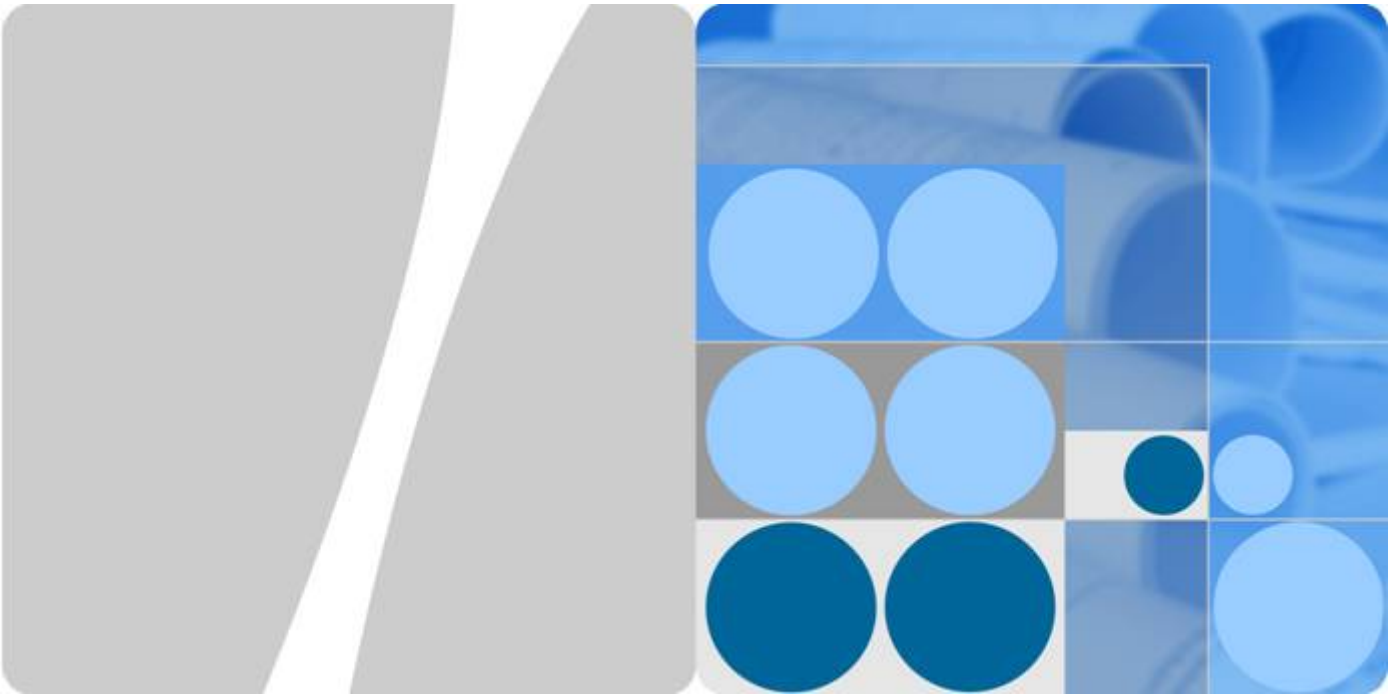


iManager U2000 Unified Network Management System

V100R002C01

Planning Guide

Issue 05

Date 2010-11-19

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 the 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

Related Version

The following table lists the product version related to this document.

Product Name	Version
iManager U2000	V100R002C01

Intended Audience

This document describes the planning you need to know before you use the U2000.

This document is intended for:

- Network planning engineers
- Technical support engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save time.

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.

GUI Conventions

The GUI conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Changes in Issue 05 (2010-11-19) Based on Product Version V100R002C01

Fixed some bugs.

Changes in Issue 04 (2010-09-24) Based on Product Version V100R002C01

Fixed some bugs.

Changes in Issue 03 (2010-08-16) Based on Product Version V100R002C01

Fixed some bugs.

Changes in Issue 02 (2010-07-16) Based on Product Version V100R002C01

Fixed some bugs.

Changes in Issue 01 (2010-05-18) Based on Product Version V100R002C01

Initial release.

Contents

Figures

Tables

1 Purpose of NMS Planning

This topic describes the purpose of NMS planning. Before you install or upgrade the NMS, the NMS planning must be ready. You can plan the NMS, the hardware and software configurations, the DCN, and the network parameters of the NMS server according to the information such as the analysis result of the current network, the networking target, and the service deployment trend.

The major contents of the NMS planning are as follows:

- **3 Network Scale Planning**
- **4 NMS Deployment Planning**
- **5 Software and Hardware Configuration Planning**
- **7 DCN Planning**
- **8 OSS Interconnection Planning**
- **6 Network Parameter Planning for the NM Server**
- **9 Security and Reliability Planning**

2 Network Management Planning Flow

This topic describes the network management planning flow.

Figure 2-1shows the flowchart for the network management planning.

Figure 2-1 Flowchart for network management planning

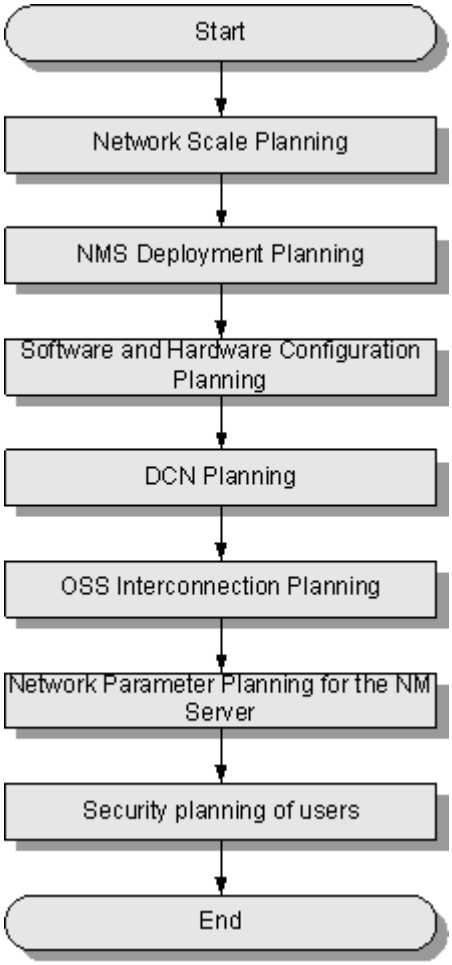


Table 2-1 Flow for network management planning

Item	Method	Input	Output
Network scale	See **3 Network Scale Planning**	Network element type, network element quantity, and reserved capacity.	Network equivalent network element total and network scale type.
Network management deployment	See **4.1 Planning of the U2000 Deployment Scheme**	Redundant protection scheme of the network management system, network scale and other deployment requirements.	Deployment scheme of the network management system and networking diagram of the deployment.
	See **4.2 Deployment Planning of NMS Components**	Network element type, network element quantity, and value-added function.	Component deployment scheme of the network element manager and component deployment scheme of the value-added function.
Software and hardware configuration of network management	See **5.1 Planning Rules for the U2000 Server Hardware Configuration**	Network scale and deployment scheme of the network management system.	Hardware configuration of the network management server
	See **5.2 Software Configuration Planning for the U2000 Server**	Hardware configuration of the network management server and redundant reliability program of the network management.	Software configuration of the network management server
	See **5.3 Client Configuration Planning**	Client configuration requirements of the network management	Client software and hardware configuration of the network management

Item	Method	Input	Output
	See **5.4 Planning of the Server Running Environment**	Running environment requirements of the network management server	Power distribution parts, cabinet, and equipment room configuration
DCN network planning	See **7 DCN Planning**	Hardware and software of the network management server and network scale.	DCN network diagram
OSS interconnection planning	See **8 OSS Interconnection Planning**	OSS system type and interconnection function.	Northbound interface program
Network parameters of network management server	See **6 Network Parameter Planning for the NM Server**	DCN network diagram and hardware configuration of the network management server.	Network parameters of the network management server, including name of the network management server, IP address, bandwidth, and port.
Security Planning	See **9.1 System Security Planning**	Security requirements of customers on the network management system	Authority and domain based management solution, user security, security of the operating system, security of the database, security of system data, security of data transmission, security of anti-virus, firewall, and system enhancement.

3 Network Scale Planning

About This Chapter

The network scale is an important input for the NMS deployment planning and hardware/ software configuration planning. In terms of the number of equivalent NEs in the network, the network scale is classified into small, medium, large and Super-large.

3.1 Network Scale Planning

This topic describes the principles and method for the network scale planning.

Planning Information Collection

You need to collect the following information for the network scale planning:

- NE type

  List the types of the NEs deployed on the management network.

- NE quantity

  List the quantity of the NEs of each type deployed on the management network.

- Reserved capacity

  Reserve the expansion capacity based on the network expansion planning in the future. If there is no capacity expansion planning, reserve 60% of the current network capacity for future expansion.

You need to collect the information listed in **Table 3-1** for the network scale planning.

Table 3-1 Collecting network scale information

NE Type/Port	Number of Physical NEs/Ports
NE type 1	X1
NE type 2	X2
...	...
NE type n	Xn
Total	X1 + X2 + ... + Xn

Planning Method

1. Calculate the current network scale.

   According to the **3.2 NE Equivalent Coefficient**, calculate the number of equivalent NEs of each NE type and the current network scale, as described in **Table 3-2**.

   Table 3-2 Calculating the current network scale

NE Type/Port	Number of Physical NEs/Ports	Number of Equivalent NEs
NE type 1	X1	Y1 **NOTE** Y1 = Equivalent coefficient of NE type 1 x Number of physical NEs or ports

NE Type/Port	Number of Physical NEs/Ports	Number of Equivalent NEs
NE type 2	X2	Y2
...	...	...
NE type n	Xn	Yn **NOTE** Yn = Equivalent coefficient of NE type n x Number of physical NEs or ports
Total	X1 + X2 + ... + Xn	Y1 + Y2 + ... + Yn

2. Plan the reserved expansion capacity.

   Reserve the expansion capacity based on the expected network scale in the future. If there is no capacity expansion planning, reserve the capacity for expansion with a proportion of 1:0.6 (wherein, **1** represents the current network scale, and **0.6** represents the reserved capacity).

3. Calculate the network scale.

   Calculation method: Planned network scale = current network capacity + reserved network capacity

4. Obtain the type of the current network scale.

   Mapping between the network scale and the number of equivalent NEs:

   - Small-scale network: less than 2000 equivalent NEs
   - Medium-scale network: 2000-6000 equivalent NEs
   - Large-scale network: 6000-15000 equivalent NEs
   - Super-large-scale network: 15000-20000 equivalent NEs

Planning Results

Table 3-3 describes the results of the network scale planning based on the NE information and equivalent NE coefficient table.

Table 3-3 Results of the network scale planning

NE Type/Port	Number of Physical NEs/ Ports	Number of Equivalent NEs
NE type 1	X1	Y1 **NOTE** Y1 = Equivalent coefficient of NE type 1 x Number of physical NEs or ports
NE type 2	X2	Y2
...	...	...

NE Type/Port	Number of Physical NEs/ Ports	Number of Equivalent NEs
NE type n	Xn	Yn **NOTE** Yn = Equivalent coefficient of NE type n x Number of physical NEs or ports
Reserved capacity	Xm	Ym
Total	X1 + X2 + ... + Xn + Xm	Y1 + Y2 + ... + Yn + Ym
Network scale	There are (xxx) equivalent NEs on the current network. This is the (xx) scale network.	

3.2 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 cards, ports, or channels are specific to NEs of different types. As these NEs require different resources of the NMS, the number of NEs that can be managed by the NMS depends on the NE types. For easy description and calculation of the management capability, the concept of equivalent NE is 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 required by them. The system resources required by an equivalent NE is 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)

Currently, a set of U2000 can manage a maximum of 15,000 physical NEs, 15,000 equivalent NEs, and 100 clients. This conclusion is drawn after the tests under a certain environment and objectively reflects the actual management capability of the U2000.

The management scales of the U2000 are defined as follows:

- Small-scale network: 2,000 equivalent NEs of the U2000
- Medium-scale network: 6,000 equivalent NEs of the U2000
- Large-scale network: 15,000 equivalent NEs of the U2000

NOTE

It is recommended that you enable no more than 100,000 performance collection instances at the same time to ensure the running efficiency of the U2000.

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 of the U2000 is OptiX Metro 1000.
- 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>
- The comparison coefficient of an equivalent NE of the U2000 to the equivalent NE in each domain is as follows:
  - 1 equivalent NE in the transport domain = 1 equivalent NE of the U2000
  - 4 equivalent nodes in the IP domain = 1 equivalent NE of the U2000
  - 3.3 equivalent nodes in the access domain = 1 equivalent NE of the U2000

  NOTE

  The preceding rules are not fixed. For more details, see the *Management Capability Instructions*.

3.2.1 Equivalent NEs in the Transport Domain
<Number of equivalent NEs in the transport domain> = (Number of transport NEs of type_I x Equivalent coefficient + ... + (Number of transport NEs of type_n x Equivalent coefficient)

3.2.2 Equivalent NEs in the IP Domain
<Number of equivalent NEs in the IP domain> = (Number of IP NEs of type_I x Equivalent coefficient) + ... + (Number of IP NEs of type_n x Equivalent coefficient)

3.2.3 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

3.2.1 Equivalent NEs in the Transport Domain

<Number of equivalent NEs in the transport domain> = (Number of transport NEs of type_I x Equivalent coefficient + ... + (Number of transport NEs of type_n x Equivalent coefficient)

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). Then, you can calculate the number of equivalent NEs in the transport domain as follows:

Number of equivalent NEs in the transport domain = 5 x 10 + 10 x 6.5 + 100 x 4.5 = 565

The management capability of the U2000 varies with OptiX NE Equivalents, as shown in **Table 3-4**.

Table 3-4 Management capabilities of the U2000 on different OptiX NE Equivalents

NE Series	NE Type	Equivalent Coefficient for the U2000
OSN series	OptiX OSN 500	1
	OptiX OSN 1500	3.5 (With ASON) 2.5 (Without ASON)
	OptiX OSN 2000	2
	OptiX OSN 2500	4.5 (With ASON) 3.5 (Without ASON)

NE Series	NE Type	Equivalent Coefficient for the U2000
	OptiX OSN 2500 REG	3.5 (Without ASON)
	OptiX OSN 3500	6.5 (With ASON) 4.5 (Without ASON)
	OptiX OSN 7500	10 (With ASON) 6.5 (Without ASON)
	OptiX OSN 9500	15 (With ASON) 10 (Without ASON)
MSTP series	OptiX Metro 100	0.5
	OptiX Metro 200	0.5
	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_I	2
	OptiX 155/622B_II	2
	OptiX 2500	3
	OptiX 2500 REG	1.5
Metro WDM series	OptiX Metro 6020	1
	OptiX Metro 6040	1
	OptiX Metro 6040V2	1
	OptiX Metro 6100	1.5
	OptiX Metro 6100V1	1.5
	OptiX Metro 6100V1E	1.5

NE Series	NE Type	Equivalent Coefficient for the U2000
	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, OptiX BWS 1600G OLA	1.5 +1.5 *N (N refers to the number of slave shelves)
	OptiX OTU40000	1
Marine series	OptiX BWS 1600S	1.5
	OptiX PFE 1670	1
	OptiX SLM 1630	1
NG WDM series	OptiX OSN 1800	1
	OptiX OSN 3800	3.5 (With ASON) 1.5 (Without ASON)
	OptiX OSN 6800	4+4*N (With ASON) 2+2*N (Without ASON) N refers to the number of slave shelves
	OptiX OSN 8800 T32	10+10*N (With ASON) 6+6*N (Without ASON) N refers to the number of slave shelves
	OptiX OSN 8800 T64	16+16*N (With ASON) 12+12*N (Without ASON) N refers to the number of slave shelves
NA WDM series	OptiX BWS 1600A	1.5
	OptiX BWS 1600(NA)	1.5
	OptiX OSN 1800(NA)	1
	OptiX OSN 3800A	3.5 (With ASON) 1.5 (Without ASON)
	OptiX OSN 6800A	4+4*N (With ASON) 2+2*N (Without ASON) N refers to the number of slave shelves

NE Series	NE Type	Equivalent Coefficient for the U2000
	OptiX OSN 8800 T32(NA)	10+10*N (With ASON) 6+6*N (Without ASON) N refers to the number of slave shelves
	OptiX OSN 8800 T64(NA)	16+16*N (With ASON) 12+12*N (Without ASON) N refers to the number of slave shelves
RTN series	OptiX RTN 605	0.4
	OptiX RTN 610	0.4
	OptiX RTN 620	0.5
	OptiX RTN 910	0.5
	OptiX RTN 950	1
	OptiX RTN 5000S	1

3.2.2 Equivalent NEs in the IP Domain

<Number of equivalent NEs in the IP domain> = (Number of IP NEs of type_I x Equivalent coefficient) + ... + (Number of IP NEs of type_n x Equivalent coefficient)

NOTE

For example, there are 5 NE5000E (equivalent coefficient: 10), 200 S5300 (equivalent coefficient: 1.25), and 1000 CX200 (equivalent coefficient: 0.625). Then, you can calculate the number of equivalent NEs in the IP domain as follows:

Number of equivalent NEs in the IP domain = 5 x 10 + 200 x 1.25 + 1000 x 0.625 = 925

The management capability of the U2000 varies with IP NE Equivalents, as shown in **Table 3-5**.

Table 3-5 Management capabilities of the U2000 on different IP NE Equivalents

NE Series	NE Type	Equivalent Coefficient for the U2000
Router	NE05/NE08(E)/NE16(E)	0.75
	NE20/NE20E	1.25
	NE40/NE80	5
	NE40E-X3	1.25
	NE40E-4	1.25

NE Series	NE Type	Equivalent Coefficient for the U2000
	NE40E-X8	2.5
	NE40E-8	2.5
	NE40E-X16	5
	NE40E-16	5
	NE5000E	10*N (N: number of chassis)
	R-series router	1
	AR-series router	0.25
Security equipment for load balancing and blocking	SSP	10
	NSE	10
Switch	S2000 series	0.125
	S2300 series	0.625
	S2700 series	0.625
	S3000 series	0.125
	S3300 series	0.75
	S3700 series	0.75
	S5000 series	0.25
	S5300 series	1.25
	S5700 series	1.25
	S6500 series	0.75
	S7800 series	1.25
	S8016 series	1.25
	S8500 series	1.25
	S9303 series	2.0
	S9306 series	3.5
	S9312 series	6.0
PTN series	OptiX PTN 1900	2.5
	OptiX PTN 3900	4.5
	OptiX PTN3900-8	4.0
	OptiX PTN 912	0.5

NE Series	NE Type	Equivalent Coefficient for the U2000
	OptiX PTN 910	0.5
	OptiX PTN 950	1
MAN service platform	CX200 series	0.625
	CX300 series	1.25
	CX600-X1	0.5
	CX600-X2	1
	CX600-X3	1.25
	CX600-4	1.25
	CX600-X8	2.5
	CX600-8	2.5
	CX600-X16	5
	CX600-16	5
Firewall	Eudomen 300/500/1000	0.5
	Eudomen 200E series	0.25
	Eudomen 1000E series	0.75
	Eudomen 8040	3
	Eudomen 8080	6
	Eudomen 8080E	4
	Eudomen 8160E	8
USG	USG9110	4
	USG9120	2
	USG9210	3
	USG9220	6
	USG9310	4
	USG9320	8
	USG5000 series	0.75
	USG3030	0.25
	USG3040	0.25
	USG2100 series	0.25

NE Series	NE Type	Equivalent Coefficient for the U2000
	USG2200 series	0.25
	USG50	0.25
SRG	SRG1200	0.25
	SRG20-10	0.25
	SRG20-11	0.25
	SRG20-12	0.25
	SRG20-15	0.25
	SRG20-20	0.25
	SRG20-21	0.25
	SRG20-30	0.25
	SRG20-31	0.25
	SRG20-31-D	0.25
SIG	SIG9810	4
	SIG9820	8
	SIG9800 Server	4
SVN	SVN3000	0.25
Broadband access	MA5200E/F series	1.5
	MA5200G series	10
	ME60 series	10
Voice gateway	VG1040/1041 series	0.25
WLAN AP	AP	0.25

3.2.3 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

- Number of FTTx OLT equivalent NEs = (Number of ONTs x Equivalent coefficient) + (Number of MDUs x Equivalent coefficient) + (Number of P2P ports x Equivalent coefficient)
- Number of FTTx MDU equivalent NEs = (Number of ports of type_I x Equivalent coefficient) + ... + (Number of ports of type n x Equivalent coefficient)
- Number of MSAN equivalent NEs = (Number of ports of type_I x Equivalent coefficient) + ... + (Number of ports of type n x Equivalent coefficient)
- Number of DSLAM equivalent NEs = (Number of ports of type_I x Equivalent coefficient) + ... + (Number of ports of type_n x Equivalent coefficient)
- Number of equivalent NEs of other access equipment = (Number of NEs of type_I x Equivalent coefficient) + ... + (Number of NEs of type_n x Equivalent coefficient)

The management capability of the U2000 varies with access NE Equivalents, as shown in **Table 3-6**.

Table 3-6 Management capabilities of the U2000 on different access NE Equivalents

Class	Type	Equivalent Coefficient for the U2000
FTTx OLT (calculation based on the managed ONT, MDU, and P2P resources in the case of OLT)	ONT	1/64
	MDU	1/32
	P2P port	1/64
FTTx MDU (calculation based on the managed user ports in the case of MDU)	xDSL port	1/128
	E1 port	1/128
	ETH port	1/128
	PSTN/ISDN/HSL port	1/160
MSAN (calculation based on the number of managed ports)	xDSL port	1/128
	E1 port	1/128
	ETH port	1/128
	PSTN/ISDN/HSL port	1/160
DSLAM (calculation based on the number of managed ports)	xDSL port	1/128
	E1 port	1/128
	ETH port	1/128
Other NEs (calculation based on the NE types)	MD5500	1.5
	8850	18
	8825	18
	8750	18
	MA5200V1R2/R9	3

4 NMS Deployment Planning

About This Chapter

Through NMS deployment planning, you can determine the NMS deployment scheme and the NMS component deployment scheme (determining the components and instances to be deployed).

4.1 Planning of the U2000 Deployment Scheme

This topic describes how to plan a U2000 deployment scheme according to the network scale and disaster recovery requirements.

4.1.1 Principles of Planning a U2000 Deployment Scheme

This topic describes the principles of planning a U2000 deployment scheme.

Planning Principle

The U2000 supports four deployment schemes. You can choose the desired NMS deployment scheme according to the supported platform and the requirement on disaster recovery.

NOTE

- 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 on 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. To realize disaster recovery, the master and slave servers can be located in different areas. The U2000 supports the HA system (remote Veritas hot standby) to achieve disaster recovery. The HA system consists of primary and secondary sites, the master and slave servers of which can be deployed in different areas. The automatic switchover between the master and slave servers ensures uninterrupted system running.
- A distributed system consists of the master server and slave server, which constitute a site to provide the functions of the U2000. The master server, the core part of the distributed system, runs the database server and the core U2000 components. The slave server runs the non-core U2000 components to save the CPU and memory usage of the master server. In this manner, the load is balanced between the master server and the slave server. Due to complicated networking, it is recommended that you choose the centralized deployment scheme.

Table 4-1 U2000 deployment scheme

NMS Deployment Solution	Supported Platform	Requirement on Disaster Recovery	Networking Complexity
Centralized Deployment Scheme for a Single-Server System	● Windows ● Solaris	Low	Simple
Centralized Deployment Scheme for an HA System	● Windows ● Solaris	High	Simple
Distributed Deployment Scheme for a Single-Server System	SUSE Linux	Low	Complex
Distributed Deployment Scheme for an HA System	SUSE Linux	High	Complex

Planning Result

According to the preceding planning principles and other requirements of customers, you can select any of the following U2000 deployment scheme:

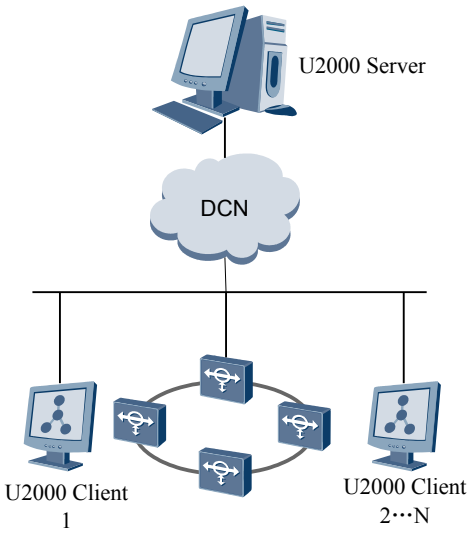
- **Centralized Deployment Scheme for a Single-Server System**
- **Centralized Deployment Scheme for an HA System**
- **Distributed Deployment Scheme for a Single-Server System**
- **Distributed Deployment Scheme for an HA System**

4.1.2 Deployment Scheme for the Centralized Single-Server System

This topic describes the principles for and networking of the deployment scheme for the centralized U2000 single-server system.

The deployment scheme for the centralized single-server system is applicable to Windows OS or Solaris OS. In the centralized deployment mode, there is only one U2000 server. Multiple clients can access and operate the server and all processes run on the server. **Figure 4-1** shows the networking diagram of the deployment scheme for the centralized single-server system.

Figure 4-1 Deployment scheme for the centralized single-server system



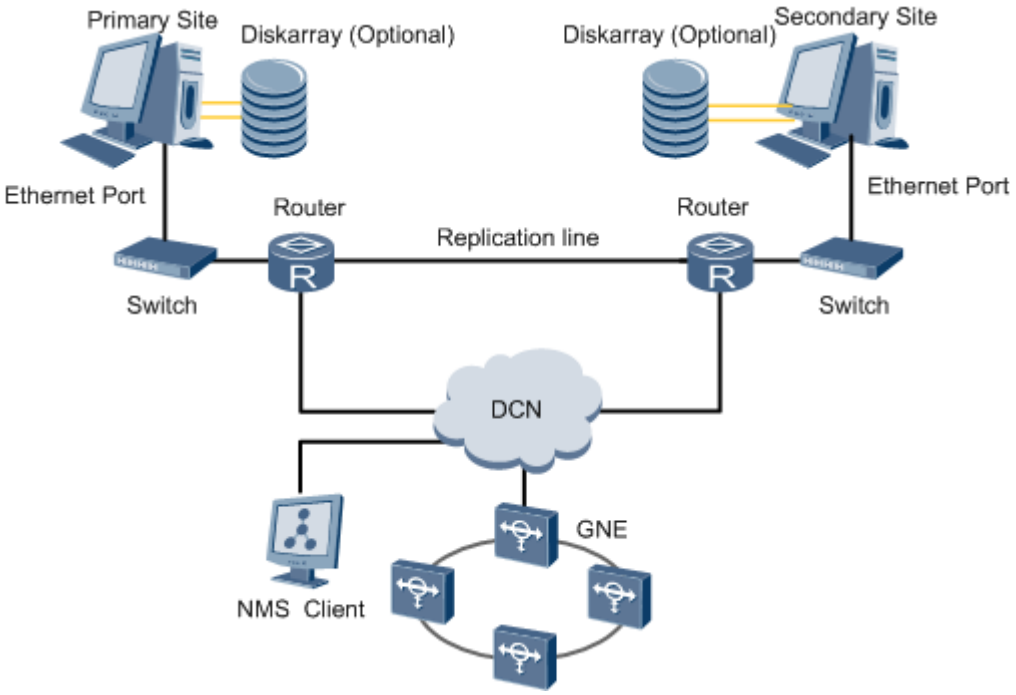
4.1.3 Deployment Scheme for the Centralized HA System

This topic describes the principles for and networking of the deployment scheme for the centralized U2000 high availability (HA) system.

- The centralized U2000 HA system can be deployed on the Windows OS or Solaris OS.
- The centralized U2000 HA system consists of primary and secondary sites. Only one server can reside on each site. The primary and secondary sites can be deployed either in the same place (local deployment) or in different cities (remote deployment).
- The centralized U2000 HA system integrates the Veritas remote hot backup technology to realize the real-time synchronization between the primary site and secondary site and the dynamic monitoring of the U2000 running status. When the primary site becomes faulty, services automatically switches to the secondary site and the system continues monitoring the network.

The following figure shows the networking diagram of the deployment scheme for the centralized U2000 HA system.

Figure 4-2 Deployment scheme for the centralized HA system

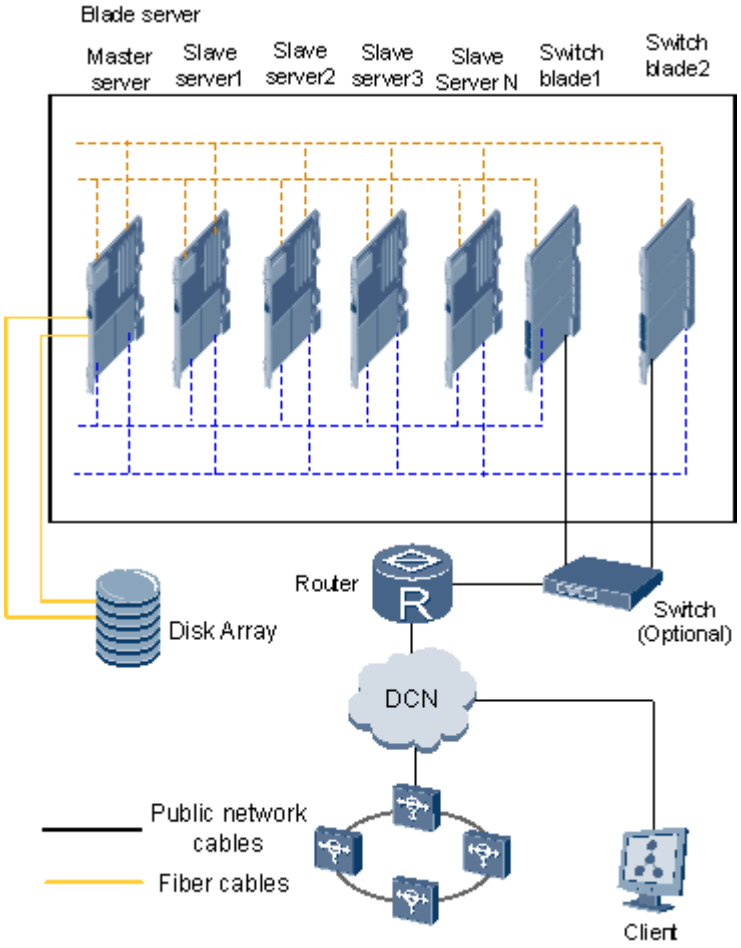


4.1.4 Deployment Scheme for the Distributed Single-Server System

This topic describes the principles for and networking of the deployment scheme for the distributed U2000 single-server system.

The distributed U2000 single-server system is deployed on the SUSE Linux OS. There are one master and multiple slave servers. The distributed U2000 single-server system supports the access to and operations on multiple clients. **Figure 4-3** shows the networking diagram of the deployment scheme for the distributed single-server system.

Figure 4-3 Deployment scheme for the distributed single-server system



The following is the networking description:

- The distributed system can be installed only on the blade server. A blade acts as a server.
- A distributed system consists of the master server and slave server, which constitutes a site to provide the functions of the U2000. The master server, the core part of the distributed system, runs the database server and the core U2000 components. The slave server runs the non-core U2000 components to save the CPU and memory usage of the master server. In this manner, the load is balanced between the master server and the slave server. The number of slave servers is determined by the current network scale.
- The disk array is used to store database data to improve the performance of the database. When the management scale of the U2000 exceeds the medium level, the master server must be configured with a disk array.

4.1.5 Deployment Scheme for the Distributed HA System

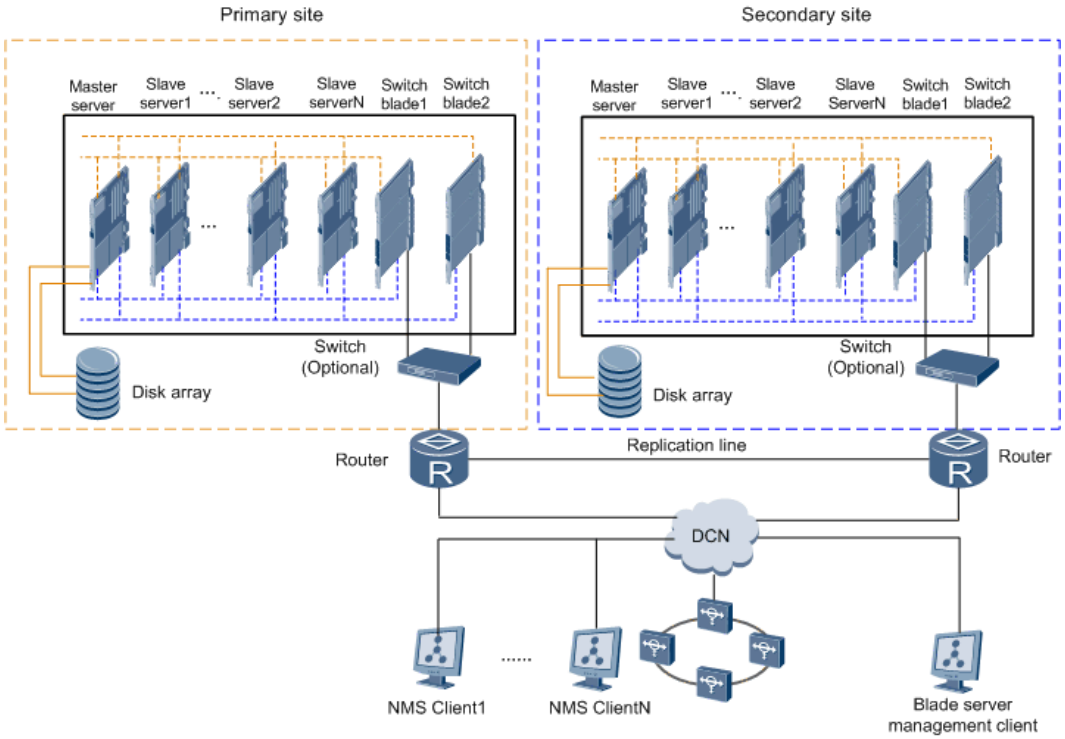
This topic describes the principles for and networking of the deployment scheme for the distributed U2000 high availability (HA) system.

- The distributed U2000 HA system is deployed on the SUSE Linux OS.

- The distributed U2000 HA system consists of primary and secondary sites. Multiple servers reside on each site. The primary and secondary sites can be deployed either in the same place (local deployment) or in different cities (remote deployment).
- The distributed U2000 HA system integrates the Veritas remote hot backup technology to realize the real-time synchronization between the primary site and secondary site and the dynamic monitoring of the U2000 running status. When the primary site becomes faulty, the system automatically switches services to the secondary site and continues monitoring the network.

Figure 4-4 shows the networking diagram of the deployment scheme for the distributed HA system.

Figure 4-4 Deployment scheme for the distributed HA system



The following is the networking description:

- The distributed HA system supports the installation only on the blade server. A blade acts as a server.
- The distributed HA system is composed of the primary site and secondary site. The master server and slave server reside on each site. The master server, the core part of the distributed system, runs the database server and the core U2000 components. The slave server runs the non-core U2000 components to save the CPU and memory usage of the master server. In this manner, the load is balanced between the master server and the slave server. The number of slave servers is determined by the current network scale.
- The disk array is used to store database data to improve the performance of the database.

4.2 Deployment Planning of NMS Components

This topic describes the deployment planning of NMS components. A component is the software function unit that you can choose to install. Before installing the U2000, you need to plan the components to be installed and the number of deployment package instances corresponding to the components according to the functions of the software the user purchases.

4.2.1 Planning the Deployment of Components on the Centralized NMS

This topic describes the rules for and method of planning the deployment of components on the centralized NMS.

Collecting Information

The following information needs to be collected for planning the deployment of network management components.

- NE type

  List NE series on the managed network according to the **NE List**.
- NE quantity

  List the number of NEs of each type on the managed network.
- Value-added functions

List the value-added functions subscribed by users.

Planning Method

The method of planning the deployment of components on the centralized NMS is as follows:

1. Plan the components to be installed.

   Component installation is applicable to the following scenarios:

   - **Installation by typical network**: The installation program supports the ability to install components of the transport domain, IP domain, access domain, or all domains. When planning components, you only need to learn the domain to which the NE to be managed belongs, instead of planning the specific components to be installed. The installation program automatically configures the required components according to that domain.
   - **Installation by license**: The installation program automatically configures the required components according to information about the obtained U2000 license. In this scenario, you only need to apply for the U2000 license before installation, instead of planning the specific components to be installed.
   - **Custom installation**: Plan the components to be installed according to the equipment to be managed and the value-added functions to be purchased. You also need to refer to **4.2.3 NMS Component Deployment Information List** during the planning.

   NOTE

   During the planning, you can plan to install all components.

   - Advantage of full installation: It facilitates network expansion in the future.
   - Disadvantages of full installation: The installation takes a long time and imposes high requirements for server configurations.

2. Plan the number of deployment package instances. Calculate the number of required deployment package instances according to **4.2.4 NMS Deployment Package List** and the number of equivalent NEs of different NE series.

   For example, the number of equivalent NEs of the OTN series is 3050 and each OTN NE management instance can manage a maximum of 2000 equipment NEs. In this case, two OTN NE management instances need to be deployed.

   NOTE

   During the planning, you only need to plan the number of deployment package instances of the **Single-server multi-instance** type. The number of deployment package instances of the **System single-instance** or **Single-server single-instance** type defaults to **1** and does not need to be planned.

4.2.2 Planning the Deployment of Components on the Distributed NMS

This topic describes the rules for and method of planning the deployment of components on the distributed NMS.

Collecting Information

The following information needs to be collected for planning the deployment of network management components.

- NE type

  List NE series on the managed network according to the **NE List**.

- NE quantity

List the number of NEs of each type on the managed network.

- Value-added functions

  List the value-added functions subscribed by users.

Planning Method

The method of planning the deployment of components on the distributed NMS is as follows:

1. Plan the components to be installed. Plan the components to be installed according to the equipment to be managed and the value-added functions to be purchased. You also need to refer to **4.2.3 NMS Component Deployment Information List** during the planning.

   For example, the OptiX OSN 3800 belongs to the OTN series and is managed by the OTN NE management component. Therefore, the OTN NE management component needs to be installed.

   NOTE

   During the planning, you can plan to install all components.

   - Advantage of full installation: It facilitates network expansion in the future.
   - Disadvantages of full installation: The installation takes a long time and imposes high requirements for server configurations.

2. Plan the number of deployment package instances and the deployment location. The planning rules are as follows:
   - Calculate the number of required deployment package instances according to **the management capability of a single instance** and the number of equivalent NEs of different NE series.
   - The primary server is preferentially used to deploy the database and deployment packages applicable to only the primary server. It is recommended that you do not deploy other deployment packages on the primary server.
   - On a server, you can deploy deployment packages of only one domain. If the number of configured slave servers is insufficient, deploy deployment packages of different domains on the same server according to the load balancing policy.
   - The NE Manager, common applications, and E2E deployment packages of the same domain should be deployed on the same server.
   - The non-default TrapReceiver service component is deployed together with the deployment packages that are applicable to SNMP. Common deployment packages applicable to SNMP include **Access Network Single Element Management Service**, **Switch Network Element Management**, **RouterMgr/SgMgr Component**, and **Security Network Element Management**.
   - **DeskTop Service Component** can be deployed only on the master server and only one instance can be deployed.
   - **NMS Log Zip Management** needs to be deployed on each server and one instance needs to be deployed on each server.

4.2.3 NMS Component Deployment Information List

A component is the minimum functional unit that can be installed. Before installing the U2000, you can select the required components according to the equipment to be managed and the value-added functions to be purchased.

U2000 Components

A component is a functional unit that you can choose to install. The U2000 components are classified into the following types:

- Common components
- Network Element management components
- Network service management components
- Northbound interface components
- Other components

Table 4-2 lists the U2000 components and their functions. Before installing the U2000, you need to plan the components to be installed according to the equipment to be managed and the value-added functions to the purchased.

NOTE

- **Base Component** and **Client Auto Upgrade** are mandatory components. By default, they are installed during installation.
- All components except **Base Component** and **Client Auto Upgrade** are optional. You can determine whether to install certain components according to the equipment to be managed and the value-added functions to be purchased. You can also install all components on the condition that high requirements for server hardware configurations are met.

Table 4-2 U2000component list

Component Type	Component Name	Description
Common component	Base Component	It provides the Web service, distributed NE deployment service, data collection of NE operation logs and running logs, and inventory data management of physical resources.
	Performance Management	It provides the performance management functions, including performance monitoring, threshold management, performance query, performance report, and performance collection.
	Client Auto Upgrade	It provides the function of automatic client upgrade.
	Auto Provisioning	When the equipment in the access domain or IP domain accesses the NMS, the NMS automatically assigns an IP address to the equipment and initializes equipment configurations.
NE management	Access Network Element Management	It manages access NEs. For details, see: ● **10.7 Manageable FTTx Series Equipment** ● **10.8 Manageable MSAN Series Equipment** ● **10.9 Manageable DSLAM Series Equipment**
	Router Network Element Management	It manages routers. For details, see: **10.10 Manageable Router Series Equipment**.

Component Type	Component Name	Description
	Switch Network Element Management	It manages switches. For details, see: **10.11 Manageable Switch Series Equipment**.
	Security Network Element Management	It manages firewall, USG, SIG, and SVN series security equipment. For details, see: ● **10.12 Manageable Metro Service Platform Equipment** ● **10.13 Manageable Broadband Access Series Equipment** ● **10.14 Manageable VoIP Gateway Equipment** ● **10.16 Manageable Firewall Series Equipment** ● **10.17 Manageable DPI Equipment** ● **10.18 Manageable SVN Series Equipment**
	PTN Network Element Management	It manages Metro Ethernet PTN frame-shaped and case-shaped NEs. For details, see: **10.6 Manageable PTN Series Equipment**.
	SDH Network Element Management	It manages SDH, MSTP, and OSN series equipment. For details, see: **SDH series** and **MSTP series** in the **10.1 Manageable MSTP Series Equipment**.
	WDM Network Element Management	It manages LH WDM and Metro WDM series equipment. For details, see: **10.2 Manageable WDM Series Equipment**.
	RTN Network Element Management	It manages RTN series equipment. For details, see: **10.5 Manageable RTN Series Equipment**.
	OTN Network Element Management	It manages OTN series equipment. For details, see: **OSN series** in the **10.1 Manageable MSTP Series Equipment**.
	Marine Network Element Management	It manages Marine series equipment. For details, see: **10.4 Manageable Submarine Line Equipment**.
	Third-Party Network Element Management	It manages third-party transport series equipment.
	NA OTN Network Element Management	It manages North America OTN series equipment.
	NA WDM Network Element Management	It manages North America WDM series equipment.

Component Type	Component Name	Description
Network Service Management	MSTP Service Management	It provides the end-to-end MSTP and ETH/ATM management function.
	OTN Service Management	It provides the end-to-end OTN management function.
	SDH Service Management	It provides the end-to-end SDH management function.
	Composite Service Management	It provides the composite service management function.
	IP Service Management	It provides the end-to-end IP management function.
	Ason SDH Management	It provides the ASON SDH management function.
	Ason OTN Management	It provides the ASON OTN management function.
North-Bound Interface	North-Bound CORBA Interface	It provides the CORBA NBI function.
	North-Bound MML Interface	It provides the MML NBI function.
	North-Bound XML Interface	It provides the XML NBI function.
	North-Bound SNMP Interface	It provides the SNMP NBI function.
	North-Bound Text Interface	It provides the text NBI function.
Other component	Optical fiber line Automatic Monitoring System	It monitors the connection status of optical fibers.
	NE Data Collector	It provides the function of collecting NE data.
	Default TrapReceiver Service Component	Receive the trap report from NE for the SNMP interface device.
	Non-Default TrapReceiver Service Component	Receive the trap report from NE as the default extension the for default TrapReceiver.

4.2.4 NMS Deployment Package List

This topic describes the list of NMS deployment packages. A deployment package is a software unit deployed on a server. You need to plan the number of deployment package instances and the deployment location before installing the U2000.

A deployment package is a software unit deployed on a server. one instance is generated each time the deployment package is deployed on the server. According to the deployment location and quantity on the U2000, the U2000 deployment package can be classified into the following types:

- System single-instance: Such deployment packages can be installed only on a single server and the server can be deployed with only one instance.
- Single-server single-instance: Such deployment packages can be installed on multiple servers and each server can be deployed with only one instance.
- Single-server multi-instance: Such deployment packages can be installed on multiple servers and each server can be deployed with multiple instances.

TIP

The differences between a component and a deployment package are as follows:

- A component is a functional unit of the U2000. That is, a component implements a function of the U2000.
- A deployment package is a software unit deployed on a server. A component can consist of one or more deployment packages.
- If a component consists of only one deployment package, the names of the deployment package and the component are the same. The function of the component is implemented if the deployment package is deployed.
- If a component consists of multiple deployment packages, all the deployment packages need to be deployed to implement the function of the component. In a distributed system, the deployment packages can be deployed on different servers.

Table 4-3 lists U2000 deployment packages.

Table 4-3 U2000 deployment packages

Deployment Package Name	Deployment Package Type	Deployment Location	Maximum Number of Equivalent NEs That Each Instance Can Manage
Default TrapReceiver Service Component	System single-instance	Master server	N/A
Physical Inventory Management	System single-instance	Master server	N/A
Equipment Log	System single-instance	Master server	N/A
Performance Management	System single-instance	Master server	N/A

Deployment Package Name	Deployment Package Type	Deployment Location	Maximum Number of Equivalent NEs That Each Instance Can Manage
NE Software Management	System single-instance	Master server	N/A
XFTP	System single-instance	Master server	N/A
Access Environment and Power Monitoring	System single-instance	Master server	N/A
Access Network Global Elements Management Service	System single-instance	Master server	N/A
Network Web LCT	System single-instance	Master server	N/A
Optical fiber line Automatic Monitoring System	System single-instance	Master server	N/A
NE Data Collector	System single-instance	Master server	N/A
Batch Config Component	System single-instance	Master server	N/A
GCLI Component	System single-instance	Master server	N/A
PnP	System single-instance	Master server	N/A
North-Bound XML Interface	System single-instance	Master server	N/A
North-Bound Text Interface	System single-instance	Master server	N/A
North-Bound SNMP Interface	System single-instance	Master server	N/A
North-Bound CORBA Interface	System single-instance	Master server	N/A
Security Policy Management	System single-instance	Master server	N/A
Security VPN Management	System single-instance	Master server	N/A

Deployment Package Name	Deployment Package Type	Deployment Location	Maximum Number of Equivalent NEs That Each Instance Can Manage
Security Common	System single-instance	Master server	N/A
Access Device Log	System single-instance	Master server	N/A
Router V8 management subsystem	System single-instance	Master server	N/A
Composite Service Management	System single-instance	Master or slave server	N/A
IP Service Management	System single-instance	Master or slave server	N/A
SDH Service Management	System single-instance	Master or slave server	N/A
OTN Service Management	System single-instance	Master or slave server	N/A
MSTP Service Management	System single-instance	Master or slave server	N/A
Service Management Base	System single-instance	Master or slave server	N/A
North-Bound MML Interface	System single-instance	Master or slave server	N/A
Ason OTN Management	System single-instance	Master or slave server	N/A
Ason SDHManagement	System single-instance	Master or slave server	N/A
Access Network Single Element Management Service	Single-server single-instance	Master or slave server	15000 equivalent NEs
Security Network Element Management	Single-server single-instance	Master or slave server	5000 equivalent NEs
Switch Management	Single-server single-instance	Master or slave server	5000 equivalent NEs
Router and Service Gateway Management	Single-server single-instance	Master or slave server	15000 equivalent NEs

Deployment Package Name	Deployment Package Type	Deployment Location	Maximum Number of Equivalent NEs That Each Instance Can Manage
Performance Collector	Single-server single-instance	Master or slave server	N/A
Non-Default TrapReceiver Service Component	Single-server single-instance	Master or slave server	N/A
DeskTop Service Component	Single-server single-instance	Master or slave server	100 clients
Marine Network Element Management	Single-server single-instance	Master or slave server	2000 equivalent NEs
SDH Network Element Management	Single-server single-instance	Master or slave server	2000 equivalent NEs
PTN Network Element Management	Single-server multi-instance	Master or slave server	2000 equivalent NEs
Third-Party Network Element Management	Single-server multi-instance	Master or slave server	2000 equivalent NEs
OTN Network Element Management	Single-server multi-instance	Master or slave server	2000 equivalent NEs
RTN Network Element Management	Single-server multi-instance	Master or slave server	2000 equivalent NEs
WDM Network Element Management	Single-server multi-instance	Master or slave server	2000 equivalent NEs
NA WDM Network Element Management	Single-server multi-instance	Master or slave server	2000 equivalent NEs
NA OTN Network Element Management	Single-server multi-instance	Master or slave server	2000 equivalent NEs

4.2.5 Example for Planning the Deployment of Components on the Centralized NMS

This topic describes how to plan the deployment scheme of NMS components with examples. The result of the planning is taken as the reference for the components required for the installation of the U2000 and the number of deployment package instances.

Example Description

A total of 500 OptiX OSN 3500 devices, 100 OptiX OSN 7500 devices, 700 OptiX OSN 3800 devices (With ASON), and 200 NE80E devices must be managed in the network. The carrier

has purchased the value-added features such as SDH end-to-end feature, WDM end-to-end feature, and Corba northbound interface feature. In this case, how to plan the NM subsystem deployment scheme for this carrier?

Planning Method

1. Determine the components to be installed according to NE types and value-added functions to be purchased.

Table 4-4 NE management components to be installed

Component Type	NE Type	Related Component
NE Type	OptiX OSN 3500	SDH NE management
	OptiX OSN 7500	
	OptiX OSN 3800 (With ASON)	OTN NE management
	NE80E	Router NE management
Value-Added Feature	SDH end-to-end feature	SDH service management
	OTN end-to-end feature	OTN service management
	CORBA northbound interface feature	North-bound CORBA interface

According to **4.2.3 NMS Component Deployment Information List**, the carrier needs to install the **SDH Network Element Management, OTN Network Element Management, Router Network Element Management, SDH Service Management, OTN Service Management, North-Bound CORBA Interface, Base Component and Client Auto Upgrade** components.

2. Calculate the number of equivalent NEs of each NE series, and calculate the number of the deployment package instances according to the maximum management capability of the NE management.

Table 4-5 Number of NE management instances to be deployed

NE Type	Number of Equivalent NEs (number of physical NEs x equivalent coefficient)	Related Component	Number of Deployment Package Instances
OptiX OSN 3500	500 x 4.5	SDH NE management	2

NE Type	Number of Equivalent NEs (number of physical NEs x equivalent coefficient)	Related Component	Number of Deployment Package Instances
OptiX OSN 7500	100 x 6.5		**NOTE** The SDH NE management instance can manage a maximum of 2000 equivalent NEs. Therefore, two SDH NE management instances must be deployed.
OptiX OSN 3800 (With ASON)	700 x 1.5	OTN NE management	1 **NOTE** The OTN NE management instance can manage a maximum of 2000 equivalent NEs. Therefore, one OTN NE management instance must be deployed.
NE80E	200 x 5	Router NE management	1 **NOTE** The router NE management instance can manage a maximum of 15000 equivalent NEs. Therefore, one router NE management instance must be deployed.

According to **4.2.4 NMS Deployment Package List**, the carrier needs to deploy **two SDH NE management instances, one OTN NE management instance, and one router NE management instance**. The number of deployment package instances that are not used for NE management does not need to be planned. By default, only one instance is deployed.

4.2.6 Example for Planning the Deployment of Components on the Distributed NMS

This topic describes how to plan the deployment of NMS component with an example. You need to plan the number of components to be installed on the U2000 and the number of deployment package instances according to the planning result.

Example Description

A total of 500 OptiX OSN 3500 devices, 100 OptiX OSN 7500 devices, 700 OptiX OSN 3800 devices (With ASON), and 200 NE80E devices must be managed in the network. The carrier has purchased the value-added features such as SDH end-to-end feature, WDM end-to-end feature, and Corba northbound interface feature. In this case, how to plan the NM subsystem deployment scheme for this carrier?

Planning Method

1. Determine the components to be installed according to NE types and value-added functions to be purchased.

Table 4-6 NE management components to be installed

Component Type	NE Type	Related Component
NE Type	OptiX OSN 3500	SDH NE management
	OptiX OSN 7500	
	OptiX OSN 3800 (With ASON)	OTN NE management
	NE80E	Router NE management
Value-Added Feature	SDH end-to-end feature	SDH service management
	OTN end-to-end feature	OTN service management
	CORBA northbound interface feature	North-bound CORBA interface

According to **4.2.3 NMS Component Deployment Information List**, the carrier needs to install the **SDH Network Element Management, OTN Network Element Management, Router Network Element Management, SDH Service Management, OTN Service Management, North-Bound CORBA Interface, Base Component and Client Auto Upgrade** components.

2. Calculate the number of equivalent NEs of each NE series and the number of deployment package instances to be deployed according to the maximum management capability of the NE Manager.

Table 4-7 Number of deployment package instances to be deployed

NE Type	Number of Equivalent NEs (number of physical NEs x equivalent coefficient)	Related Component	Number of Deployment Package Instances
OptiX OSN 3500	500*4.5	SDH NE management	2

NE Type	Number of Equivalent NEs (number of physical NEs x equivalent coefficient)	Related Component	Number of Deployment Package Instances
OptiX OSN 7500	100*6.5		**NOTE** The SDH NE management instance can manage a maximum of 2000 equivalent NEs. Therefore, two SDH NE management instances must be deployed.
OptiX OSN 3800 (With ASON)	700*1.5	OTN NE management	1 **NOTE** The OTN NE management instance can manage a maximum of 2000 equivalent NEs. Therefore, one OTN NE management instance must be deployed.
NE40E	100*10	Router NE management	1 **NOTE** The router NE management instance can manage a maximum of 15000 equivalent NEs. Therefore, one router NE management instance must be deployed.
Total (current network scale)	4950		
Reserved network capacity	4950*0.6		
Total (planned network scale)	4950+4950*0.6		

NE Type	Number of Equivalent NEs (number of physical NEs x equivalent coefficient)	Related Component	Number of Deployment Package Instances
Network scale	There is a total of 7920 equivalent NEs, which is within the range from 6K to 15K. Therefore, the network scale is large. According to **5.1.1 Principles for Hardware Configuration Planning of the NMS Server**, the **blade*5+disk array** configurations can meet the requirement. That is, the distributed system should consist of one master server and four slave servers. **NOTE** Mapping between the network scale and the number of equivalent NEs: ● Small-scale network: less than 2000 equivalent NEs ● Medium-scale network: 2000-6000 equivalent NEs ● Large-scale network: 6000-15000 equivalent NEs ● Super-large-scale network: 15000-20000 equivalent NEs		

3. Plan the deployment location of each deployment package according to the number of deployment package instances and deployment locations.

Server	Deployment Package	Number of Instances
Master server	CORBA NBI + deployment package that is deployed on the master server by default	Default quantity: **1**
Slave server 1	SDH Network Element Management	**1**
	SDH Service Management	Default quantity: **1**
Slave server 2	SDH Network Element Management	**1**
Slave server 3	OTN Network Element Management	**1**
	OTN Service Management	Default quantity: **1**
Slave server 4	Router and Service Gateway Management	**1**
	Non-default TrapReceiver service component	**1**

5 Software and Hardware Configuration Planning

About This Chapter

This topic describes the principles of the configuration planning for the U2000 server. In addition, this topic describes how to choose the configuration of server software and hardware, and how to configure a client.

5.1 Planning Rules for the U2000 Server Hardware Configuration

This topic describes how to reasonably plan the hardware configuration of the U2000 server.

5.1.1 Principles for Hardware Configuration Planning of the NMS Server

This topic describes the method of and procedure for the hardware configuration planning of the NMS server.

Planning Information Collection

You need to collect the following information for hardware configuration planning of the NMS server:

- Network scale

  You can obtain the network scale of the carrier according to **Network Scale Planning**.
- NMS deployment scheme

  You can obtain the NMS deployment scheme according to **Planning of the U2000 Deployment Scheme**.

Planning Principles

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

- Select proper hardware configurations according to the network scale.
- Configure independent uninterrupted power supply (UPS) for the U2000 server. This can avoid some serious problems such as hardware damage, system restoration failure, and data loss caused by abnormal power failure.
- If multiple configuration schemes can meet the requirements of the current network scale, determine the specific hardware configurations according to the requirements of customers.
- If the deployments in both distributed mode and centralized mode can meet the requirements in the current network scale, do not adopt distributed deployment in consideration of the complexity of networking and maintenance.

Planning Method

You need to determine hardware configurations according to the network scales and the management capacities of the NMSs based on different hardware platforms.

NOTE

- Hardware selection is relevant to the number of managed equivalent NEs only. All the following hardware support high availability system installation.
- If the HA system is applied, you need to multiply the hardware quantity by 2. For example, if the current large-scale network applies the HA system, the following hardware requirements need to be met:
  - Two M4000s and two OceanStor S2600s.
  - Two blade server shelves and two OceanStor S2600s. Each blade server shelf contains at least five blades.
- If a blade server is used, you can install multiple U2000s on the same shelf.

Table 5-1 Management capacities of NMSs based on different hardware platforms

Network Scale	PC Server (Windows OS-Supported)	Sun Server (Solaris OS-Supported)	Blade Server (SUSE Linux OS-Supported)
Small-scale network: less than 2000 equivalent NEs	HP DL380G6 (CPU: 2 x Xeon quatri-core 2.0 GHz or later; memory: 8 GB; hard disk: 5 x 146 GB)	Sun T5220 (CPU: 4C x 1.2 GHz; memory: 16 GB; hard disk: 6 x 146 GB)	Centralized scenario: blade server x 1+ **disk array** **NOTE** The blade acts as the master server. The slave server is not configured.
Medium-scale network: 2000-6000 equivalent NEs	HP DL580G5 (CPU: 4 x Xeon quatri-core 2.13 GHz or later; memory: 16 GB; hard disk: 4 x 146 GB)	Sun T5220 (CPU: 8C x 1.4 GHz; memory: 32 GB; hard disk: 6 x 146 GB)	Centralized scenario: Master server blade x 3 + **disk array** **NOTE** One blade acts as the master server. The other two blades act as the slave servers.
Large-scale network: 6000-15000 equivalent NEs	-	Sun M4000 (CPU: 4CPU x 2.53GHz (quatri-core); memory: 32 GB; hard disk: 2 x 146 GB or 2 x 300 GB) + **disk array**	Distributed scenario: blade server x 5 + **disk array** **NOTE** One blade acts as the master server. The other four blades act as the slave servers.
Super-large-scale network: 15000-20000 equivalent NEs	-	-	Distributed scenario: blade server x 6 + **disk array** **NOTE** One blade acts as the master server. The other five blades act as the slave servers.

Table 5-2 Recommended configurations of the blade server

Model of the Blade Server	Configurations
IBM blade server	Blade center E chassis + IBM HS21 (CPU: 2 x Intel Xeon quatri-core 2.5 GHz; memory: 16 GB; hard disk: 2 x 146 GB)
ATAE blade server	T8223 chassis + BH23C server card (CPU: 2 x Intel Xeon quatri-core 2.33 GHz; memory: 16 GB; hard disk: 2 x 146 GB)

Table 5-3 Recommended configurations of the disk array

Hardware Configuration Item	Capacity
OceanStor S2600	6 x 300 GB

5.1.2 Example: Hardware Configuration Planning for the U2000 Server

This example describes how to reasonably plan the hardware configuration for the U2000 server.

Example Description

The number of equivalent NEs of a certain carrier is 9376 (large-scale network). If 80 clients and high availability (Veritas hot standby) protection need to be configured, how should the U2000 be configured in terms of hardware?

Planning Methods

1. The network of the carrier is large. According to the **Management capacities of NMSs based on different hardware platforms**, the configurations applicable to the NMS server on the network of the carrier are as follows.

   Table 5-4 Applicable NMS server hardware

Network Scale	PC Server (Windows OS-Supported)	Sun Server (Solaris OS-Supported)	Blade Server (SUSE Linux OS-Supported)
Large-scale network: 6000-15 000 equivalent NEs	-	Sun M4000 (CPU: 4CPU x 2.53GHz (quatri-core); memory: 32 GB; hard disk: 2 x 146 GB or 2 x 300 GB) + **disk array**	Distributed scenario: blade server x 5 + **disk array** **NOTE** One blade acts as the master server. The other four blades act as the slave servers.

2. The network of the carrier adopts the high availability system (Veritas hot standby). The high availability system (Veritas hot standby) is applicable to the Solaris and SUSE Linux OSs. Therefore, the configurations applicable to the NMS server on the network of the carrier are as follows.

Table 5-5 Applicable NMS server hardware

Network Scale	PC Server (Windows OS-Supported)	Sun Server (Solaris OS-Supported)	Blade Server (SUSE Linux OS-Supported)
Large-scale network: 6000-15000 equivalent NEs	-	Sun M4000 (CPU: 4CPU x 2.53GHz (quatri-core); memory: 32 GB; hard disk: 2 x 146 GB or 2 x 300 GB) + **disk array**	Distributed scenario: blade server x 5 + **disk array** **NOTE** One blade acts as the master server. The other four blades act as the slave servers.

3. The networking and subsequent maintenance in the centralized deployment mode are simpler than those in the distributed deployment mode. Therefore, the recommended configuration is Sun server+disk array.

Table 5-6 Planning result

Network Scale	PC Server (Windows OS-Supported)	Sun Server (Solaris OS-Supported)	Blade Server (SUSE Linux OS-Supported)
Large-scale network: 6000-15000 equivalent NEs	-	Sun M4000 (CPU: 4CPU x 2.53GHz (quatri-core); memory: 32 GB; hard disk: 2 x 146 GB or 2 x 300 GB) + **disk array**	-

5.2 Software Configuration Planning for the U2000 Server

This topic describes which software, including system software and NMS software, can be configured on the U2000 server.

5.2.1 Principles for Software Configuration Planning of the NMS Server
This topic describes the software that can be configured for the NMS server, including system software and NMS software.

5.2.2 Example: Software Configuration Planning for the U2000 Server
This example describes how to reasonably plan the software configurations for the U2000 server.

5.2.1 Principles for Software Configuration Planning of the NMS Server

This topic describes the software that can be configured for the NMS server, including system software and NMS software.

Planning Principles

The software of the NMS server is classified into the following types:

- System software: It includes the operating system software and database software.
- High availability software: It refers to the Veritas software that is applicable to only the high availability system.
- NMS software: It refers to the software developed by Huawei. The NMS software in this document refers to the U2000 software.

When planning the software configurations of the NMS server, observe the following principles:

- Determine the system software to be used according to **Principles for Hardware Configuration Planning of the NMS Server**.
- Determine whether to use the Veritas software according to **NMS Deployment Planning**.
- The NMS software is mandatory.

System Software

The U2000 can run on multiple OSs, including Windows, Solaris, and SUSE Linux. **Table 5-7** lists the configuration standards of the system software.

Table 5-7 System software of the U2000

Item	Software Platform	Software Type	Version	Supported OS Language
Delivered software platform	x86 (Windows 32bit)	OS	Windows Server 2003R2 Enterprise + SP2	Chinese English
		Database	MSSQLServer 2000 Standard + SP4	
	SPARC (Solaris 64bit)	OS	Solaris 10 (10/08) + Huawei Patch 9.0.1	
		Database	SYBASE 15.0.3 with EBF16476 + EBF16548	
	x86 (Linux 64bit)	OS	SUSE Linux 10 SP3	
		Database	Oracle 11g Enterprise Edition Release 11.1.0.7	

Item	Software Platform	Software Type	Version	Supported OS Language
Compatible software platform	x86 Windows (32bit)	OS	Windows Server 2003 Standard	
		Database	SQL Server 2000 Standard	
	SPARC (Solaris 64bit)	OS	Solaris 10	
		Database	SYBASE 12.5	
Software platform no longer supported	x86 Windows (32bit)	OS	Windows 2000 Server	
		Database	MS SQL Server 7.0 or SQL Server 2000	
	SPARC (Solaris 32bit)	OS	Solaris 8	
		Database	SYBASE 12.0	

High Availability Software

The high availability system of the U2000 can be deployed on the Windows, Solaris, and SUSE Linux OSs with the high availability software being Veritas. **Table 5-8** shows the Veritas software versions in each platform.

Table 5-8 High availability software

Platform	High Availability Software
Solaris	● Delivered configurations: Veritas 5.1 ● Compatible configurations: Veritas 5.0MP3+RP2 and Veritas 4.1 ● Configurations no longer supported: Veritas 4.0 and earlier versions + Watchman scheme
SUSE Linux	Delivered configurations: Veritas 5.1
Windows	Delivered configurations: Veritas 5.1

Software Configurations of the U2000

The NMS software, namely, the U2000 server software, can be installed through the installation DVD or the installation package.

Configuration Item	Typical Configuration
U2000 software	Installation DVD or installation software package **NOTE** If you install the server software through the software package, prepare a proper software package according to the components to be installed.

5.2.2 Example: Software Configuration Planning for the U2000 Server

This example describes how to reasonably plan the software configurations for the U2000 server.

Example Description

The NMS on the network of a carrier adopts the high availability system (Veritas hot standby). How should the software configuration for the NMS server be planned on the network?

Planning Method

1. According to **5.1.2 Example: Hardware Configuration Planning for the U2000 Server**, the Sun server can be used as the NMS server on the network of the carrier.

   Table 5-9 Planning result

Network Scale	PC Server (Windows OS-Supported)	Sun Server (Solaris OS-Supported)	Blade Server (SUSE Linux OS-Supported)
Large-scale network: 6000-15000 equivalent NEs	-	Sun M4000 (CPU: 4CPU x 2.53GHz (quatri-core); memory: 32 GB; hard disk: 2 x 146 GB or 2 x 300 GB) + **disk array**	-

2. According to the OS supported by the hardware and the deployment of the network where the high availability system (Veritas hot standby) is adopted, the planning results of the software configurations are as follows.

Table 5-10 Planning results of the software configurations

No.	Software Type	Software Version
1	System software	1. OS software: Solaris 10 (10/08) + Huawei Patch 9.0.1 2. Database software: SYBASE 15.0.3 with EBF16476 + EBF16548
2	high availability software	Veritas 5.1
3	NMS software	U2000 installation DVD or installation software package

5.3 Client Configuration Planning

This topic describes the requirements on software and hardware configuration when the U2000 client runs on the Windows and Solaris OSs.

Software and Hardware Configuration

The U2000 client can be installed in the Windows OS and Solaris OSs instead of the SUSE Linux OS. **Table 5-11** shows the hardware configuration and software configuration.

Table 5-11 Hardware configuration and software configuration of the U2000 client

Platform	Hardware Configuration	Software Configuration
Windows	● Recommended configuration: Intel E5200 (dual-core) (2.5 GHz or greater); memory (2 GB or greater) ● Lowest configuration: Intel E2140 (dual-core) (1.6 GHz or greater); memory (2 GB or greater)	**Recommended OS:** ● Windows XP Professional **Compatible OS:** ● Windows XP Professional ● Windows Vista Business with SP1 ● Windows 7 Professional (64-bit version)
Solaris	SUN T5220 (CPU: quadri-core)(1.2 GHz or greater); memory (8 GB); hard disk (4 x 146 GB)	Solaris 10 (10/08) with Huawei Patch 9.0.1

NOTE

It is recommended that the U2000 client be installed on the Windows platform.

Specifications of Citrix Server and Client

The Citrix access solution includes the Citrix server and the Citrix client. The applications run on the Citrix server; the Citrix client only provides the operation interface for the applications and displays the operation results of the applications.

The Citrix client communicates with the Citrix server through the independent computing architecture (ICA) software. During the running of the applications, only the information such as refreshing the screen, pressing the keyboard, and dragging the mouse is communicated between the Citrix server and the client.

In the Citrix client access solution for the U2000, the Citrix server is deployed in the U2000 server network. To implement the O&M on the network, you can operates the U2000 client that runs on the Citrix server by using the Citrix client.

By using the Citrix client access solution, you only need to install the Citrix client software on the terminal, which means that the solution is much less demanding on the terminal.At the same time, the bandwidth required between the Citrix server and the Citrix client can be very small. Therefore, you can choose the access device and the network flexibly.

In the U2000 Citrix access scheme, it is recommended that the PC servers in **Table 5-12** be used.

Table 5-12 Configurations of the Citrix server and client

Server Model	Maximum Number of Client
HP DL380G6 (memory: 8 GB)	24
HP DL580G5 (memory: 16 GB)	40

5.4 Planning of the Server Running Environment

The planning for the server running environment involves the planning of the rack and telecommunications room.

5.4.1 Cabinet Planning

The U2000 server can be deployed independently or placed in a cabinet. This topic describes the planning when the U2000 server is placed in a cabinet.

Overview

The U2000 server can be placed in an N610E or N68E-22 cabinet. **Table 5-13** describes the type and dimensions of the cabinets.

Table 5-13 Cabinet description

Cabinet Type	Dimension	Use Instructions
N610E	600 mm (W) x 1000 mm (D) x 2200 mm (H)	This cabinet is applicable to the M4000, T5220, IBM BladeCenter E, HP DL380G6, and HP DL580G5 servers.

Cabinet Type	Dimension	Use Instructions
N68E-22	600 mm (W) x 800 mm (D) x 2200 mm (H)	This cabinet is applicable to the ATAE-T8223 server.

Specifications of Components in the Cabinet

Table 5-14 lists the specifications of components in the cabinet.

NOTE

1 U = 44.45 mm

Table 5-14 Cabinet overview

Component	High (U)	Power Consumption (W)
M4000	6	2100
T5220	2	750
IBM BladeCenter E	7	● Shelf: 400 ● Mother board: 250 ● Backplane: 200
ATAE	14	2400
HP DL380G6	2	1000
HP DL580G5	4	1200
S2600	2	1000
Quidway S2016	1	30
KVM	1	50

Cabinet Quantity Planning

Refer to Table 5-15 to plan the cabinet quantity.

Table 5-15 Cabinet configurations

Cabinet Type	Single-cabinet Configurations
N610E	2 M4000s + 2 disk arrays + 1 KVM + 3 switches
	2 T5520s + 1 KVM + 2 switches
	1 IBM BladeCenter E + 3 disk arrays + 1 switch
	4 HP DL380G6s + 1 KVM + 2 switches

Cabinet Type	Single-cabinet Configurations
	4 HP DL580G5s + 1 KVM + 2 switches
N68E-22	1 ATAE + 1 disk array + 1 KVM + 2 switches

NOTE

The cabinet configurations are verified strictly and meet the requirements of power consumption and heat dissipation. It is recommended that you do not change the cabinet configurations randomly. For example, if 1 M4000, 2 T5220s, 3 HP DL380G6s, and 1 DL580G5 are configured at a site, how to plan the cabinets?

- According to **Table 5-15**, the correct planning is to plane 1 N610E cabinet for 1 M4000, 1 N610E cabinet for 2 T5220s, 1 N610E cabinet for 3 HP DL380G6s, and 1 N610E cabinet for 1 HP DL580G5. That is, totally 4 N610E cabinets are needed.
- An incorrect planning is to plane 1 N610E cabinet for 1 M4000, 1 N610E cabinet for 2 T5220s, and 1 N610E cabinet for 3 HP DL380G6s and 1 HP DL580G5. That is, totally 3 N610E cabinets are planned.

5.4.2 Telecommunications Room

This topic describes the planning of the environment and power in the telecommunications room.

Environment Requirements

Table 5-16 lists the requirements on temperature, humidity, air pressure, and floor load in the telecommunications room.

Table 5-16 Temperature, humidity, and air pressure

Environment Parameter	Value
Temperature	Long-term working condition: 15°C to 30°C Short-term working condition: 0°C to 45°C
Relative humidity	Long-term working condition: 40% to 65% Short-term working condition: 20% to 90%
Air pressure	70 kPa to 106 kPa
Floor load	No less than 450 kg/m²

Air Cleanness Requirements

Table 5-17 lists the air cleanness requirements.

Table 5-17 Air cleanness requirements

Mechanical Active Substance	Unit	Content
Dust particle	Particle/m³	≤ 3 x 104 (no visible dust accumulated on the workbench in three days)

NOTE

The diameter of dust particle is equal to or greater than 5 μm.

Power Supply Requirements

This topic describes the requirements on AC power supply, DC power supply, and grounding in the telecommunications room.

Table 5-18 Power Supply Requirements

Power Supply	Requirements
Requirements on AC Power Supply	The AC power supply in the telecommunications room consists of two mains, a UPS, and a generator set. The voltage of the AC power supply ranges from 93 V to 121 V or from 188 V to 265 V.
Requirements on DC Power Supply	The DC power supply in the telecommunications room requires two DC power inputs and two DC batteries for backup. The voltage of the DC power supply ranges from -40.5 V to -57 V.
Requirements on Grounding	● The resistance of the grounding cable must be less than 10 ohms. It is recommended that the resistance of the total grounding bar be less than 1 ohm. ● The distance between the equipment and the grounding bar in the telecommunications room should be no more than 30 meters. The shorter the better. If the distance between the equipment and the grounding bar in the telecommunications room exceeds 30 meters, the grounding bar should be reconfigured. ● The resistance between the rack and the ground should be greater than five megohms.

Electromagnetic Environment

The electromagnet environment requirements in the telecommunications room are as follows:

- Industrial frequency magnetic field: 50 Hz, ≤ 10 A/m
- Radio frequency electromagnetic field: 0.009-2000 MHz, ≤ 3 V/m

6 Network Parameter Planning for the NM Server

About This Chapter

The network parameters of the NMS server include IP address, port number and bandwidth. The settings of the network parameters determine the network connectivity, reliability, and performance of the NMS server. This topic details the principles of the network parameter planning.

6.1 Host Name Planning
Generally, the host name of the U2000 server should be easy to remember and recognize.

6.2 NTP Service Planning
This topic describes the purpose of and principles for NTP service planning.

6.3 IP Address Planning
IP addresses must be planned according to the server deployment scheme and the number of NICs.

6.4 Planning of the Hard Disk Redundancy Backup
To ensure the security of system data, the U2000 supports the hard disk redundancy backup function. This topic describes the planning relevant to this function.

6.5 Route Planning
Routes need to be planned based on the current network during the server deployment. This helps to ping through the IP addresses of all the NEs and remote clients on the U2000 server.

6.6 U2000 Port List
This topic describes the service ports used by the U2000.

6.7 Bandwidth Planning
The U2000 uses the standard client/server (C/S) architecture. The clients and the servers communicate with each other through the local area network (LAN) or the wide area network (WAN). The U2000 server communicates with NEs in the outband or inband mode, which has a certain requirement on bandwidth.

6.8 Planning Reference for Performance Database Size

Performance data expands as time goes by. Therefore, you need to properly plan the database size.

6.1 Host Name Planning

Generally, the host name of the U2000 server should be easy to remember and recognize.

Host Name Planning Rules and Restrictions

When planning the host name of the U2000 server, observe the following principles:

- The host name of the U2000 server must be unique on the network.
- The host name must be a string consisting of no more than 24 characters that can only be letters (A to Z), digits (0 to 9) and hyphen (-).
- The first character must be a letter and the last character cannot be a hyphen.
- The host name must be case-sensitive.
- The host name cannot contain any space.
- The host name cannot contain only one character.
- The host name cannot contain **--**.
- The host name cannot be any of the following keywords in the high availability system.

```
action  false  keylist  static  after  firm  local  stop    requires
remotecluster
system  group  resource global  Start  str   temp   set     heartbeat
ArgListValues
System  Group  boolean  hard    Name   soft  before online  condition
MonitorOnly
remote  start  cluster  event   VCShm  type  Path   offline Signaled
HostMonitor
Probed  state  Cluster  IState  int    Type  State  VCShmg   NameRule
ConfidenceLevel
```

NOTE

The host name of the U2000 server must meet the customer habits. It is recommended that you ask customers to provide host names during the planning.

Examples for Planning Host Names

Plan the host names of NMS servers according to **Planning of the U2000 Deployment Scheme**.

Table 6-1 Examples for planning the host names of NMS servers

NMS Deployment Scheme	Example
centralized single-server system	NMSserver
distributed single-server system	● Master Server: Masterserver ● Slave Server: SlaveserverN
centralized high availability system	● Primary Site: Primaster ● Secondary Site: Secmaster

NMS Deployment Scheme	Example
distributed high availability system	● Master server of the primary site: Primaster ● Slave server of the primary site: PrislaveN ● Master server of the secondary site: Secmaster ● Slave server of the secondary site: SecslaveN

NOTE

- The preceding host names are only examples. Plan the host names according to the actual situation and customer habits.
- The letter N in the preceding table represents the serial number of the Slave Server. The host names of the Slave Servers can be increased in sequence along with the increase of the number of Slave Servers. For example, the host names can be Prislave1, Prislave2, and Prislave3.

6.2 NTP Service Planning

This topic describes the purpose of and principles for NTP service planning.

Purpose of NTP Service Planning

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.

Time incorrectness causes the following problems:

- The sequence of alarm generation, the actual alarm duration, and the association between alarms cannot be determined according to the alarm information.
- When performance data is recorded and collected, the precision of statistics collection is directly affected.

Therefore, a non-manual-intervened method is required for precisely adjusting the time of the U2000 and NEs at any time to keep the time consistency.

Planning Principles for the NTP Service

When planning the NTP service, observe the following principles:

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.

- If a standard external clock source is available, it is recommended that you configure the NMS server as an NTP client to trace the standard clock source.
- If no external clock source is available, plan the NTP service according to **NMS Deployment Planning**. The recommended schemes are as follows.

Table 6-2 Recommended schemes for NTP service planning

NMS Deployment Scheme	Recommended Scheme
centralized single-server system	● Configuring the U2000 server as the NTP server of the highest stratum. ● Configuring U2000 clients and NEs as NTP clients to trace the clock of the U2000 server.
distributed single-server system	● Configuring the Master Server as the NTP server of the highest stratum. ● Configuring the Slave Server, U2000 clients, and NEs as NTP clients to trace the clock of the Master Server.
centralized high availability system	● Configuring the Primary Site server as the NTP server of the highest stratum. ● Configuring the Secondary Site server, U2000 clients, and NEs as NTP clients to trace the clock of the Primary Site server.
distributed high availability system	● Configuring the master server of the primary site as the NTP server of the highest stratum. ● Configuring the slave server of the primary site as the NTP clients to trace the clock of the master server of the primary site. ● Configuring the master server of the secondary site as the NTP server of the medium stratum to trace the clock of the master server of the primary site. ● Configuring the slave server of the secondary site as NTP clients to trace the clock of the master server of the secondary site. ● Configuring U2000 clients and NEs as NTP clients to trace the clock of the master server of the primary site.

6.3 IP Address Planning

IP addresses must be planned according to the server deployment scheme and the number of NICs.

This topic describes the IP address planning of the centralized single-server system scheme. The centralized single-server system scheme is applicable to Windows and Solaris OSs.

6.3.3 IP Address Planning of the Centralized High Availability System
This topic describes the IP address planning of the centralized high availability system scheme. The centralized high availability system scheme is applicable to the Windows and Solaris OSs.

6.3.4 IP Address Planning of a Distributed Single-Server System
This topic describes the IP address planning of the distributed single-server system scheme. The distributed single-server system scheme is applicable to the SUSE Linux OS.

6.3.5 IP Address Planning of the Distributed High Availability System
This topic describes the IP address planning of the distributed high availability system. The distributed high availability system scheme is applicable to the SUSE Linux OS. This topic describes the IP address planning of the distributed high availability system scheme, which includes the planning of the IP addresses of the Master Server and Slave Server.

6.3.1 General Principles for IP Address Planning

When planning the IP addresses of U2000 servers, observe the following principles.

Planning Principles for IP Addresses

- The IP addresses must be unique on the network.
- The servers communicate with the managed equipment in the normal state.
- The U2000 servers communicate with U2000 clients in the normal state.
- You can plan only one IP address for one network interface. It is not allowed to plan or set multiple IP addresses for the same network interface.
- You need to plan the equipment control IP address according to the selected NMS server hardware.
- You need to plan the NMS IP address according to the deployment scheme of the NMS.

6.3.2 IP Address Planning of the Centralized Single-Server System

This topic describes the IP address planning of the centralized single-server system scheme. The centralized single-server system scheme is applicable to Windows and Solaris OSs.

IP Address Planning of Centralized Single-Server System (Windows)

centralized single-server systemIf the centralized single-server system is installed in the Windows OS, you need to plan the system IP address before installing the NMS. The system IP address is used to:

- Configure and manage OSs.
- Provide external NMS services, such as the communication between the NMS server and the clients or NEs.

centralized single-server system**Table 6-3** shows an example of IP address planning for the centralized single-server system (Windows).

Table 6-3 Example of IP address planning for the centralized single-server system (Windows)

Item	Example
System IP address	● IP address: 129.9.1.1/255.255.255.0 ● Gateway: 129.9.1.254

IP Address Planning of Centralized Single-Server System (Solaris)

centralized single-server system: If the centralized single-server system is installed in the Solaris OS, you need to plan the following types of IP addresses:

- IP address of the workstation controller: This type of IP address is used to remotely log in to a workstation to manage and maintain workstation hardware. For example, you can use it to remotely install the OS or log in to a workstation to perform operation and maintenance if the OS fails to start properly.
- IP address of the disk array controller: This type of IP address is used to remotely manage and maintain equipment.
- System IP address: This type of IP address is used to log in to a server to manage and maintain the OS. It is the IP address of the OS.
- NMS application IP address: This type of IP address is used to provide external NMS services, such as the communication between the NMS server and the clients or NEs.

centralized single-server systemTwo IP address planning schemes are available for the centralized single-server system (Solaris), namely, single-NIC scheme and double-NIC scheme.

- Single-NIC scheme (**recommended**): Only one NIC is required. The system IP address is used as the NMS application IP address. That is, the system IP address has the functions of the NMS application IP address. **Table 6-4** shows an example of IP address planning of the single-NIC scheme.

Table 6-4 Example of IP address planning of the single-NIC scheme

Item	Example (IP Address/ Subnet Mask/Gateway)	Description
IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
	M4000 workstation: ● Primary controller: 129.9.1.21/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.21/255.255.255.0/129.9.2.254	

Item	Example (IP Address/ Subnet Mask/Gateway)	Description
IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.10/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.11/255.255.255.0/129.9.2.254	-
System IP address	● 129.9.1.1/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-

- Double-NIC scheme: Two NICs are required. You need to plan the NMS application IP address and system IP address separately. **Table 6-5** shows an example of IP address planning of the double-NIC scheme.

CAUTION

The system IP addresses and NMS application IP address cannot be on the same network segment.

Table 6-5 Example of IP address planning of the double-NIC scheme

Item	Example (IP Address/ Subnet Mask/Gateway)	Description
IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
	M4000 workstation: ● Primary controller: 129.9.1.21/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.21/255.255.255.0/129.9.2.254	
IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.10/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.11/255.255.255.0/129.9.2.254	-

Item	Example (IP Address/ Subnet Mask/Gateway)	Description
System IP address	● 129.9.1.1/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-
NMS application IP address	● 129.9.1.2/255.255.255.0/129.9.1.254 ● Used NIC: e1000g1	-

6.3.3 IP Address Planning of the Centralized High Availability System

This topic describes the IP address planning of the centralized high availability system scheme. The centralized high availability system scheme is applicable to the Windows and Solaris OSs.

6.3.3.1 IP Address Planning of the HA System (Solaris)
This topic describes the IP address planning of the high availability (HA) system (Solaris).

6.3.3.2 IP Address Planning of the High Availability System (Windows)
This topic describes the IP address planning of the high availability system (Windows).

6.3.3.1 IP Address Planning of the HA System (Solaris)

This topic describes the IP address planning of the high availability (HA) system (Solaris).

You need to plan the following types of IP addresses:

- IP address of the workstation controller: This type of IP address is used to remotely log in to a workstation to manage and maintain workstation hardware. For example, you can use it to remotely install the OS or log in to a workstation to perform operation and maintenance if the OS fails to start properly.
- IP address of the disk array controller: This type of IP address is used to remotely manage and maintain equipment.
- System IP address: This type of IP address is used to log in to a server to manage and maintain the OS. It is the IP address of the OS.
- IP address of the heartbeat network service: This type of IP address is used to detect status of the network connection between the primary and secondary sites.
- IP address of the replication network service: This type of IP address is used to replicate data between Primary and secondary sites.
- NMS application IP address: This type of IP address is used to provide external NMS services, such as the communication between the NMS server and the clients or NEs.

NOTE

- During the network planning, the heartbeat network, replication network, and NMS application network can be planed separately or in reuse mode. Planning the heartbeat network, replication network, and NMS application network separately is not recommended.
- The heartbeat network, replication network, and NMS application network can be configured with network protection, that is, IPMP. It is not recommended that IPMP be configured.
- IPMP is short for IP network multipathing. In this mode, two NICs work in 1+1 backup mode. During configuration, an IP address is assigned to each of the NICs and a floating IP address is also set. When the active NIC is faulty, services can be switched to the standby NIC. Configuring IPMP requires two NICs and three IP addresses, and the three IP addresses must be on the same network segment.

According to the number of required NICs, function types of configured IP addresses, and whether IPMP is configured, multiple IP address planning schemes are available for the HA system (Solaris). The typical IP address planning schemes are as follows.

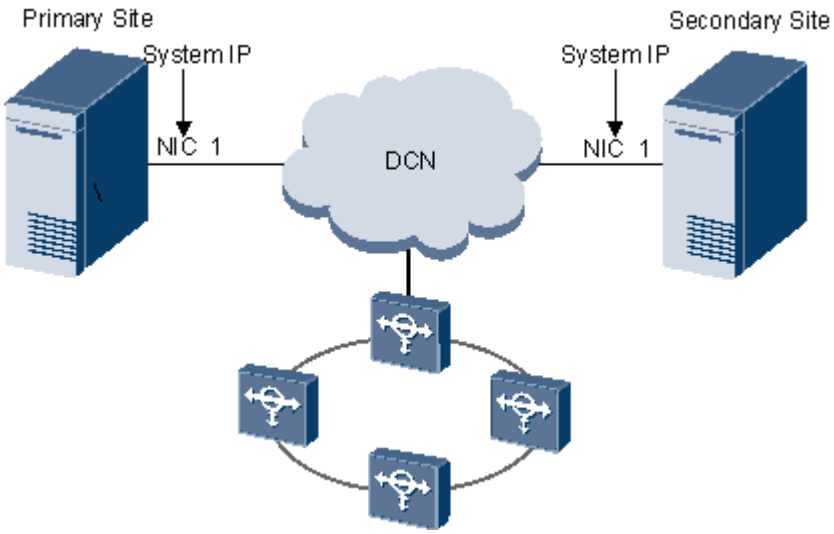
NOTE

In the HA system, the primary and secondary sites can be deployed either in the same place (local deployment) or in different cities (remote deployment). The following uses local deployment as an example to describe IP address planning. If remote deployment is required, ensure that routes between the primary and secondary sites are reachable.

Single-NIC Scheme (Recommended)

Single-NIC scheme: Only one NIC is required. **Figure 6-1** shows the networking diagram. The single-NIC scheme is recommended.

Figure 6-1 Networking example (single-NIC scheme)



IP planning description: Only the System IP address needs to be planned. Heartbeat detection, data replication, and external NMS services between primary and secondary sites are all implemented through NIC 1.

- Advantage: The networking is simple and IP addresses can be saved.
- Disadvantage: All data is transmitted over one link and faults cannot be isolated.

IP planning example: Table 6-6 shows the planning example.

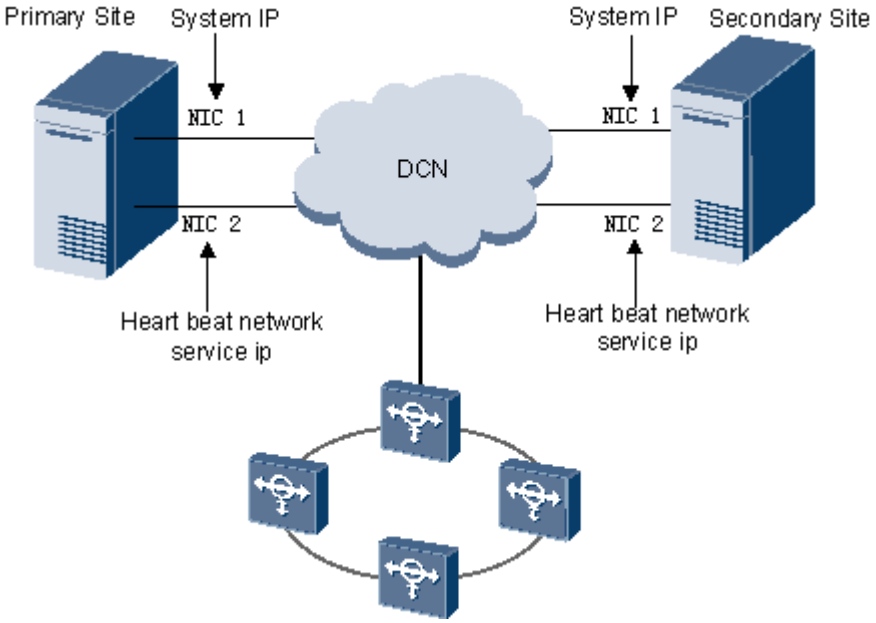
Table 6-6 Example of IP address planning of the single-NIC scheme

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
Primary site	IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254 M4000 workstation: ● Primary controller: 129.9.1.21/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.21/255.255.255.0/129.9.2.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.22/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.23/255.255.255.0/129.9.2.254	-
	System IP address	● 129.9.1.1/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-
Secondary site	IP address of the workstation controller	T5220 workstation: 129.9.1.24/255.255.255.0/129.9.1.254 M4000 workstation: ● Primary controller: 129.9.1.25/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.25/255.255.255.0/129.9.2.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.26/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.27/255.255.255.0/129.9.2.254	-
	System IP address	● 129.9.1.2/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-

Double-NIC Scheme (Without IPMP)

Double-NIC scheme (without IPMP): Two NICs are required. **Figure 6-2** shows the networking diagram.

Figure 6-2 Networking example (double-NIC scheme (without IPMP))



IP planning description: Only the System IP address and IP address of the heartbeat network service need to be planned.

- OS management and NMS application are implemented through NIC 1.
- Heartbeat services and data replication services between primary and secondary sites are implemented through NIC 2.

CAUTION

IP addresses of NIC 1 and NIC 2 must be on different network segments.

- Advantage: NMS management and HA system application are implemented through different routes, and thus faults can be isolated.
- Disadvantage: Configurations are complex.

IP planning example: Table 6-7 shows the planning example.

Table 6-7 Example of IP address planning of the double-NIC scheme (without IPMP)

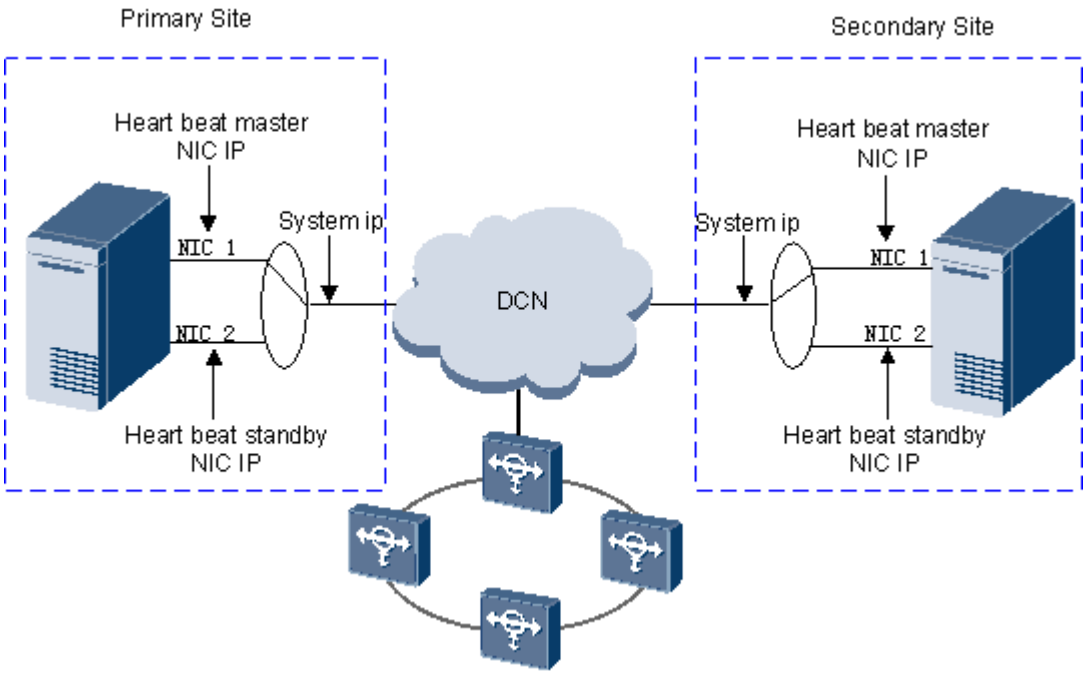
Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
Primary site	IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: ● Primary controller: 129.9.1.21/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.21/255.255.255.0/129.9.2.254	
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.22/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.23/255.255.255.0/129.9.2.254	-
	System IP address	● 129.9.1.1/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-
	IP address of the heartbeat network service	● 129.9.2.3/255.255.255.0/129.9.2.254 ● Used NIC: e1000g1	-
Secondary site	IP address of the workstation controller	T5220 workstation: 129.9.1.24/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: ● Primary controller: 129.9.1.25/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.25/255.255.255.0/129.9.2.254	

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.26/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.27/255.255.255.0/129.9.2.254	-
	System IP address	● 129.9.1.2/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-
	IP address of the heartbeat network service	● 129.9.2.4/255.255.255.0/129.9.2.254 ● Used NIC: e1000g1	-

Double-NIC Scheme (with IPMP)

Double-NIC scheme (with IPMP): Two NICs are required. **Figure 6-3** shows the networking diagram.

Figure 6-3 Networking example (double-NIC scheme (with IPMP))



IP planning description:

- NIC 1 and NIC 2 work in 1+1 backup mode. The System IP address, IP address of the active heartbeat NIC, and IP address of the standby heartbeat NIC need to be planned.
- If the NICs are running properly, the System IP address maps to the IP address of the active heartbeat NIC. Heartbeat detection, data replication, and external NMS services between primary and secondary sites are all implemented through the System IP address. If the active NIC is faulty, the System IP address automatically maps to the IP address of the standby heartbeat NIC. Heartbeat detection, data replication, and external NMS services between primary and secondary sites are still implemented through the System IP address, thereby implementing NIC protection.

CAUTION

The System IP address, IP address of the active heartbeat NIC, and IP address of the standby heartbeat NIC must be on the same network segment.

- Advantage: The NICs work in 1+1 backup mode and network security is high.
- Disadvantage: The networking is complicated and many IP addresses are required. Future maintenance is complex and switch performance must be high.

IP planning example: Table 6-8 shows the planning example.

Table 6-8 Example of IP address planning of the two-NIC scheme (with IPMP)

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
Primary site	IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254	• Plan the IP address according to the model of the selected workstation. • The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: • Primary controller: 129.9.1.21/255.255.255.0/129.9.1.254 • Secondary controller: 129.9.2.21/255.255.255.0/129.9.2.254	
	IP address of the disk array controller	OceanStor S2600: • Primary controller: 129.9.1.22/255.255.255.0/129.9.1.254 • Secondary controller: 129.9.1.23/255.255.255.0/129.9.2.254	-
	System IP address	129.9.1.1/255.255.255.0/129.9.1.254	-

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
	IP address of the active heartbeat NIC	● 129.9.1.2/255.255.255.0 /129.9.2.254 ● Used NIC: e1000g0	-
	IP address of the standby heartbeat NIC	● 129.9.1.3/255.255.255.0 /129.9.3.254 ● Used NIC: e1000g1	-
Secondary site	IP address of the workstation controller	T5220 workstation: 129.9.1.24/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: ● Primary controller: 129.9.1.25/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.25/255.255.255.0/129.9.2.254	
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.26/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.27/255.255.255.0/129.9.2.254	-
	System IP address	129.9.1.4/255.255.255.0/129.9.1.254	-
	IP address of the active heartbeat NIC	● 129.9.1.5/255.255.255.0 /129.9.2.254 ● Used NIC: e1000g0	-
	IP address of the standby heartbeat NIC	● 129.9.1.6/255.255.255.0 /129.9.3.254 ● Used NIC: e1000g1	-

Other Schemes

Contact Huawei engineers for scheme design.

6.3.3.2 IP Address Planning of the High Availability System (Windows)

This topic describes the IP address planning of the high availability system (Windows).

The following table shows an example of IP address planning for the high availability system (Windows).

Table 6-9 IP address planning of the single-networking-interface scheme

Site	Equipment Description	IP Planning	Sample IP Address/Subnet Mask
Primary site	System IP address	It is set during the OS installation. It is used for client and NE communication (optional and recommended) for heartbeat detection and data replication.	129.9.1.1/255.255.255.0
	Virtual IP address	It is used for client and NE communication (optional and not recommended; the virtual IP address is easy to be occupied, or the communication will fail if the virtual IP address is not enabled due to VCS abnormality). It is used to check NICs.	129.9.1.2/255.255.255.0
Secondary site	System IP address	It is set during the OS installation. It is used for client and NE communication (optional and recommended) for heartbeat detection and data replication.	129.9.1.3/255.255.255.0
	Virtual IP address	It is used for client and NE communication (optional and not recommended; the virtual IP address is easy to be occupied, or the communication will fail if the virtual IP address is not enabled due to VCS abnormality). It is used to check NICs.	129.9.1.4/255.255.255.0

6.3.4 IP Address Planning of a Distributed Single-Server System

This topic describes the IP address planning of the distributed single-server system scheme. The distributed single-server system scheme is applicable to the SUSE Linux OS.

distributed single-server systemYou need to plan the following IP addresses:

- IP address of the server management network interface: This type of IP address is used to manage and maintain blade servers.
- IP address of the disk array controller: This type of IP address is used to remotely manage and maintain equipment.
- System IP address: This type of IP address is used to provide external NMS services, such as the communication between the NMS server and the clients or NEs.

distributed single-server system**Table 6-10** shows an example of IP address planning.

Table 6-10 Example of IP address planning

Item	Example (IP Address/Subnet Mask/Gateway)	Description
IP address of the server management network interface	IP address of the NIC on the SMM card of ATAE server: 129.9.1.20/255.255.255.0/129.9.1.254	Plan the IP address according to the model of the selected blade server.
	IP address of the management module of IBM Blade center E: 129.9.1.20/255.255.255.0/129.9.1.254	
IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.10/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.11/255.255.255.0/129.9.2.254	-
System IP address	System IP address of the Master Server: ● 129.9.1.1/255.255.255.0/129.9.1.254 ● Used NIC: eth0	-
	System IP address of the SlaveServer: ● 129.9.1.2/255.255.255.0/129.9.1.254 ● Used NIC: eth0	If there are multiple Slave Servers, you need to plan the system IP address for each Slave Server.

6.3.5 IP Address Planning of the Distributed High Availability System

This topic describes the IP address planning of the distributed high availability system. The distributed high availability system scheme is applicable to the SUSE Linux OS. This topic describes the IP address planning of the distributed high availability system scheme, which includes the planning of the IP addresses of the Master Server and Slave Server.

distributed high availability systemYou need to plan the following IP addresses:

- IP address of the server management network interface: This type of IP address is used to manage and maintain blade servers.
- IP address of the disk array controller: This type of IP address is used to remotely manage and maintain equipment.
- System IP address: This type of IP address is used to provide external NMS services, such as the communication between the NMS server and the clients or NEs.

distributed high availability system**Table 6-11** shows an example of IP address planning.

Table 6-11 Example of IP address planning

Site	Item	Example (IP Address/Subnet Mask/Gateway)	Description
Primary site	IP address of the server management network interface	IP address of the NIC on the SMM card of ATAE server: 129.9.1.20/255.255.255.0/129.9.1.254	Plan the IP address according to the model of the selected blade server.
		IP address of the management module of IBM Blade center E: 129.9.1.20/255.255.255.0/129.9.1.254	
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.10/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.11/255.255.255.0/129.9.2.254	-
	System IP address	System IP address of the Master Server: ● 129.9.1.1/255.255.255.0/129.9.1.254 ● Used NIC: eth0	-
		System IP address of the SlaveServer: ● 129.9.1.2/255.255.255.0/129.9.1.254 ● Used NIC: eth0	If there are multiple Slave Servers, you need to plan the system IP address for each Slave Server.
Secondary site	IP address of the server management network interface	IP address of the NIC on the SMM card of ATAE server: 129.9.1.21/255.255.255.0/129.9.1.254	Plan the IP address according to the model of the selected blade server.

Site	Item	Example (IP Address/Subnet Mask/Gateway)	Description
		IP address of the management module of IBM Blade center E: 129.9.1.21/255.255.255.0/129.9.1.254	
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.12/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.13/255.255.255.0/129.9.2.254	-
	System IP address	System IP address of the Master Server: ● 129.9.1.3/255.255.255.0/129.9.1.254 ● Used NIC: eth0	-
		System IP address of the SlaveServer: ● 129.9.1.4/255.255.255.0/129.9.1.254 ● Used NIC: eth0	If there are multiple Slave Servers, you need to plan the system IP address for each Slave Server.

6.4 Planning of the Hard Disk Redundancy Backup

To ensure the security of system data, the U2000 supports the hard disk redundancy backup function. This topic describes the planning relevant to this function.

RAID Technology

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 5: RAID uses more than three hard disks for disk mirroring. Each hard disk has a block for storing the verification information of other hard disks. In the case of a fault repairing, you need to restore data by computing the verification code. RAID 5 distributes verification blocks to all data disks. This ensures that all access and write operations performed on the verification blocks are balanced among all RAID disks and thus prevents low system efficiency during the access and write operations on the verification blocks. RAID 5 requires at least three hard disks.

Principles of Planning the Hard Disk Redundancy Backup

With reference to **Table 6-12**, plan the hard disk redundancy backup According the server hardware and the number of hard disks in the U2000 server.

Table 6-12 Recommended RAID level

Server Hardware	Configuration Principle
HP PC server	● RAID 1 is recommended for two hard disks. ● RAID 10 is recommended for four hard disks. Specifically, configure RAID 0 by using two hard disks and then configure RAID 1 by using the two RAID 0 hard disk groups. ● The RAID 10 and hot spare disk are is 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.
Sun T5220/Sun M4000	● RAID 1 is recommended for two hard disks. ● Two RAID 1 groups are recommended for four hard disks.
Blade server	RAID 1 is recommended for a blade server where only two hard disks are configured.
Disk array	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.

6.5 Route Planning

Routes need to be planned based on the current network during the server deployment. This helps to ping through the IP addresses of all the NEs and remote clients on the U2000 server.

Choose the U2000 server, U2000 client, and routing policy based on the current network of carriers. It is recommended that you use the default route on the U2000. In this manner, the default router can implement the routing to the network segment where the NEs and remote clients are located and also the reverse routing. Finally, you can ping through the IP addresses of all the NEs and remote clients on the U2000 server.

6.6 U2000 Port List

This topic describes the service ports used by the U2000.

6.6.1 U2000 Service Port Overview

This topic describes the U2000, service ports to be filtered and the method to query service ports.

Overview of U2000 service ports

In the security policy of the firewall, you must filter the traffic according to the IP address and the Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) port number.

The TCP/UDP port number is used to split a datagram, and transfer the datagram to the proper applications.

The TCP/UDP port range is 0~65535, which is divided into three segments:

- 0~1023: Identifies some standard services, such as FTP, Telnet, and Trivial File Transfer Protocol (TFTP).
- 1024~49151: Assigned by Internet Assigned Number Authority (IANA) to the registered applications.
- 32768~65535: Private port numbers, which are dynamically assigned to any applications.

U2000 service ports are classified into the following types:

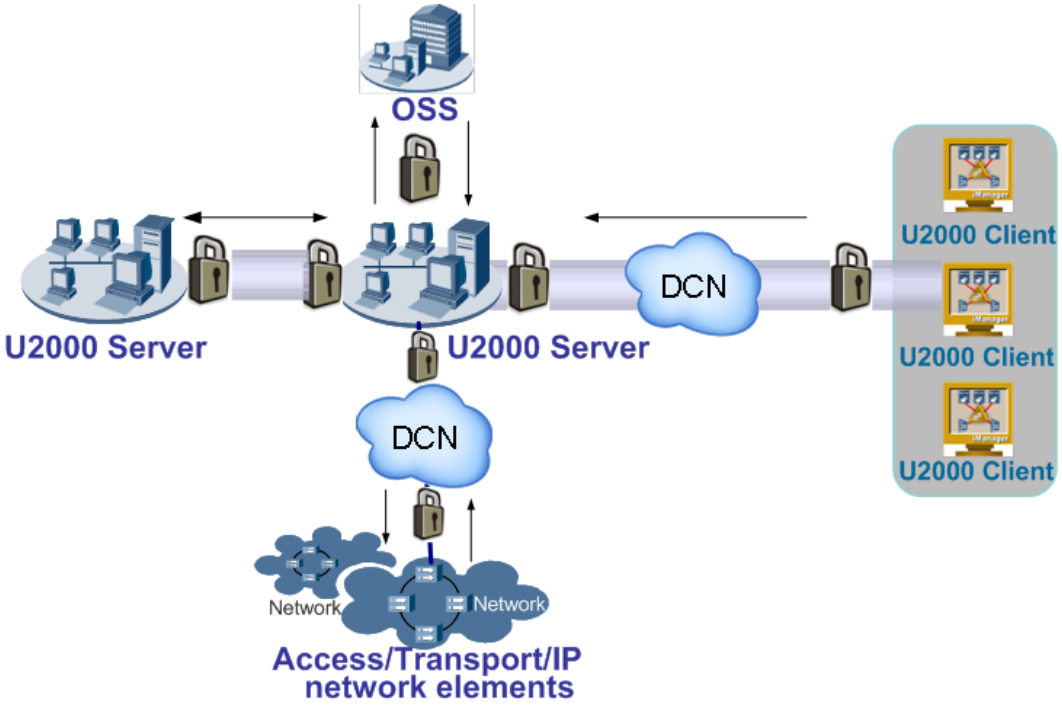
- Ports on the U2000 server for connecting the OSS
- Ports on the OSS for Connecting the U2000 Server
- Ports on the U2000 server for connecting clients
- Ports on the U2000 server for connecting NEs
- Ports on NEs for connecting the U2000 server
- Ports on primary and secondary sites of the Veritas HA system
- Ports for internal processes of the U2000 server

- Ports for other connections
- Ports for remote maintenance

Diagram of U2000 service ports

The diagram of U2000 service ports shows the relationships between the U2000 server and peripherals, and the position and direction of firewalls.

Figure 6-4 Relationship between the U2000 server and peripherals



Method to query service ports

The method to query service ports is as follows:

- Solaris OS

  ```
  # /usr/bin/netstat -an -P tcp
  ```

  Information similar to the following is displayed:

  ```
  TCP: IPv4
     Local Address        Remote Address    Swind Send-Q Rwind Recv-Q    State
  -------------------- -------------------- ----- ------ ----- ------
  -----------
        *.*                  *.*                0      0 49152      0 IDLE
        *.4145               *.*                0      0 49152      0 LISTEN
        *.8989               *.*                0      0 131760      0 LISTEN
        *.8199               *.*                0      0 49152      0 LISTEN
        *.14150              *.*                0      0 49152      0 LISTEN
        *.111                *.*                0      0 49152      0 LISTEN
        ...
  ```

- Windows OS

  ```
  # netstat -ano
  ```

  Information similar to the following is displayed:

  ```
  Active Connections
  ```

```
  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       900
  TCP    0.0.0.0:371            0.0.0.0:0              LISTENING       1892
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:2401           0.0.0.0:0              LISTENING       2032
  TCP    0.0.0.0:2967           0.0.0.0:0              LISTENING       1284
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       852
  TCP    0.0.0.0:20100          0.0.0.0:0              LISTENING       2556
  TCP    10.112.38.168:139      0.0.0.0:0              LISTENING       4
  TCP    10.112.38.168:1204     10.72.18.62:445        ESTABLISHED     4
  TCP    10.112.38.168:1248     10.82.20.114:80        CLOSE_WAIT      2380
  TCP    10.112.38.168:1320     10.72.112.73:1352      ESTABLISHED     3644
  TCP    10.112.38.168:1333     10.82.20.135:80        CLOSE_WAIT      2380
  TCP    10.112.38.168:1351     10.110.0.27:135        ESTABLISHED     648
      ...
```

- SUSE Linux OS

  ```
  # /bin/netstat -ant
  ```

  Information similar to the following is displayed:

  ```
  TCP: IPv4
     Local Address          Remote Address      Swind Send-Q Rwind Recv-Q    State
  -------------------- -------------------- ----- ------ ----- ------
  ------------
        *.*                  *.*                  0      0 49152      0 IDLE
        *.4145               *.*                  0      0 49152      0 LISTEN
        *.8989               *.*                  0      0 131760       0 LISTEN
        *.8199               *.*                  0      0 49152      0 LISTEN
        *.14150              *.*                  0      0 49152      0 LISTEN
        *.111                *.*                  0      0 49152      0 LISTEN
        ...
  ```

6.6.2 Ports Between the U2000 Server and the NEs

This topic describes the ports used between the U2000 server and the NEs.

While setting up a firewall between the U2000 server and the NEs, you must enable ports as follows:

- Any port on the U2000 server can connect to the ports listed in **Table 6-13**.
- Any port on the NEs can connect to the ports listed in **Table 6-14**.

Table 6-13 Ports on the NEs for connecting the U2000

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	NEs	UDP	Any port	161	Port for NEs to receive SNMP requests. NEs and other processes send messages to this port.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	NEs	TCP	Any port	21	FTP-based port. The NE functions as the FTP server and the bulk collector periodically obtains PW performance files from NEs over the FTP protocol through this port
U2000 Server	NEs	TCP	Any port	1400	Port for transport GNEs. This port is used for the NMS server to communicate with and manage NEs.
U2000 Server	NEs	UDP	35600 to 35654	1500	Port for transport NEs. This port is used for the NMS server to communicate with NEs, and automatic discovery of equipment.
U2000 Server	NEs	TCP	Any port	3081	For the TL1 NE, port on the NE side whose ID is 3081. This port is used for the communication between the NMS and NEs.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	NEs	TCP	Any port	5432	Port on the NE side whose ID is 5432. This port is used for the communication between the NMS and NEs.
U2000 Server	NEs	TCP	Any port	23	Telnet protocol port which ne management processes use to configure and synchronize the resources
U2000 Server	NEs	UDP	Any port	68	Port for the PnpMgrDM process. This is the destination port for DHCP responses. NEs listen to this port. The PnP process sends DHCP responses to such ports of NEs.
U2000 Server	NEs	TCP	Any port	22	NetConf protocol port. This port is used for the interaction between the U2000 and NEs.

Table 6-14 Ports on the U2000server for connecting NEs

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
NEs	U2000 Server	TCP	Any port	21	FTP-based port. The NMS functions as the FTP server and NEs periodically upload performance files to the NMS server through this port
NEs	U2000 Server	TCP	Any port	21	Port for the FTP server process to provide file transfer services. Some NEs of the access, datacom, and transport domains that are managed by the data center (DC) rely on FTP services to back up data and load software.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
NEs	U2000 Server	TCP	Any port	22	Port for the SFTP server process. This port is used for SFTP services. Some NEs of the access, datacom, and transport domains that are managed by the data center (DC) rely on SFTP services to back up data and load software.
NEs	U2000 Server	TCP	Any port	69	ort for the TFTP server process. This port is used for TFTP services. The DC uses TFTP services to back up data for and load software on NEs in the access domain.
NEs	U2000 Server	UDP	Any port	4999	Port for the secdevregdm process. This port is used for security NEs to proactively register with the NMS server.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
NEs	U2000 Server	UDP	Any port	13005	Port for the UniteUitlDM process. This port is used for automatic discovery of PTN NEs. NEs regularly send NE data in UDP packets through this port to the NMS.
NEs	U2000 Server	UDP	Any port	514	Port for the SyslogCollec-torDM process. This is a general Syslog port. This port is used for the OSS to receive operation logs and running logs from NEs. Operation logs and running logs are sent in UDP packets through this port after NEs are properly configured.
NEs	U2000 Server	UDP	Any port	162	Port for the trapdispatcher process. It is used by the NMS to receive alarms and events of NEs by means of SNMP trap packets.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
NEs	U2000 Server	UDP	Any port	67	Port for the PnpMgrDM process. This is the destination port for DHCP requests. The plug and play (PnP) process listens to this port and receives the DHCP requests from NEs.
NEs	U2000 Server	TCP	Any port	13029	Port for the U2560TR069 Dm process. The NMS server communicates with TR069-compliant access NEs through this port in HTTP mode by using the TR069 protocol stack.
NEs	U2000 Server	TCP	Any port	13030	Port for the U2560TR069 Dm process. The NMS server communicates with TR069-compliant access NEs through this port in HTTPS mode by using the TR069 protocol stack.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
NEs	U2000 Server	TCP	Any port	13033	Port for the U2560TR069 Dm process. The NMS server communicates with TR069-compliant access NEs through this TR069 protocol stack-based port.

6.6.3 Ports Between the U2000 Server and the Clients

This topic describes the ports used between the U2000 server and the clients.

While setting up a firewall between the U2000 server and the clients, you must enable the ports on the U2000 server. Any port on the U2000 server can connect to the ports listed in **Table 6-15**.

Table 6-15 Ports on the U2000 server for connecting the clients

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Clients	U2000 Server	TCP	Any port	12200	Port used to perform oprations on the QuickStep in command lines.
U2000 Clients	U2000 Server	TCP	Any port	12201	Port used by the QuickStep client to send HTTP requests.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Clients	U2000 Server	TCP	Any port	12204	Port for the Quickstep commissioning. It is recommended that this port is enabled for only the maintenance of the server.
U2000 Clients	U2000 Server	TCP	Any port	13006	SSL-based port for the toolkit process on the server and this port is open to Toolkit clients. The Toolkit is an upgrade tool for board-level NEs in the transport domain, which is part of the NE Software Management System.
U2000 Clients	U2000 Server	TCP	Any port	21	General port for FTP services for NE software management. FTP files (such as NE software packages and NE configuration files) can be delivered between the NMS server and clients through this port.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Clients	U2000 Server	TCP	Any port	22	Port for the SFTP server process. The NMS client and server transfer files to each other through this port. The DC uses the SFTP service to configure data on NEs and transfer NE software between clients and the server of the NMS.
U2000 Clients	U2000 Server	TCP	Any port	8999	Port for the toolkit process on the server. This port can be used by the Toolkit client. This port is based on the SSL protocol. The Toolkit is an upgrade tool for board-level NEs in the transport domain, which is part of the NE Software Management System.
U2000 Clients	U2000 Server	TCP	Any port	443	Port for the xmlagent process in SSL mode. This port is used for the NMS to listen to HTTPs requests from the OSS.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Clients	U2000 Server	TCP	Any port	11080	Web service port for the standalone Web LCT.
U2000 Clients	U2000 Server	TCP	Any port	13003	Port for the gcli process. This port is an HTTP-based port. Service processes of the intelligent configuration tool listen to this port and receive operation requests.
U2000 Clients	U2000 Server	TCP	Any port	13004	Port for the gcli process. This port is an HTTPS-based port. Service processes of the intelligent configuration tool listen to this port and receive operation requests.
U2000 Clients	U2000 Server	TCP	Any port	12212	Port for the msserver process. This port is used to for MSuite clients to communicate with the MSuite server.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Clients	U2000 Server	TCP	Any port	12213	Port for the msserver process in SSL mode. This port is used to for MSuite clients to communicate with the MSuite server.
U2000 Clients	U2000 Server	TCP	Any port	12214	Port for the msserver process. This port is used for file transfer between the MSuite server and clients.
U2000 Clients	U2000 Server	TCP	Any port	12215	Port for the msserver process in SSL mode. This port is used to for MSuite clients to communicate with the MSuite server.
U2000 Clients	U2000 Server	TCP	Any port	14150	Port for the VCS Command process on the Veritas HA system. This port is used for the NMS server to issue VCS commands to NMS clients.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Clients	U2000 Server	TCP	Any port	8080	Universal port for the HTTP service. This port is provided by the NMS server for clients to use HTTP services. This port is used by client auto update (CAU), HedEx online help, and Web LCT.
U2000 Clients	U2000 Server	TCP	Any port	8181	Port for VCS Web service in a Veritas-based HA system. By default, the NMS server does not use the VCS web service.
U2000 Clients	U2000 Server	TCP	Any port	8443	Service port provided by the NMS server for clients to use HTTPS services. This port is used for the online help and Web LCT.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Clients	U2000 Server	TCP	Any port	12216	Web proxy port for managing the SRG equipment. This port is used by processes of the server to manage the SRG equipment by means of Web proxy.
U2000 Clients	U2000 Server	TCP	Any port	31030	Port for the imapmrb process. The MDP process sends messages through this port.
U2000 Clients	U2000 Server	TCP	Any port	31032	Port for the EventService process. This port is used when events are sent.
U2000 Clients	U2000 Server	TCP	Any port	31035	Port for the porttrunk_agent process. This port is used for the porttunk process.
U2000 Clients	U2000 Server	TCP	Any port	31037	Port for the DesktopService process. Java clients communicate with the server through this port.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Clients	U2000 Server	TCP	Any port	31038	Port for the DesktopService process. A Web client connects with the server through this port.
U2000 Clients	U2000 Server	TCP	Any port	31039	Port for the DesktopService process (in SSL mode). Java clients communicate with the server through this port.
U2000 Clients	U2000 Server	TCP	Any port	31040	Port for the DesktopService0101 process (in HTTPS mode). A Web client connects with the server through this port.
U2000 Clients	U2000 Server	TCP	Any port	31041 to 31050	process. When multiple instances are deployed for the DesktopService, port IDs range from 31041 to 31050.
U2000 Clients	U2000 Server	TCP	Any port	31080	Port for the imapmrb process (in SSL mode). This port is used when the MDP process sends massages.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Clients	U2000 Server	TCP	Any port	31082	Port for the EventService process (in SSL mode). This port is used for sending events.
U2000 Clients	U2000 Server	TCP	Any port	13001	Port for the Nemgr_vmf process. This port is used for the interaction between the client and the server.

6.6.4 Ports Between the U2000 Server and the OSS

This topic describes the ports used between the U2000 server and the operation support system (OSS).

While setting up a firewall between the U2000 server and the OSS, make sure that any port on the U2000 server can connect to the ports listed in **Table 6-16**.

Table 6-16 Ports on the U2000 server for connecting the OSS

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
OSS	U2000 Server	TCP	Any port	21	FTP protocol port. The performance text NBI process transfers performance files to the OSS through this port by means of the FTP protocol.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
OSS	U2000 Server	TCP	Any port	12001	Port for the Naming_Service process in non-SSL mode. The Naming_Service process, an ACE/TAO-based open-source naming service process of the CORBA NBI, is used to register CORBA service objects.
OSS	U2000 Server	TCP	Any port	12002	Port for the itnotify process in non-SSL mode. The Notify_Service process, an ACE/TAO-based open-source notification service of the CORBA NBI, is used to forward events to the OSS through the CORBA NBI.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
OSS	U2000 Server	TCP	Any port	12002	Port for the itnotify process. The itnotify is a notify process developed by Progress Software. This port is used for the NMS to forward CORBA events to the OSS.
OSS	U2000 Server	TCP	Any port	12003	Port for the Agent_CORBA process. This port is used for the NMS to listen to CORBA requests from the OSS through the CORBA NBI.
OSS	U2000 Server	TCP	Any port	22001	Port for the Naming_Service process in SSL mode. The Naming_Service process, an ACE/TAO-based open-source naming service process of the CORBA NBI, is used to register CORBA service objects.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
OSS	U2000 Server	TCP	Any port	22002	Port for theNotify_Service in SSL mode. The Notify_Service process, an ACE/TAO open-source notification service of the CORBA NBI, is used to forward events to the OSS through the CORBA NBI.
OSS	U2000 Server	TCP	Any port	22002	Port for the itnotify process in SSL mode. The itnotify is a notify process developed by Progress Software. This port is used for the NMS to forward CORBA events to the OSS.
OSS	U2000 Server	TCP	Any port	22003	Port for the Agent_CROBA process in SSL mode. This port is used for the NMS to listen to CORBA requests from the OSS through the CORBA NBI.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
OSS	U2000 Server	TCP	Any port	61616	Port for the JMSServer process (service port in non-SSL mode). This port is used by the JMS message server to interconnect with the OSS.
OSS	U2000 Server	TCP	Any port	61617	Port for the JMSServer process (service port in SSL mode). This port is used by the JMS server to interconnect with the OSS
OSS	U2000 Server	TCP	Any port	8161	Port for the JMSServer process. This port is used for monitoring and maintenance.
OSS	U2000 Server	UDP	Any port	9812	Port for the snmp_agent process. This is an SNMP listening port for the NMS to receive requests from the OSS.
OSS	U2000 Server	TCP	Any port	9997	Port for the xmlagent process in SSL mode. This port is used for the NMS to listen to HTTP requests from the OSS.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
OSS	U2000 Server	TCP	Any port	15000	Port for the Eml_mml process. This port is used for the NMS to communicate with the OSS through the MML interface.
OSS	U2000 Server	TCP	Any port	15001	Port for the Eml_mml process in SSL mode. This port is used for the NMS server to communicate with the OSS through the MML interface.
OSS	U2000 Server	TCP	Any port	10501	Port for the iNBXMLSoap Agent process. This port interconnects with the XML1.1 NBI and is used to provision services for access NEs through the XML1.1 NBI.
OSS	U2000 Server	TCP	Any port	8001	Port for the CFMSiDm process. This port is used to dynamically adjust the process commissioning switch.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
OSS	U2000 Server	TCP	Any port	9000	Port for the cltsi process. This port interconnects with NBIs and is used to conduct narrowband line tests on access NEs.
OSS	U2000 Server	TCP	Any port	9001	Port for the CFMSiDm process. This port interconnects with the CFMSi NBI and is used to set telephone numbers for access NEs.

Table 6-17 lists the ports on the OSS for connecting the U2000 server.

Table 6-17 Ports on the OSS for connecting the U2000 server

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	OSS	TCP	Any port	982	Port for the snmp_agent process. It is an SNMP forwarding port for the delivery of trap packets.

6.6.5 Ports on Primary and Secondary Sites of the Veritas HA System

This topic describes the ports required when the U2000 uses the Veritas HA system.

When the U2000 uses the Veritas HA system, you need to configure the ports required by the Veritas HA system. See Table 6-18.

NOTE

When configuring the firewall between the primary and secondary sites, you need to set only the protocol type, source IP address, and destination IP address, but not the source port and destination port.

Table 6-18 Veritas on primary and secondary sites of the HA system ports

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	12212	Port for the msserver process. This port is used for MSuite clients to communicate with the MSuite server. On the high availability (HA) system, this port is used for servers at the primary site to notify the secondary site for cooperative deployment.
U2000 Server	U2000 Server	TCP	Any port	12213	Port for the msserver process. This port is used for MSuite clients to communicate with the MSuite server. On the HA system, this port is used for the primary site to notify the secondary site for cooperative deployment.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	12214	Port for the msserver process. This port is used to for MSuite clients to communicate with the MSuite server. On the HA system, this port is used for file transfer between the primary and secondary.
U2000 Server	U2000 Server	TCP	Any port	12215	Port for the msserver process in SSL mode. This port is used for MSuite clients to communicate with the MSuite server. On the HA system, this port is used for file transfer between the primary and secondary sites.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	14145	Port for the VCS global cluster on the Veritas HA system. This port is used for the WAC (Wdie-Area connector) process on the local cluster to listen to connection from remote clusters.
U2000 Server	U2000 Server	TCP	Any port	14155	Port for the GCO WAC process on the Veritas HA system. This port is used for the WAC (Wdie-Area connector) process on the local cluster to listen to connection from remote clusters.
U2000 Server	U2000 Server	TCP,UDP	Any port	4145	Port for Veritas volume replicator (VVR) heartbeat communication between the active and standby servers. This port listens to the transport layer of the system.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	8199	Port for the vradmind process of the VVR in a Veritas-based HA system. The active and standby servers communicate by means of the vradmind process through this port.
U2000 Server	U2000 Server	TCP	Any port	8989	Port for the in.vxrsyncd process of the VVR in a Veritas HA system. The active and standby servers communicate by means of the vradmind process through this port.

6.6.6 Ports for Internal Processes of the U2000 Server

This topic describes the ports for internal processes of the U2000 server.

The ports for internal processes of the U2000 server are used only for communication between internal processes of the U2000, but not external communication. You can view these ports by using the port scanning tool and do not need to configure them on firewalls.

U2000 internal processes of the server listed in **Table 6-19**.

Table 6-19 Ports for internal processes of the U2000 server

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	12202	Port used by the Quickstep Tomcat to send shutdown requests.
U2000 Server	U2000 Server	TCP	Any port	12203	Port used by the Quickstep tomcat AJP.
U2000 Server	U2000 Server	TCP	Any port	11000 to 11100	Port for transport NE management processes. This port is used for communication between NEs and the Web LCT and ASON management process.
U2000 Server	U2000 Server	TCP	Any port	135	RPC port for the Windows OS. This port contains the endpoint mapper and other RPC services. Most services of the Windows-based sever depends on this port.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	14141	Port for the VCS process on the Veritas HA system. This port is used for connection between the VCS server and clients. The VCS clients can be deployed either on the NMS server or on other PC.
U2000 Server	U2000 Server	TCP	Any port	14144	Port for the VCS process on the Veritas HA system. This is a VCS Notifier listening port. This port is used for the NMS to listen to the VCS server.
U2000 Server	U2000 Server	TCP	Any port	1433	Service port of the Microsoft SQL Server for connecting a remote database.
U2000 Server	U2000 Server	UDP	Any port	1434	Service port of the Microsoft SQL Monitor for monitoring a database.
U2000 Server	U2000 Server	TCP	Any port	1521	Service port of the Oracle database.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	2994	Port for internal database management. This port is blocked by the firewall.
U2000 Server	U2000 Server	TCP,UDP	Any port	4045	Port for network file system (NFS) services of SUSE Linux. In a distributed system, the active and standby servers share files by using the NFS service.
U2000 Server	U2000 Server	TCP	Any port	4100	Service port for Sybase database.
U2000 Server	U2000 Server	TCP	Any port	4200	Service port for backing up the Sybase database.
U2000 Server	U2000 Server	TCP	Any port	587	SMTP service port provided by the OS. This port is not used by the NMS server.
U2000 Server	U2000 Server	TCP	Any port	9819	Port for the TL1NBiDm process. This port interconnects with the TL1 NBI and is used to provision services for access NEs through the TL1 NBI.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	11101 to 11104	TCP port for forwarding traps internally. Traps are forwarded to NEs through this port.
U2000 Server	U2000 Server	TCP	Any port	31000	Port for the imapsysd process. It is used to call the CORBA NBI of the sysd.
U2000 Server	U2000 Server	TCP	Any port	31001	Port for the lic_agent process. It is used to call the CORBA NBI of the lic.
U2000 Server	U2000 Server	TCP	Any port	31005	Port for the log_agent process. This port is used when the CORBA NBI of the log is called.
U2000 Server	U2000 Server	TCP	Any port	31006	Port for listening to logs. This port is used when services call the log of the log_client.
U2000 Server	U2000 Server	TCP	Any port	31007	Port for the SettingService process. This port is used when services call the setting_client to obtain configurations.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	31008	Port for the sm_agent process. This port is used when the corba NBI of the sm is called.
U2000 Server	U2000 Server	TCP	Any port	31010	Port for the tm_agent process. This port is used when the CORBA NBI of the tm is called.
U2000 Server	U2000 Server	TCP	Any port	31011	Port for the ifms_agent process. This port is used when the CORBA NBI of the fm is called.
U2000 Server	U2000 Server	TCP	Any port	31013	Port for the manager_agent process. This port is used when the CORBA NBI of the manager is called.
U2000 Server	U2000 Server	TCP	Any port	31015	Port for the itm_agent process. This port is used when the CORBA NBI of the itm is called.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	31033	Port for the lte_agent process. This port is used when the CORBA NBI of the Ite is called.
U2000 Server	U2000 Server	TCP	Any port	31036	Port for the eam_agent process. This port is used when the CORBA NBI of the eam is called.
U2000 Server	U2000 Server	TCP	Any port	31050	Port for the imapsysd process (in SSL mode). This port is used when the CORBA NBI of the sysd is called.
U2000 Server	U2000 Server	TCP	Any port	31051	Port for the lic_agent process (in SSL mode). This port is used when the CORBA NBI of the lic is called.
U2000 Server	U2000 Server	TCP	Any port	31055	Port for the log_agent process (in SSL mode). This port is used when the CORBA NBI of the log is called.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	31057	Port for the SettingService process (in SSL mode). This port is used when services call the setting_client to obtain configurations.
U2000 Server	U2000 Server	TCP	Any port	31058	Port for the sm_agent process (SSL). This port is used when the CORBA NBI of the sm is called.
U2000 Server	U2000 Server	TCP	Any port	31060	Port for the tm_agent process. This port is used when the CORBA NBI of the tm is called.
U2000 Server	U2000 Server	TCP	Any port	31061	Port for the ifms_agent process (SSL). This port is used when the CORBA NBI of the fm is called.
U2000 Server	U2000 Server	TCP	Any port	31063	Port for the manager_agent process (in SSL mode). This port is used for calling the CORBA NBI of the manager.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
U2000 Server	U2000 Server	TCP	Any port	31065	Port for the itm_agent process (SSL). This port is used when the CORBA NBI of the itm is called.
U2000 Server	U2000 Server	TCP	Any port	31083	Port for the lte_agent process (in SSL mode). This port is used when the CORBA NBI of the lte is called.
U2000 Server	U2000 Server	TCP	Any port	31099	Port for the eam_agent process (in SSL mode). This port is used when the CORBA NBI of the eam is called.
U2000 Server	U2000 Server	TCP	Any port	8250	Port listened to by the CAU. This port is used by the Cau service part of the Tomcat to partly check whether Cau services are available at present.

6.6.7 Ports for Remote Maintenance

This topic describes the ports for remote maintenance.

Table 6-20 lists the ports for remote maintenance.

Table 6-20 Ports for remote maintenance

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
Any port	U2000 Server	UDP	Any port	177	Standard XDMCP-based service port for Solaris and SUSE Linux OSs. X terminals, such as the XManager, operate Solaris and Linux OSs remotely through this port. It is recommended that you enable this port only for server maintenance.
Any port	U2000 Server	TCP	Any port	2148	Port for the VXSVC server on the Veritas-based HA system. Port for a customer Veritas Enterprise Administrator (VEA) client to connect to the VXSVC server to view and configure volumes.
Any port	U2000 Server	TCP	Any port	23	Standard Telnet-based service port. It is recommended that you enable this port only for server maintenance.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
Any port	U2000 Server	TCP	Any port	3389	Port for Windows to provide remote desktop services over the Remote Desktop Protocol (RDP).
Any port	U2000 Server	TCP	Any port	445	Port for sharing services on Window OS. It is recommended that this you enable this port only for server maintenance.
Any port	U2000 Server	TCP	Any port	6112	Port for the Solaris OS. This port is applicable to the CDE Subprocess Controls Server daemon (dtspcd). Through this port, you can log in to the Solaris-based server remotely from a CDE GUI.
Any port	U2000 Server	TCP	Any port	7100	Port for X Font services of Solaris. It is recommended that you enable this port only for server maintenance.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
Any port	U2000 Server	TCP	Any port	8005	Service port provided by the Tomcat for disabling Tomcat services.
Any port	U2000 Server	TCP	Any port	9003	Port for the StdCltsiDm process. This port is used to dynamically adjust the process commissioning switch.

6.6.8 Ports for Other Connections

This topic describes the ports for communication between the U2000 server and other applications.

Table 6-21 lists the ports for communication between the U2000 server and other applications.

Table 6-21 Ports for other connections

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
Any port	U2000 Server	TCP,UDP	Any port	111	RPC port for the Solaris-based server. This port is used to provide services such as NFS service. This port is not used for the NMS.

Source End	Destination End	Protocol Type	Source Port	Destination Port	Description
Any port	U2000 Server	UDP	Any port	123	General port for the NTP process. This port is used for time synchronization in a network. The NMS server that does not run on Windows can function as the NTP server.
Any port	U2000 Server	TCP	Any port	513	Port for Rlogin services of Solaris. This port is not used by the NMS server.
Any port	U2000 Server	TCP	Any port	6481	Port for Tag services of Solaris. This port is not used by the NMS server.
Any port	U2000 Server	TCP	Any port	8009	Port provided by the Tomcat for AJP services. This port is not used by the NMS.

6.7 Bandwidth Planning

The U2000 uses the standard client/server (C/S) architecture. The clients and the servers communicate with each other through the local area network (LAN) or the wide area network (WAN). The U2000 server communicates with NEs in the outband or inband mode, which has a certain requirement on bandwidth.

This topic describes the server-OSS bandwidth planning. The planning for the bandwidth between the server and the OSS needs to meet the requirements for the communication between them.

6.7.4 Bandwidth Planning of the Primary and Secondary Sites in the HA Mode
This topic describes the rules for calculating the bandwidth between the active site and standby site in the HA system and the requirements on network stability.

6.7.5 Bandwidth Planning for Distributed Deployment of the Master Server and the Slave Server
Bandwidth planning for the distributed deployment of the master server and the slave server needs to meet the requirements for the communication in between.

6.7.1 Server-NE Bandwidth Planning

The server-NE bandwidth must meet the requirements of the U2000 server on issuing commands and of the NEs on reporting information.

Principle

The following section describes the principle of the bandwidth for the communication between N equivalent NEs and the U2000 server. For different networks, the bandwidth of 2 Mbit/s may not meet the requirement of the current network. In this case, you can determine the CIR (Committed Information Rate) and PIR(Peak Information Rate) of the bandwidth according to the following formula:

- CIR
  - N > 56: 2048 k + (N - 56) x 0.5 k
  - N ≤ 56: 2 Mbit/s
- PIR
  - N > 56: 10240 k + (N - 56) x 5 k
  - N ≤ 56: 10 Mbit/s

Calculation Method

For example, if the U2000 server can manage up to 2,000 equivalent NEs, the bandwidth for the U2000 server to manage NEs must be no less than 3.02 Mbit/s.

6.7.2 Server-Client Bandwidth Planning

The server-client bandwidth must meet the requirement of clients for communication.

Principle

It is recommended that the server-client bandwidth for a U2000 client and the U2000 be higher than 2 Mbit/s. In some special scenarios, the server-client bandwidth cannot be lower than 128 Kbit/s. For example, if a notebook computer is used. If the server-client bandwidth is 128 Kbit/s, risks are posed to U2000 operation.

Calculation Method

Server-client bandwidth = Bandwidth for a U2000 client and the U2000 server x Number of U2000 clients

For example, if the U2000 server needs to communicate with 10 clients, the bandwidth for the communication between the U2000 server and clients must be no less than 20 Mbit/s.

6.7.3 Server-OSS Bandwidth Planning

This topic describes the server-OSS bandwidth planning. The planning for the bandwidth between the server and the OSS needs to meet the requirements for the communication between them.

The minimum bandwidth for the communication between the OSS and the U2000 server is 2 Mbit/s.

6.7.4 Bandwidth Planning of the Primary and Secondary Sites in the HA Mode

This topic describes the rules for calculating the bandwidth between the active site and standby site in the HA system and the requirements on network stability.

The rules for calculating the bandwidth between the active site and standby site are as follows:

- The size of each alarm data is 10000 bit. The NMS handles 100 alarms per second. The consumption rate of the Veritas replication is 10%.

  The maximum bandwidth for the remote synchronization of alarms in the HA system is calculated as follows: (A) = 10000 x 100 x (1 + 10%)/(1024 x 1024) = 1.1 Mbit/s.
- According to the experience data, the bandwidth (C) for data configuration is 0.6 Mbit/s at least.
- The size of each performance data is 3650 bit. The consumption rate of Veritas replication is 10%.

  The bandwidth for the remote synchronization of each performance data is calculated as follows: (P) = 3650 x (1 + 10%)/(1024) = 3.9 Kbit/s. On performance collection task corresponds to M pieces of performance data. The number of supported performance collection tasks is related to the management capability of the NMS.
- The bandwidth between the active site and standby site in the HA system is calculated as (T) = A + C + P×M×N

The following table shows the requirements on the network between the active site and standby site in the HA system.

Table 6-22 Requirements on bandwidth planning

Network Parameter	Requirement
Minimum Bandwidth	2 Mbit/s
Recommended Bandwidth	10 Mbit/s
Delay	Less than 10 seconds
Packet Loss Ratio	Less than 1%
Jitter	Less than 3 hours

NOTE

By default, the performance data is not synchronized remotely. The preceding minimum bandwidth is obtained by assuming that performance data is not synchronized by default.

6.7.5 Bandwidth Planning for Distributed Deployment of the Master Server and the Slave Server

Bandwidth planning for the distributed deployment of the master server and the slave server needs to meet the requirements for the communication in between.

The planning rules for the bandwidth between the master server and the slave server are as follows:

- The network configuration of the U2000 distributed system contains a private network and a public network.
- The interface used to configure the private network must connect to an independent private network switch instead of sharing a switch with the interface used to configure the public network.

The minimum bandwidth between the master server and the slave server is 100 Mbit/s.

6.8 Planning Reference for Performance Database Size

Performance data expands as time goes by. Therefore, you need to properly plan the database size.

The space required by performance data depends on the monitored resource type, resource quantity, collection period, and data saving period. You can specify different data saving periods as the collection period according to the requirement. Usually, the longer the collection period, the longer the data saving period. For the same data saving period, the shorter the collection period, the larger the required disk space.

For the estimation of performance database size, the collection period for each indicator in an indicator group requires approximately 0.6 KB.

Table 6-23 shows the sample space required by the performance data of router or switch interfaces. The calculation method of other resource types, such as link, is the same as that of the interface.

Table 6-23 Planning reference for performance database size

Resource Quantity	Collection Period	Saving Period (Day)	Total Saving Period (Saving Period/ Collection Period)	Required Disk Space (GB) (Total Saving Period x Resource Quantity x 0.3)
100,000 interfaces (23 indicators for each interface)	15 minutes	35	3360 **NOTE** Total saving period = 35 x 24 x 60/15	192 **NOTE** Total disk space = (35 x 24 x 60/15) x 100,000 x 0.6/(1024 x 1024)

Resource Quantity	Collection Period	Saving Period (Day)	Total Saving Period (Saving Period/ Collection Period)	Required Disk Space (GB) (Total Saving Period x Resource Quantity x 0.3)
	Disk space required when data is not merged			192
100,000 interfaces (23 indicators for each interface)	15 minutes	35	3360 **NOTE** Total saving period = 35 x 24 x 60/15	192 **NOTE** Total disk space = (35 x 24 x 60/15) x 100,000 x 0.6/(1024 x 1024)
	1 hour	60	1440 **NOTE** Total saving period = 60 x 24/1	247 **NOTE** Total disk space = (60 x 24/1) x 100,000 x 0.6 x 3 /(1024 x 1024)
	1 day	730	730 **NOTE** Total saving period = 730/1	125 **NOTE** Total saving period = (730/1) x 100,000 x 0.6 x 3 /(1024 x 1024)
	Disk space required when data is merged			564

NOTE

The importance of performance data decreases as time goes by. In particular, the smaller the time granularity, the less important the performance data.

The PMS supports the time-based merge of performance data. You can specify lifetime for performance data based on granularity. To be specific, the greater the granularity, the longer the lifetime; the smaller the granularity, the shorter the lifetime. This ensures that the disk space occupied by performance data does not increase sharply.

The PMS supports two merge schemes: minute to hour and hour to day. After the data merge, the maximum and minimum values are reserved. Therefore, the number of data records after merge changes from one to three, namely automatic merge value, maximum value, and minimum value.

7 DCN Planning

About This Chapter

The U2000 manages and maintains NEs by communicating with NEs over the Data Communication Network (DCN).

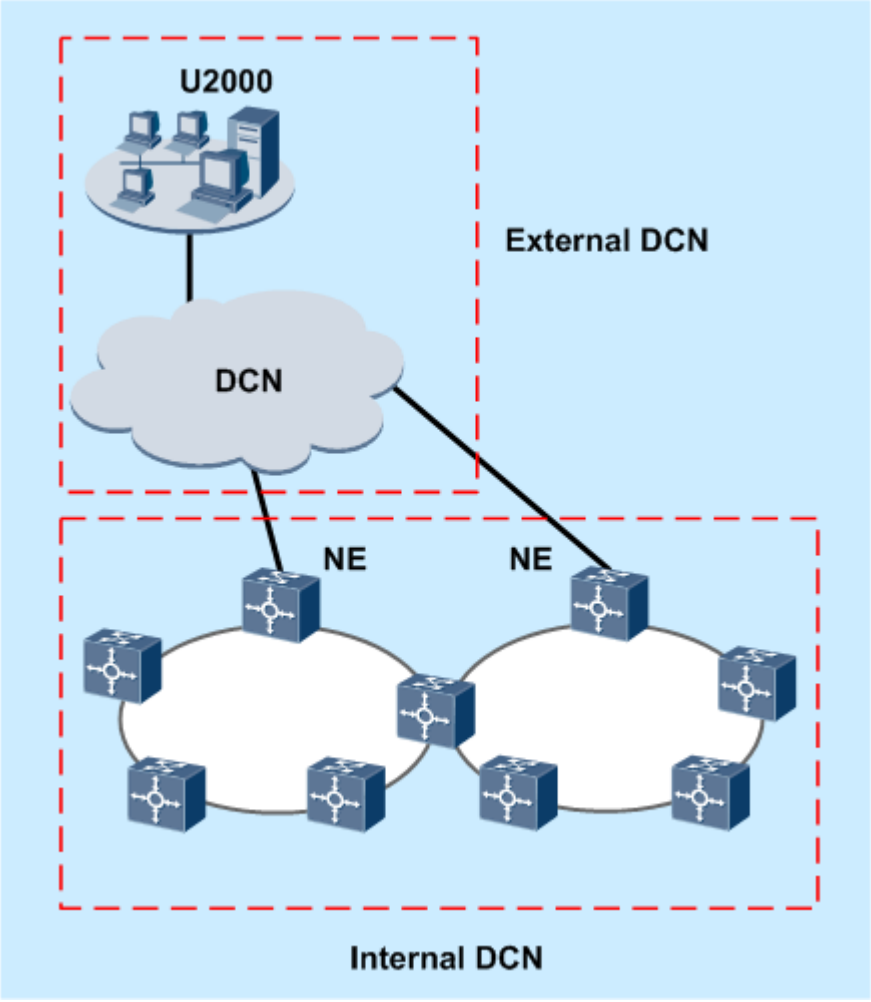
7.1 DCN Planning Rules

This topic describes how to reasonably plan DCN networking.

DCN Types

DCN is the Data Communication Network deployed for network management, as shown in Figure 7-1. DCN planning is a prerequisite for NE management.

Figure 7-1 DCN topology



A DCN is divided into two parts:

- External DCN

  An external DCN is usually a LAN or WAN and its main applications include:

  - DCN between network management systems, for example, between the U2000 server and the OSS, between the U2000 server and the clients, and between the primary site and the secondary site of the U2000 HA system.

NOTE

The DCN network between the NMSs must support the TCP/IP protocol.

- DCN between the U2000 server and NEs.

  NOTE

  The DCN network between the U2000 server and NEs must support the TCP/IP or OSI protocol.

- Internal DCN

  Communication network between NEs

Requirements for the Physical Structure of DCN

The general requirements of the U2000 for the physical structure of DCN are as follows:

- The DCN network between the NMSs and the managed network can be classified into LAN, WAN, and MAN in terms of the physical structure. It is required that the TCP/IP protocol be supported.
- The NMSs can directly connect to the NEs, Ethernet switches, or routers. The U2000 server and client provides only external RJ45 Ethernet ports. Therefore, the DCN network must provide RJ45 ports to connect with the U2000.
- The bandwidth of the DCN network must meet the communication requirement.

  For details, see **6.7 Bandwidth Planning**.

7.2 DCN (Between U2000s)

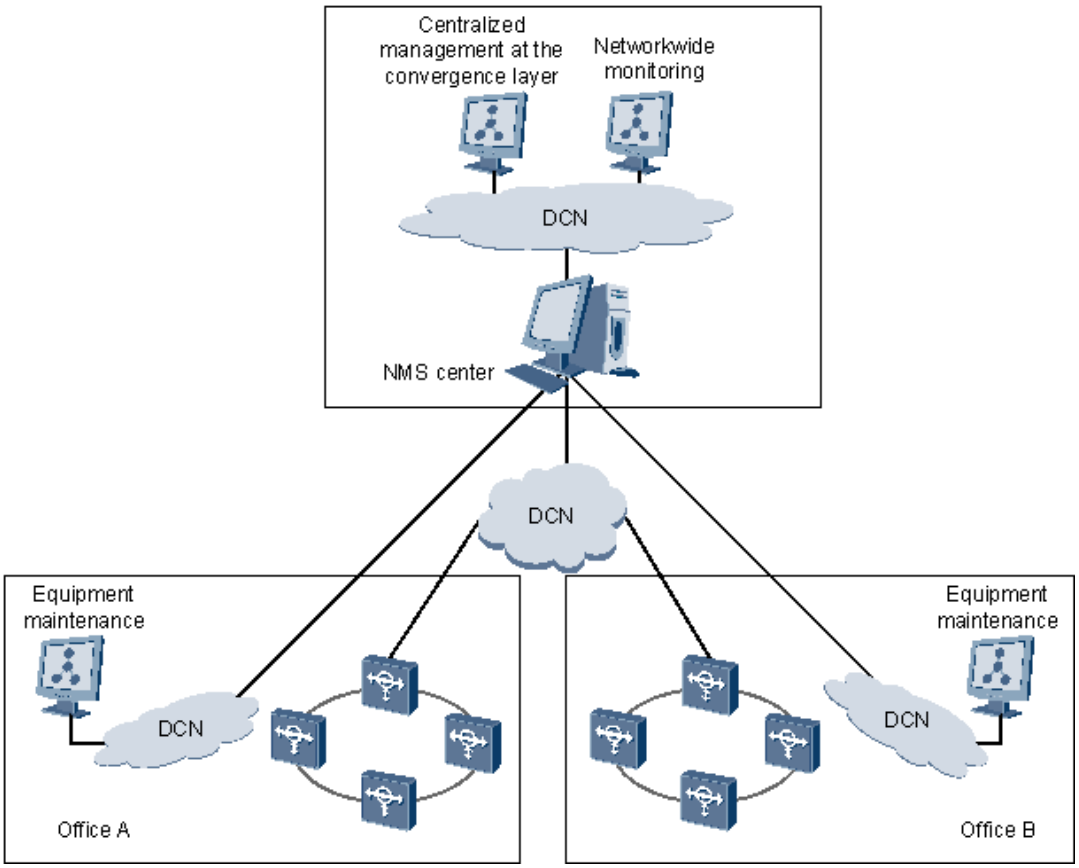
The DCN (between U2000s) indicates the DCN between the U2000 server and the clients and the DCN between the primary site and the secondary site of the HA U2000 system.

DCN Between the U2000 Server and the Clients

DCN networking between the clients and the server (distributed deployment)

The standard client/server structure is adopted in the U2000 and the server connects to the clients through a LAN or WAN. **Figure 7-2** shows the DCN networking between multiple clients and the server.

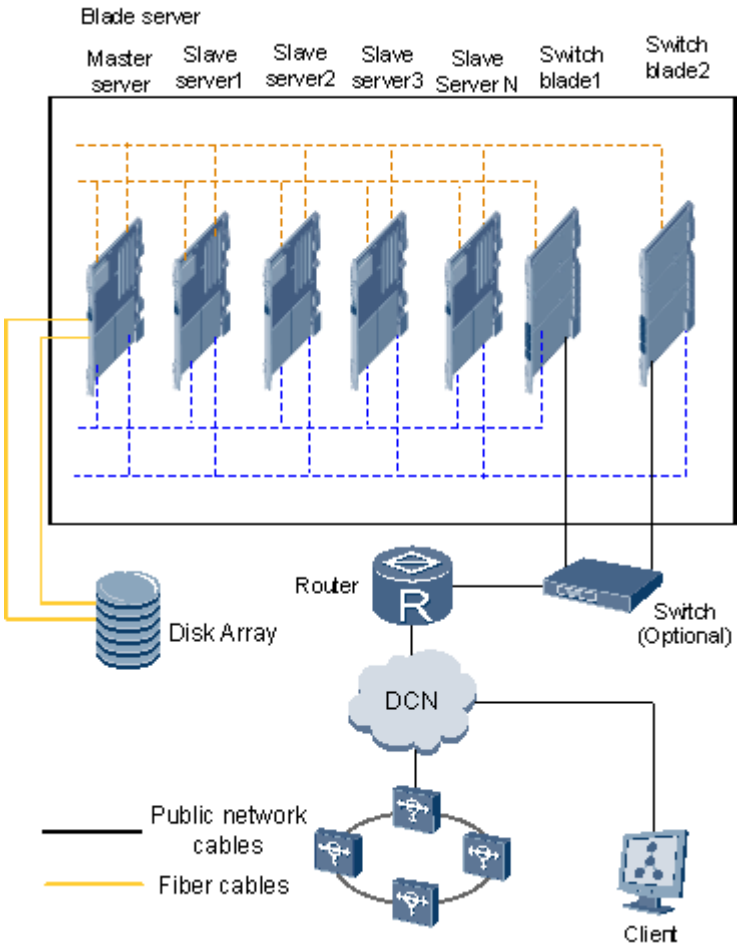
Figure 7-2 DCN networking between the client and the server (centralized deployment)



DCN networking between the client and the server (distributed deployment)

There are multiple slave servers in the distributed deployment system. Slave servers interconnect with the master server through the LAN. **Figure 7-3** shows the DCN networking between the master server and slave servers.

Figure 7-3 DCN networking between the client and the server (distributed deployment)

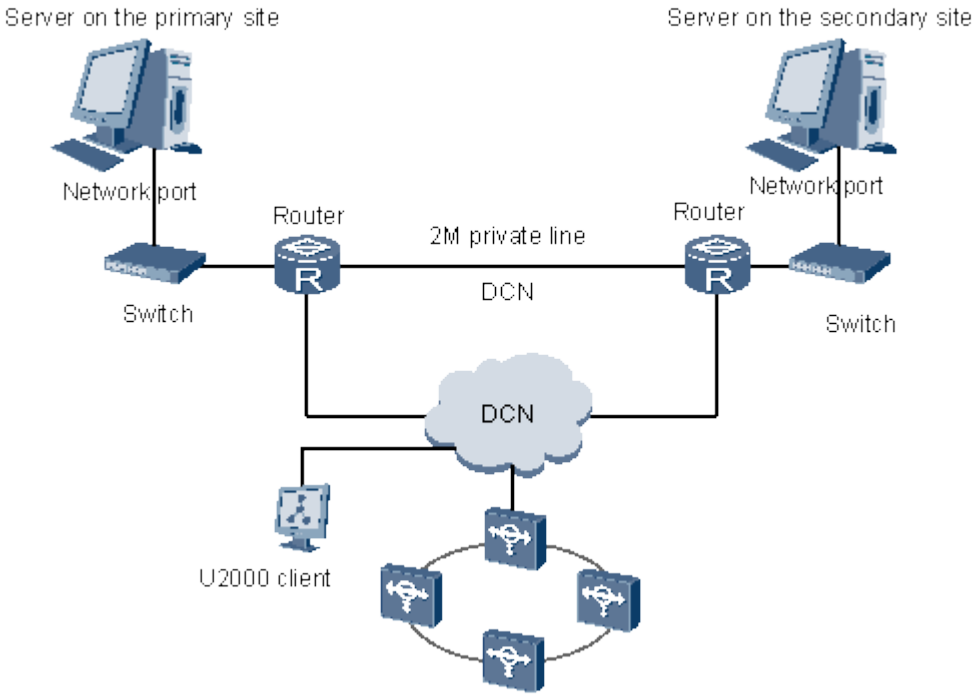


DCN between the primary site and the secondary site of the HA U2000 system

DCN networking between the primary site and secondary site (centralized deployment)

In the centralized deployment system, the primary site interconnects with the secondary site through a LAN or WAN. **Figure 7-4** shows the DCN networking between the primary site and the secondary site.

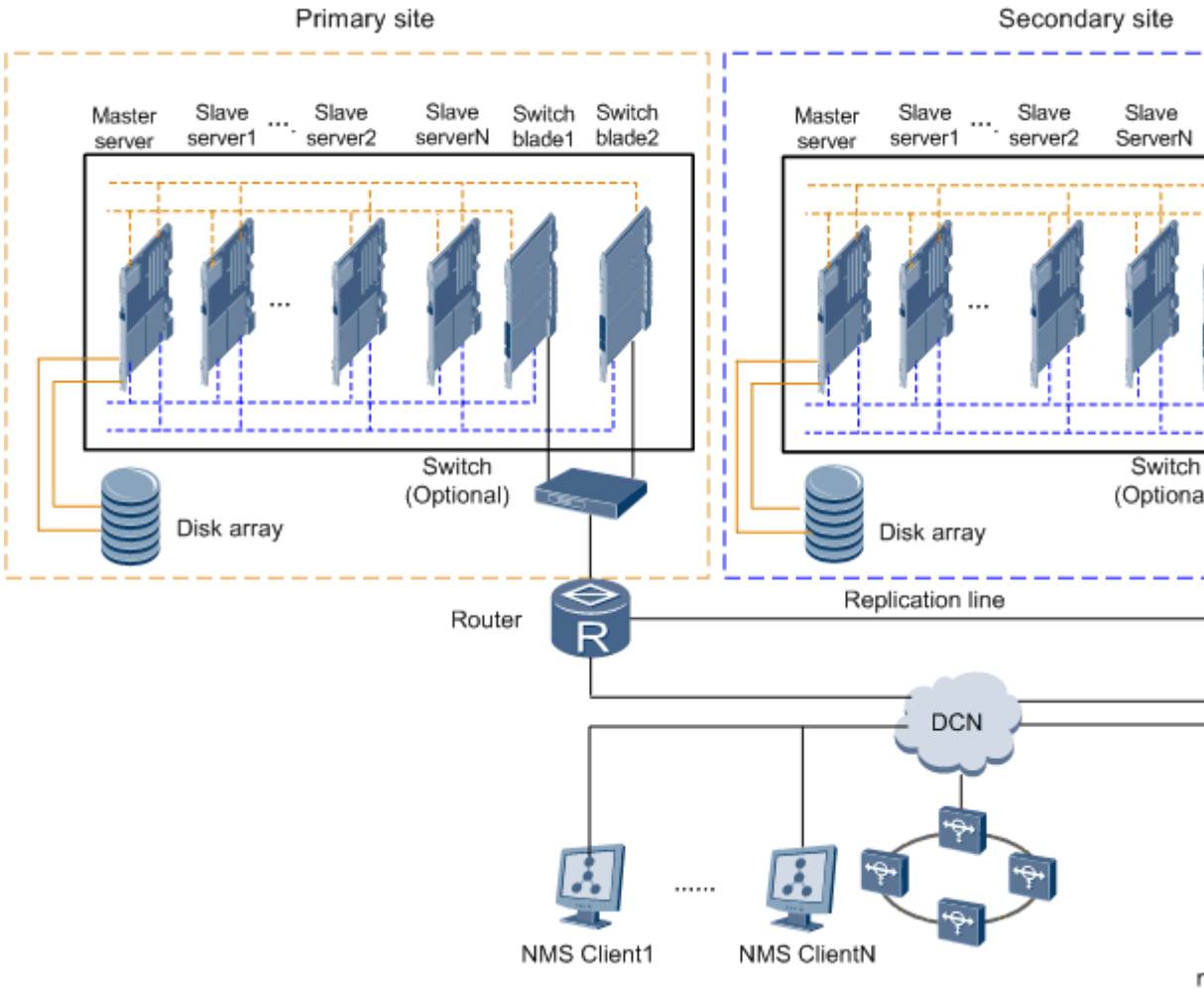
Figure 7-4 DCN networking between the primary site and secondary site (centralized deployment)



DCN networking between the primary site and the secondary site (distributed deployment)

In the distributed deployment system, the primary site interconnects with the secondary site through a LAN or WAN. **Figure 7-5** shows the DCN networking between the primary site and the secondary site.

Figure 7-5 DCN networking between the primary site and secondary site (distributed deployment)



7.3 DCN (U2000 and Managed Network)

This topic describes the DCN application between the U2000 and the managed network.

The DCN between the U2000 and the managed network is usually divided into two parts:

- DCN between the U2000 server and NEs

  Usually, a LAN or WAN is adopted for DCN communication between the U2000 server and NEs.

- DCN between NEs

  NEs can communicate with the U2000 in inband networking mode or outband networking mode.

7.3.1 DCN Application (Between the U2000 Server and NEs)
In actual networking, the U2000 server connects to NEs through an external DCN consisting of devices such as LAN switches and routers.

7.3.2 DCN Application (Between Transmission NEs)

The U2000 manages and maintains NEs by communicating with NEs through the DCN.

7.3.3 DCN Application (Between IP NEs)
Inband or outband networking is adopted for communications between the U2000 server and managed NEs.

7.3.4 DCN Application (Between Access NEs)
The outband or Inband U2000 is adopted for communications between the U2000 server and managed NEs.

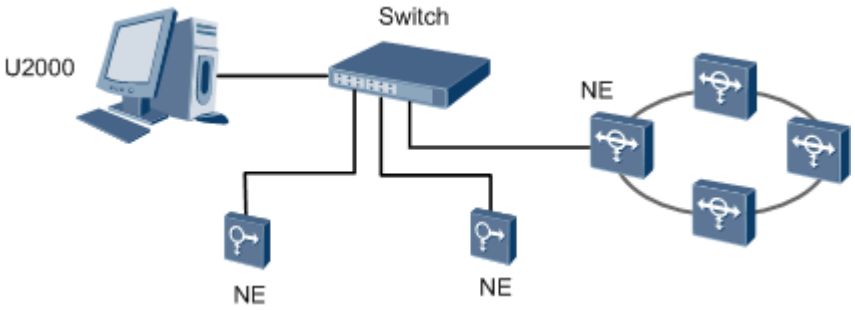
7.3.1 DCN Application (Between the U2000 Server and NEs)

In actual networking, the U2000 server connects to NEs through an external DCN consisting of devices such as LAN switches and routers.

Connecting the U2000 and NEs Through Switches

When the distance between the U2000 and NEs is less than or equal to 100 m, connecting the U2000 and NEs through switches is adopted, as shown in **Figure 7-6**.

Figure 7-6 Connecting the U2000 and NEs through DCN networking consisting of switches



Connecting the U2000 and NEs Through Router+E1

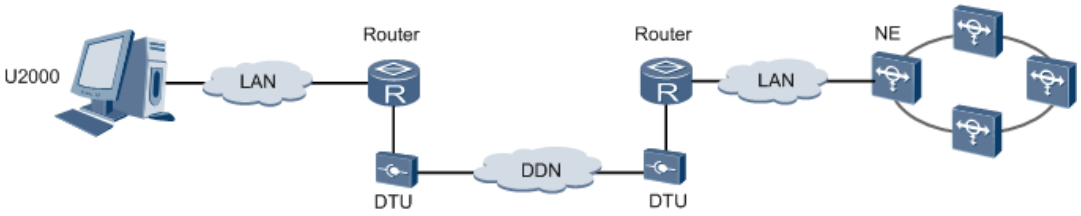
If the U2000 is far from NEs and there is the Router+E1 network between the U2000 and NEs, connecting the U2000 and NEs through Router+E1 can be adopted, as shown in **Figure 7-7**.

Figure 7-7 Connecting the U2000 and NEs through DCN networking consisting of switches

Connecting the U2000 and NEs Through Router+DTU+DDN

If the U2000 is far from NEs and there is the Router+DTU+DDN network between the U2000 and NEs, connecting the U2000 and NEs through Router+DTU+DDN can be adopted, as shown in **Figure 7-8**.

Figure 7-8 Connecting the U2000 and NEs Through Router+DTU+DDN



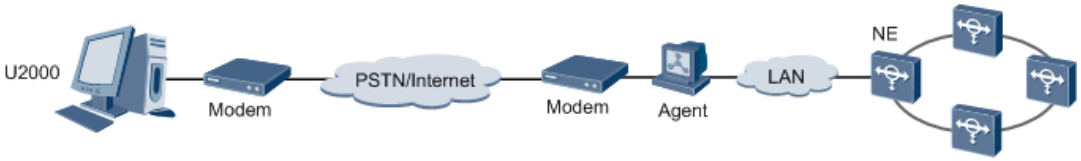
NOTE

DTU is the data transmission unit used by DDN links between data devices. It is actually a converter used between different physical ports and protocols.

Remote Maintenance

If the U2000 is far from NEs, the network management mode of remote maintenance can be adopted, as shown in **Figure 7-9**.

Figure 7-9 DCN networking in remote maintenance mode



NOTE

DCN networking in remote maintenance mode only applies to transmission NEs.

7.3.2 DCN Application (Between Transmission NEs)

The U2000 manages and maintains NEs by communicating with NEs through the DCN.

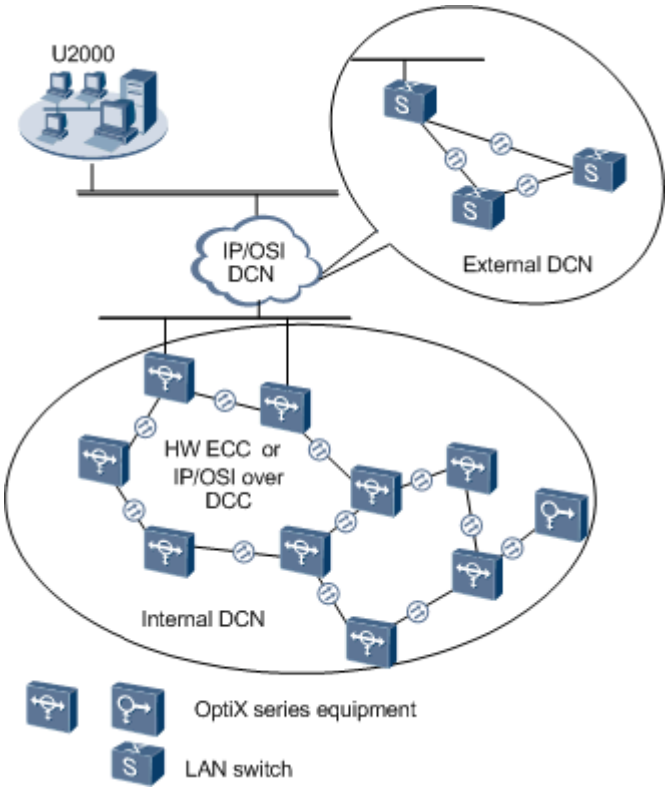
DCN Networking Diagram

On the DCN management network, the U2000 and NEs can be considered as nodes on a DCN and these nodes can be connected through Ethernet or DCC physical channels.

In actual networking, the U2000 server connects to NEs through an external DCN consisting of devices such as LAN switches and routers. DCNs among NEs are called internal DCNs. This topic focuses on the internal DCN that consists of transmission NEs.

Figure 7-10 shows such a DCN.

Figure 7-10 DCN networking



Internal DCN Application

Huawei's transmission 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.

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.

7.3.2.1 HWECC Application
TheECCthat Huawei implements provides a more flexible networking mode. The NEs can be connected through an optical port or the Ethernet port forECCcommunication. In some special conditions, the Huawei equipment can transparently transmit theOAMinformation from the third-party equipment.

7.3.2.2 Application of IP over DCC
An Ethernet port is used to connect the U2000 and NEs. The NEs are connected to each other through fibers or Ethernet.

7.3.2.3 Application of OSI over DCC
According to different network situations,OSI over DCC has two major applications.

7.3.2.1 HWECC Application

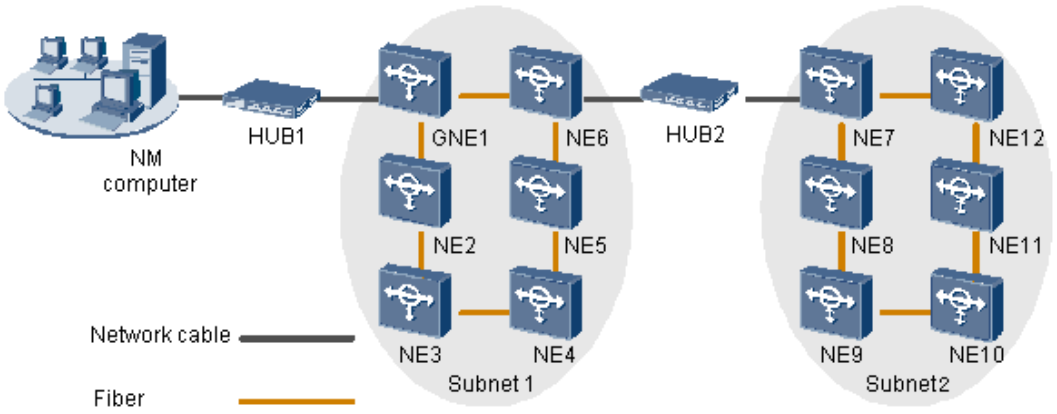
TheECCthat Huawei implements provides a more flexible networking mode. The NEs can be connected through an optical port or the Ethernet port forECCcommunication. In some special conditions, the Huawei equipment can transparently transmit theOAMinformation from the third-party equipment.

There are two typical applications of the HWECC protocol for networking schemes.

Application 1 Networking That Involves Only Huawei Equipment

Figure 7-11 shows the networking that involves only Huawei equipment.

Figure 7-11 Networking that involves only Huawei equipment



Such networking requires that one gatewayNE(GNE) be present for the communication between other NEs and the U2000 through the Ethernet interface. The NEs communicate with each other

through an optical port or Ethernet interfaces. The subnetworks in **Figure 7-11** perform the extendedECCcommunication through Ethernet interfaces, such as NE6 and NE7.

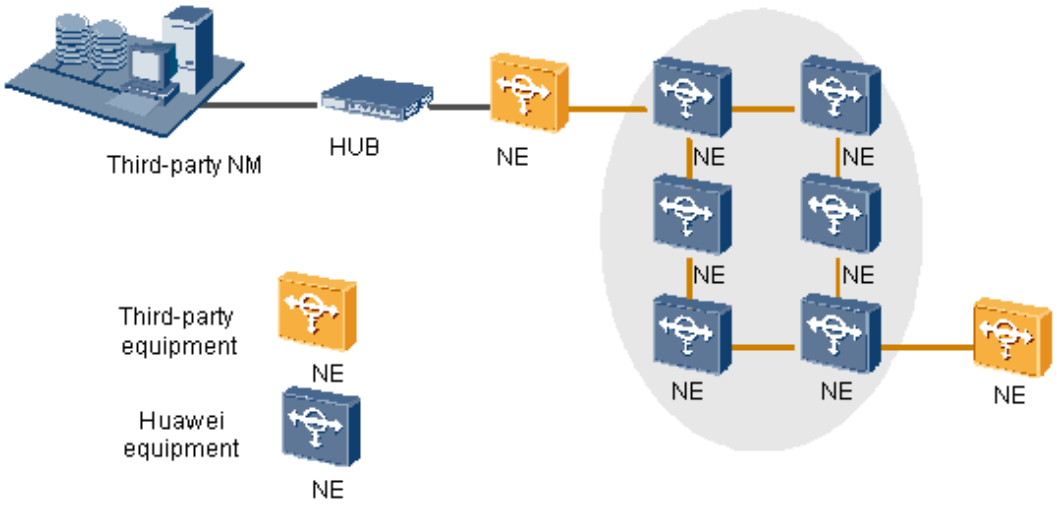
NOTE

ExtendedECCmeans theECCcommunication by using the Ethernet when there is no connected optical path between two or more NEs.

Application 2 Networking That Involves Huawei Equipment and Third-Party Equipment

Figure 7-12 shows the networking that involves Huawei equipment and third-party equipment.

Figure 7-12 Networking that involves Huawei equipment and third-party equipment



For such networking, theOAMinformation of the third-party equipment should travel through Huawei equipment, which provides the function to transparently transmit the DCC. During the transmission, Huawei equipment does not analyze the data. For theDCCtransparent transmission, perform the corresponding configuration at eachNEalong the data transmitting trail.

7.3.2.2 Application of IP over DCC

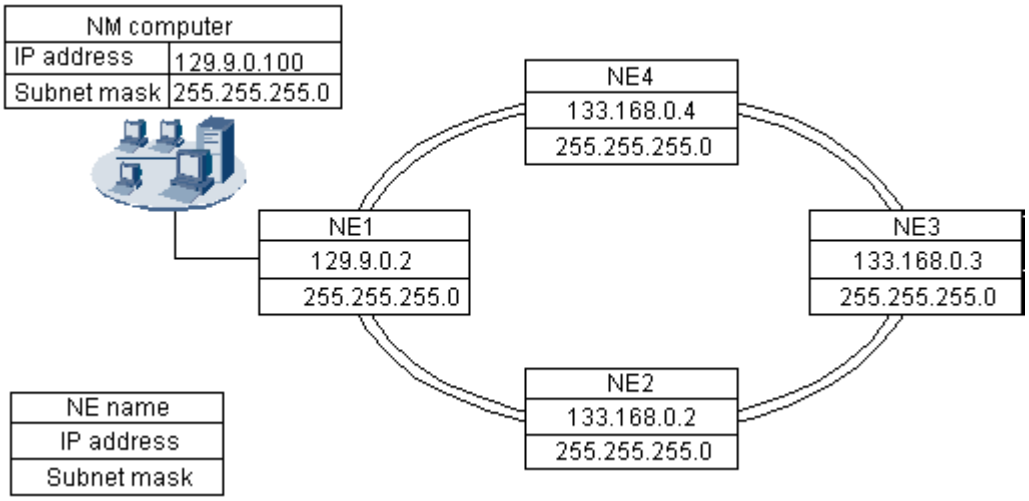
An Ethernet port is used to connect the U2000 and NEs. The NEs are connected to each other through fibers or Ethernet.

Application 1:Gateway NE Mode

If the U2000 and the GNE connect to the same Ethernet (the U2000 and the GNE need to be in the same subnet), and other NEs are accessed in the gateway NE mode, you need not to add any static routes.

As shown in **Figure 7-13**, the U2000 with the IP address of 129.9.0.100 uses the nearby NE1 as the GNE to access other NEs. You need not to add static routes on the U2000 or NEs.

Figure 7-13 Gateway NE mode

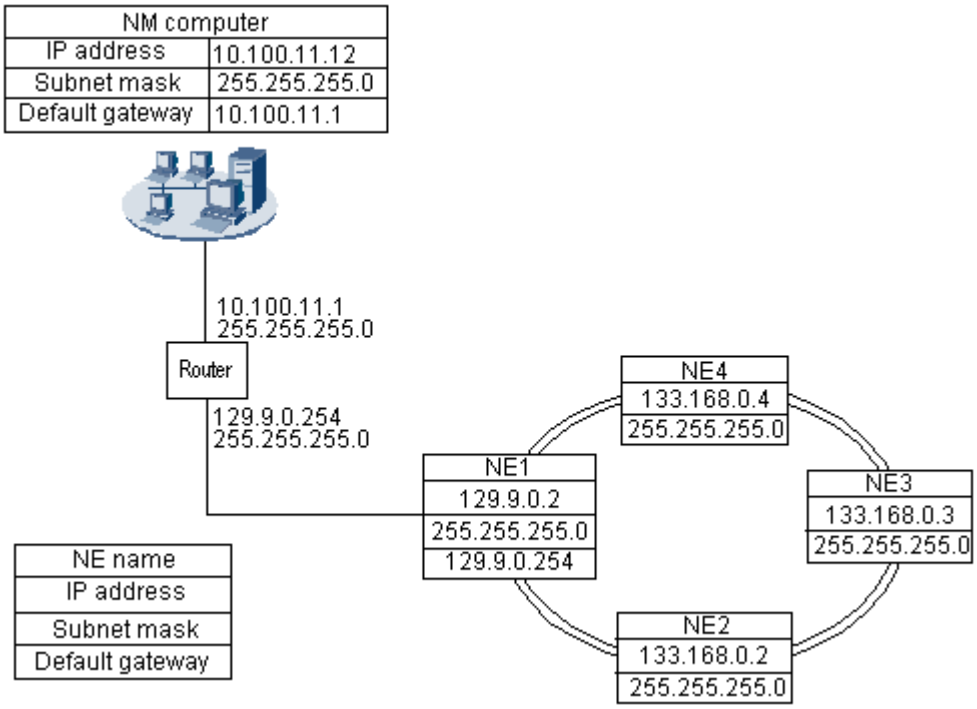


Application 2:Gateway NE Mode (by Default Gateway)

If the U2000 is connected to the GNE through a router and other NEs are accessed in the gateway NE mode, you need to add a default gateway on the U2000 and on the GNE.

As shown in **Figure 7-14**, the U2000 with the IP address of 10.100.11.12 connects with the GNE (NE1) through a router and accesses other NEs in the gateway NE mode. In this case, you need to set a default gateway on both the U2000 and NE1. Set the default gateway on the U2000 to 10.100.11.1, and that on NE1 to 129.9.0.254.

Figure 7-14 Gateway NE mode (by default gateway)

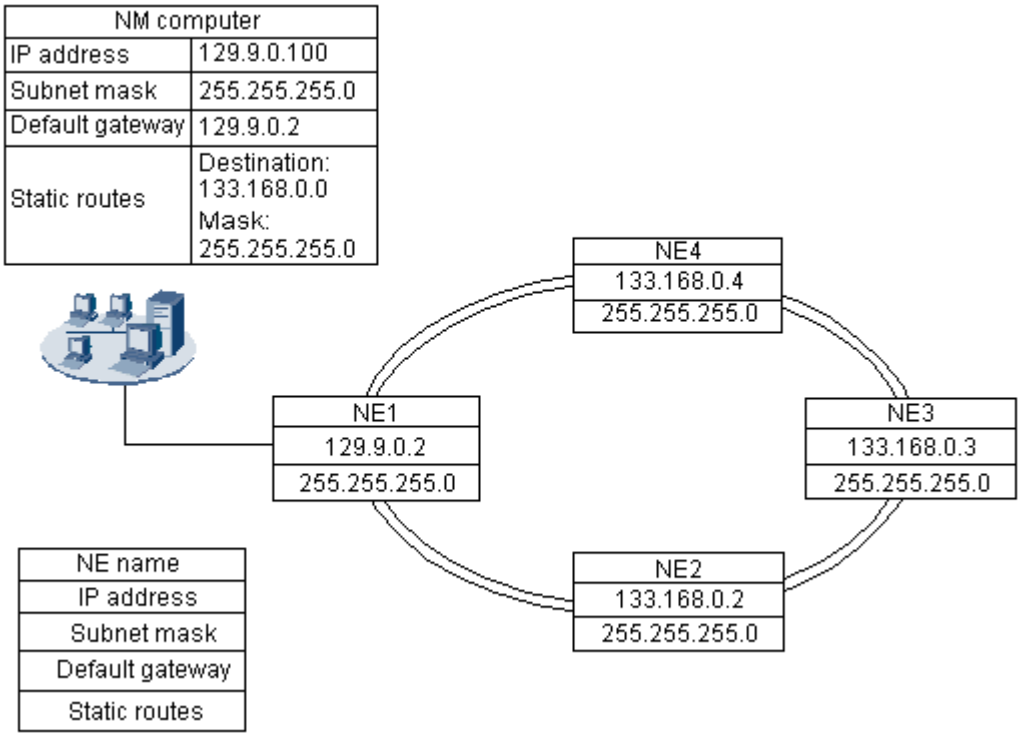


Application 3: Direct Connection Mode (by Static Routes)

If the U2000 and the GNE connect to the same Ethernet and other NEs are accessed in the direct connection mode, you need to set on the U2000 the default gateway to the IP address of the NE that is connected to the U2000 directly. Or you need to add the static route to the non-GNEs, with the forwarding address as the IP address of the GNE.

As shown in **Figure 7-15**, if the U2000 with the IP address of 129.9.0.100 needs to access NE3 directly, you need to add the static route to 133.168.0.0/24 on the U2000.

Figure 7-15 Direct connection mode (by static routes)



Application 4: Direct Connection Mode through a Router (by Static Routes)

The U2000 connects to the Ethernet port of a certain NE through a router and accesses other NEs in the direct connection mode. You need to perform the following operations.

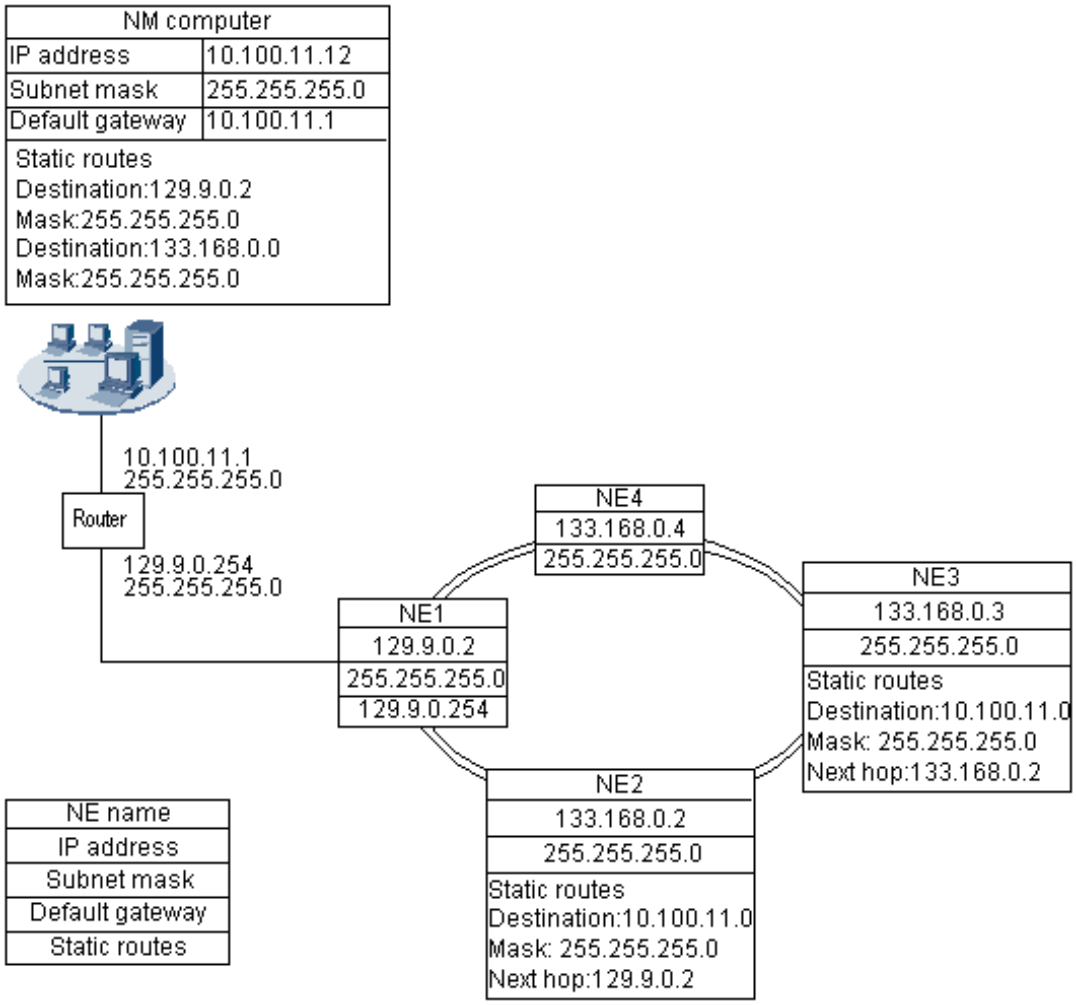
- On the U2000, set the static route to the GNE and non-GNEs.
- On the GNE, set the default route to the U2000.
- Add static routes to the U2000 on the destination station and the intermediate station.

As shown in **Figure 7-16**, the U2000 with the IP address of 10.100.11.12 connects to NE1 through a router and accesses NE3 in the direct connection mode. Suppose the IP address of the U2000 is 10.100.11.0 (subnet mask 255.255.255.0). Perform the listed operations:

- Add the static route on the U2000 to the gateway 129.9.0.2.

- Set the default gateway on NE1 to 129.9.0.254.
- Add the static route on NE2 to 10.100.11.0, with the next hop address as 129.9.0.2.
- Add the static route on NE3 to 10.100.11.0, with the next hop address as 133.168.0.2.

Figure 7-16 Direct connection mode through a router (by static routes)



Configuration Requirements

If NEs communicate with each other through IP over DCC, note the following rules for setting the network scale.

- To prevent data loss, limit the number of NE nodes in the same OSPF area to 60.
- When using the U2000 to monitor NEs, limit the number of non-GNEs monitored by one GNE to 60.

If NEs communicate with each other through IP over DCC, note the following rules for setting the IP address.

- If NEs communicate through IP addresses on the network layer, each NE need to have a unique IP address to avoid routing error due to conflict.

- NEs support standard A, B, C types of IP addresses, that is, the IP address ranges from 1.0.0.1 to 223.255.255.254. The 127.x.x.x, a loopback address, cannot be used.
- The IP address must be used with the subnet mask. The subnet mask supports consecutive masks in addition to natural masks, for example, 255.255.224.0.
- When the IP over DCC communication is used between a GNE and a non-GNE, the IP addresses can be of different network sections.
- The GNE and non-GNEs cannot be in the same IP subnet. The NEs managed through the same GNE can be in different IP subnets.
- Do not configure one GNE and one non-GNE into the same IP subnet.
- The Ethernets in the network must belong to different subnets. Otherwise, a routing error will occur in the whole network. This is not allowed.
- The subnet masks of the NEs must be the same.
- The priority of static routes is higher than that of dynamic routes. If there is a conflict, static routes take priority.

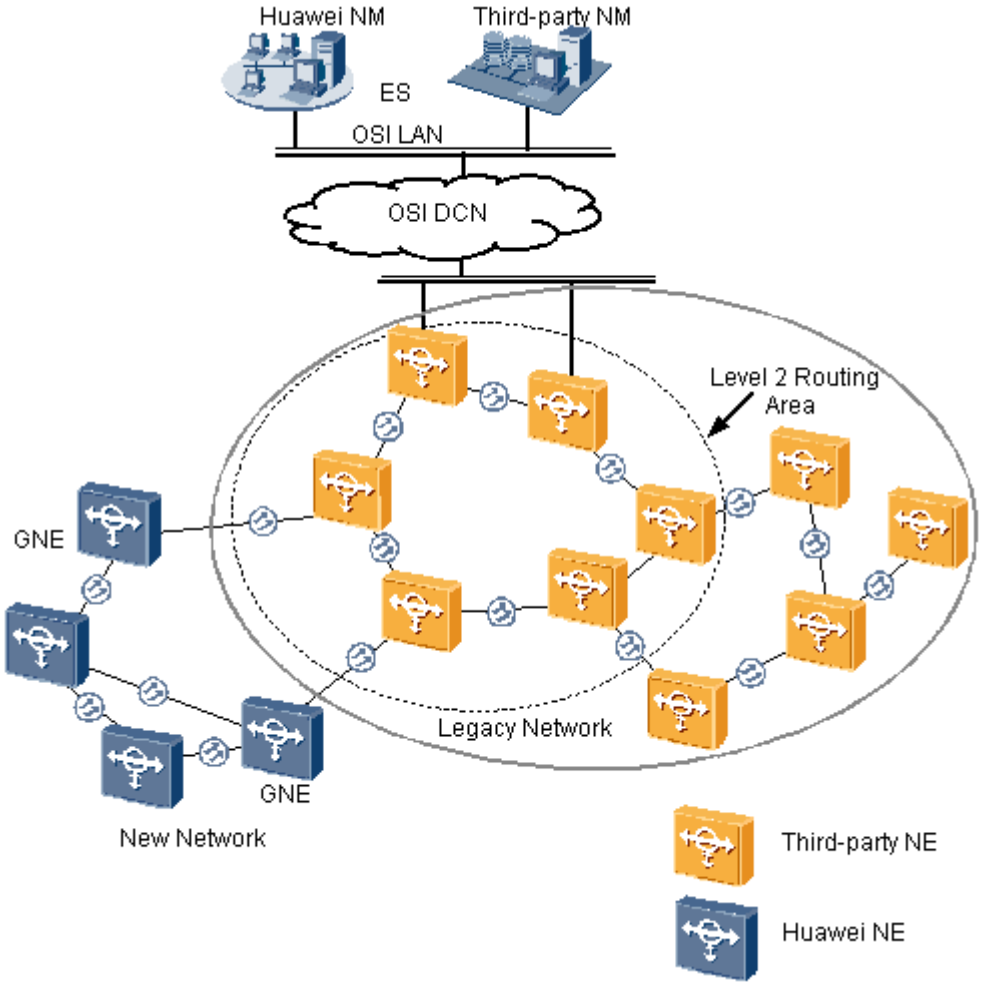
7.3.2.3 Application of OSI over DCC

According to different network situations,OSI over DCC has two major applications.

Application 1 Third-Party Equipment Forwarding OAM Information of Huawei Equipment

As shown in **Figure 7-17**, Huawei equipment locates at the edge of the network and third-party equipment locates at the core. The third-party equipment forwards the OAM information between Huawei equipment and the Huawei U2000. In this case, at least one GNE should be configured in the subnet of the Huawei equipment.

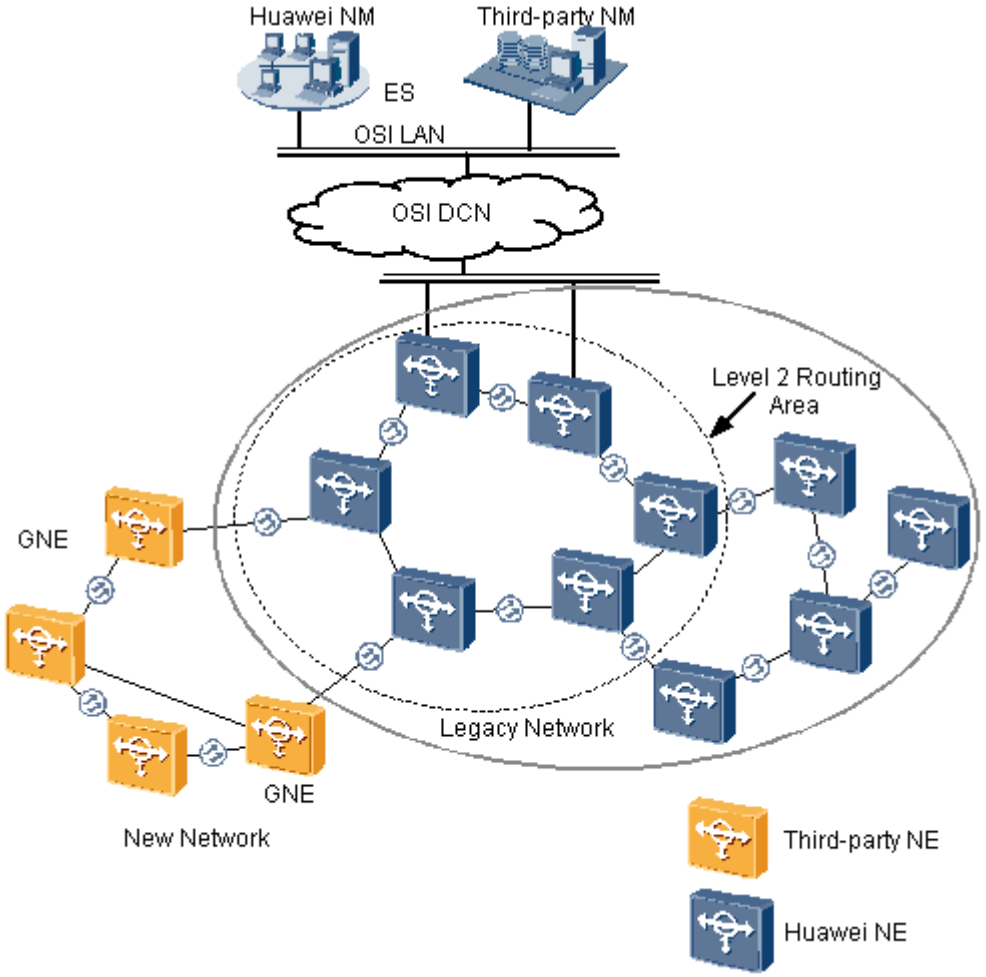
Figure 7-17 Third-party equipment forwarding OAM information of Huawei equipment



Application 2 Huawei Equipment Forwarding OAM Information of Third-Party Equipment

As shown in **Figure 7-18**, Huawei equipment locates at the core of the network while third-party equipment at the edge. Huawei equipment forwards the OAM information between the third-party NM and equipment.

Figure 7-18 Huawei equipment forwarding OAM information of third-party equipment



7.3.3 DCN Application (Between IP NEs)

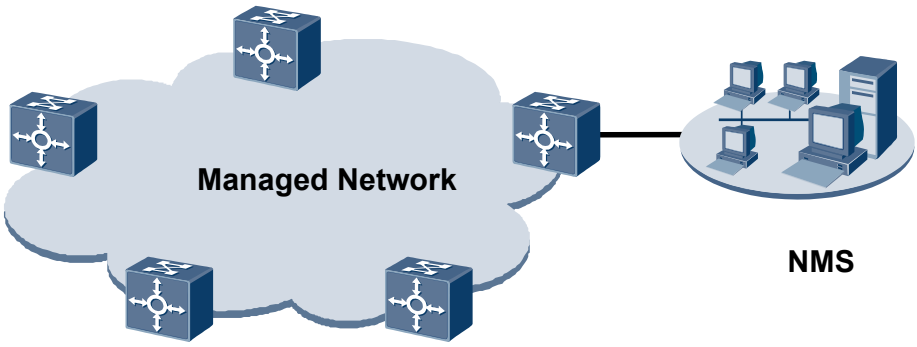
Inband or outband networking is adopted for communications between the U2000 server and managed NEs.

Inband Networking

Inband networking indicates the networking mode that the U2000 utilizes the service channels provided by managed devices to implement network management. In this mode, the NMS exchange information is transmitted through the service channels of managed devices.

Figure 7-19 shows the inband networking.

Figure 7-19 Inband networking



Networking description

NEs managed by the U2000 are connected to the managed network. U2000 can manage NEs on the managed network by connecting to the nearest NE and configuring a relevant route.

How the U2000 is connected to the managed network depends on the location relationship between the U2000 and the nearest NE. If the U2000 and the nearest NE are located in the same equipment room, LAN networking is adopted. If the U2000 and the nearest NE are distant from each other, networking through dedicated lines, which is similar to outband networking, can be adopted.

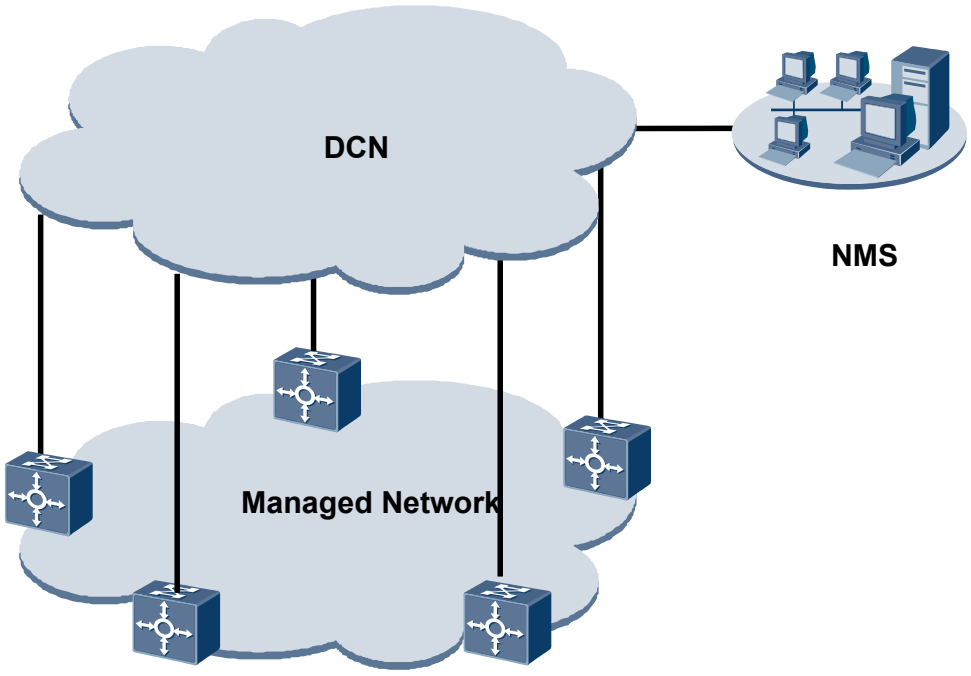
- Networking advantage: It is flexible, does not require other devices, and thus cost-effective.
- Networking disadvantage: If the network fails, maintenance through the U2000 is not supported because the information channel connecting to the managed network is interrupted.

Outband Networking

Outband networking indicates the networking mode that the U2000 utilizes the communication channels provided by the devices other than the managed devices to transmit the NMS information and implement network management. Generally, the management interfaces on the main control boards of the managed devices act as the access interfaces.

In outband networking mode, the U2000 communicates with managed devices in multiple modes. The U2000 manages devices within its management scope through a DCN. **Figure 7-20** shows outband networking.

Figure 7-20 Outband networking



Networking description

NEs managed by the U2000 are connected to the managed network. U2000 can manage the managed devices on the managed network by setting up connections with such devices through the DCN consisting of other devices.

- Networking advantage: It provides more reliable device management channels compared with the inband networking mode because the U2000 uses other devices to set up connections with the managed devices rather than directly connecting to the managed devices. If a managed device fails, the U2000 can locate the device information in time and monitor the device in real time.
- Networking disadvantage: It is not cost-effective because maintenance channels irrelevant to the service channels exist due to the need for setting up a network consisting of other devices to enable U2000 to manage the devices on the managed network.

7.3.4 DCN Application (Between Access NEs)

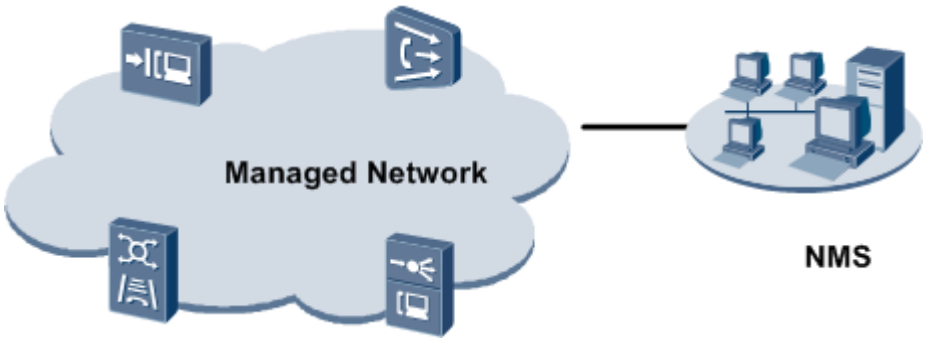
The outband or Inband U2000 is adopted for communications between the U2000 server and managed NEs.

Inband Networking

Inband networking indicates the networking mode that the U2000 utilizes the service channels provided by managed devices to implement network management. In this mode, the NMS exchange information is transmitted through the service channels of managed devices.

Figure 7-21 shows inband networking.

Figure 7-21 Inband networking



Networking description

NEs managed by the U2000 are connected to the managed network. The U2000 can manage NEs on the managed network by connecting to the nearest NE and configuring a relevant route.

How the U2000 connects to the managed network depends on the location relationship between the U2000 and the nearest NE. If the U2000 and the nearest NE are located in the same equipment room, LAN networking is adopted. If the U2000 and the nearest NE are distant from each other, networking through dedicated lines, which is similar to outband networking, can be adopted.

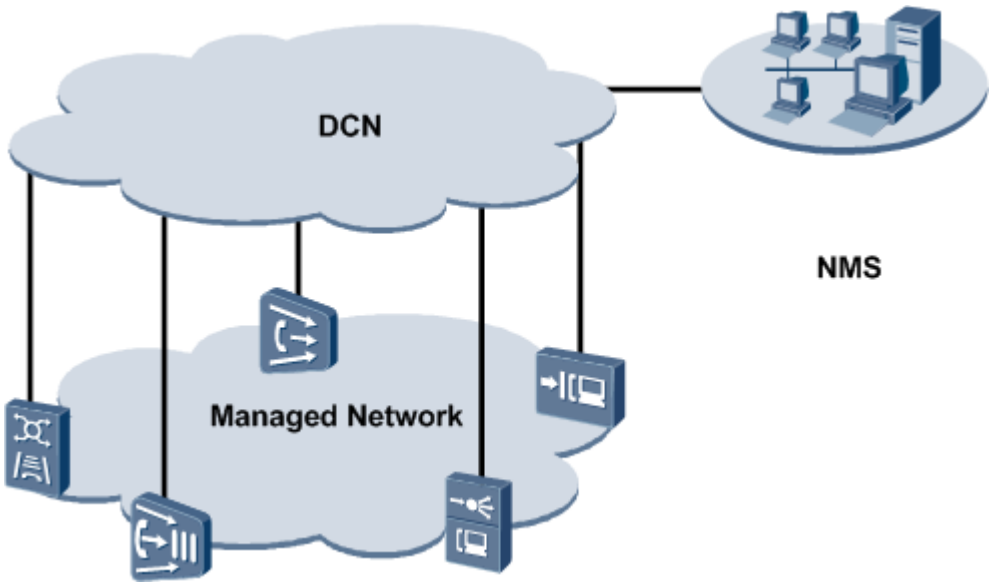
- Networking advantage: It is flexible, does not require other devices, and thus cost-effective.
- Networking disadvantage: If the network fails, maintenance through the U2000 is not supported because the information channel connecting to the managed network is interrupted.

Outband Networking

Outband networking indicates the networking mode that the U2000 utilizes the communication channels provided by the devices other than the managed devices to transmit the NMS information and implement network management. Generally, the management interfaces on the main control boards of the managed devices act as the access interfaces.

In outband networking mode, the U2000 communicates with managed devices in multiple modes. The U2000 manages devices within its management scope through a DCN. **Figure 7-22** shows outband networking.

Figure 7-22 Outband networking



Networking description

NEs managed by the U2000 are connected to the managed network. U2000 can manage the devices in the managed network by setting up connections with such devices through the DCN consisting of other devices.

- Networking advantage: It provides a more reliable device management channel compared with the inband networking mode because the U2000 utilizes other devices to set up connections with the managed devices, rather than directly connecting to the managed devices. If a managed device fails, the U2000 can locate the device information in time and monitor the device in real time.
- Networking disadvantage: It is not cost-effective because maintenance channels irrelevant to the service channels exist due to the need for setting up a network consisting of other devices to enable U2000 to manage the devices on the managed network.

7.4 Example: DCN Planning

This example describes how to perform DCN planing.

Example Description

The U2000 of a certain carrier adopts the HA system (Veritas hot standby) deployed in centralized mode. The following figure shows the U2000 topology and the DCN network connections. The DCN networking is as follows:

- Connecting the client and server of the primary site at location A in "switch" mode
- Connecting the client and server of the secondary site at location B in "switch" mode
- Connecting the primary site at location A and the secondary site at location B in "router +2M" mode

- Connecting the primary site server at location A and the remote networks in zones 1 to 4 in "router+2M" mode
- Connecting the secondary site server at location B and the remote networks in zones 1 to 4 in "router+2M" mode

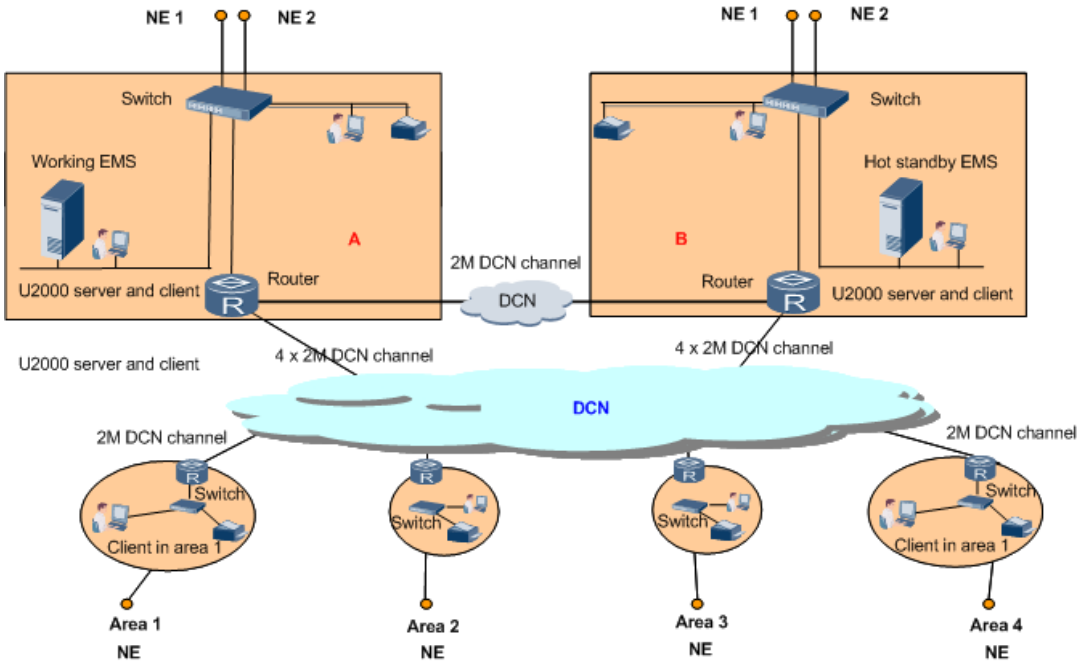
Planning Methods

1. Planning for DCN networking between the U2000 server and clients
2. Planning for DCN networking between the primary site and the secondary site of the HA system
3. Planning for DCN networking between the U2000 and managed networks

Planning Output

Figure 7-23 shows the DCN networking planned according to the planning requirement of the carrier.

Figure 7-23 Planning result based on the DCN networking diagram



Networking description

DCN networking diagram

- Connecting the primary site server at location A and the local clients in "switch" mode
- Connecting the secondary site server at location B and the local clients in "switch" mode
- Connecting the primary site at location A and the secondary site at location B in "router +2M" mode

  DCN bandwidth: 2 Mbit/s
- Connecting the primary site server at location A and the remote networks in zones 1 to 4 in "router+2M" mode

DCN bandwidth: 4 x 2 Mbit/s

- Connecting the secondary site server at location B and the remote networks in zones 1 to 4 in "router+2M" mode

  DCN bandwidth: 4 x 2 Mbit/s

- Connecting the networks in zones 1 to 4 and the U2000 server in "router+2M" mode

  DCN bandwidth: 2 Mbit/s

8 OSS Interconnection Planning

About This Chapter

The OSS is a software system based on which the following management functions of the equipment are provided to carriers: performance management, inventory management, service management, and fault management. The network layer of the OSS is above the EMS layer. Usually, the OSS manages the equipment through EMSs. The EMSs communicate with the OSS through NBIs. The U2000 supports multiple NBIs such as TL1, XML, CORBA, FTP, and SNMP to implement fast integration with the OSS provided by the carrier.

This topic describes the interconnection of the U2000 and the service diagnosis system, especially for XML.

8.1 Introduction to the OSS

The OSS is an independent software system that is used to enhance the work efficiency of equipment maintenance engineers. According to its different functions, the OSS is classified into the service assurance system, service provisioning system, inventory management system, and service diagnosis system.

The OSS reduces the maintenance costs and enhances the maintenance efficiency.

Table 8-1 lists the features of different OSSs.

Table 8-1 Features of different OSSs

OSS	Feature	Description
Service assurance system	Monitoring and assurance of the system performance	Provides unified ports for performance measurement and supports the performance statistics reports for various services. Supports the ability to report equipment alarms in real time, and filter and clear equipment alarms.
Service provisioning system	Fast service provisioning	Supports unified provisioning flow for various services and screens the differences of the equipment provided by different vendors.
Inventory management system	Unified resource management	Implements the functions of the inventory query for network wide resources and the resource change notification.

8.2 NBI Type

The U2000 provides various NBIs to the network management layer. This helps the U2000 to connect to different NMSs.

Table 8-2 lists the U2000 NBIs provided to the network management layer.

Table 8-2 List of U2000 NBIs

Interface Type	Function
XML NBI	Through the XML NBI, the U2000 provides unified management for alarms, performance, inventory, and service provisioning to the OSS. This NBI supports the equipment of router, Metro, transport, and access domains.

Interface Type	Function
CORBA NBI	● Through the CORBA NBI, the U2000 provides unified management for alarms to the OSS. This NBI supports the equipment of router, Metro, transport, and access domains. ● Through the CORBA NBI, the U2000 provides management for performance, inventory, and service provisioning for the equipment of Metro and transport domains.
SNMP alarm NBI	Through the SNMP alarm NBI, the U2000 provides management for alarms to the OSS. This NBI supports the equipment of router, Metro, transport, and access domains.
TL1 NBI	Through the TL1 NBI, the U2000 provides the functions of service provisioning (xDSL, xPON, broadband, and narrowband services), inventory query, and inventory provisioning to the OSS.
FTP performance NBI	Through the FTP performance NBI, the U2000 provides the function of exporting performance data to the specified FTP server for analysis by the OSS.
MML test NBI	The U2000 can access an OSS test system, and can support tests on narrowband access devices (lines and terminals) and ADSL lines through the OSS test NBI.

8.3 NBI Interconnection Capability

This topic describes performance indicators of each type of NBI to provide reference during the interconnection with the OSS.

XML NBI

Table 8-3 shows the performance indicators of each XML NBI.

Table 8-3 Performance indicators of an XML NBI

Item	Indicator
Number of NMS connections received concurrently	10
Delay of response to XML request	Less than 3 s when CPU usage is lower than 50%
Alarm notification processing capability	No less than 60 records per second when 3 NMSs are connected
Alarm notification transmission delay	Less than 10 s when 3 NMSs are connected

CORBA NBI

Table 8-4 shows the performance indicators of each CORBA NBI.

Table 8-4 Performance indicators of a CORBA alarm NBI

Item	Indicator
Number of NMS connections received concurrently	10
Delay of response to CORBA request	Less than 3 s when CPU usage is lower than 50%
Alarm notification processing capability	No less than 40 records per second when 3 NMSs are connected
Alarm notification transmission delay	Less than 10 s when 3 NMSs are connected

SNMP Alarm NBI

Table 8-5 shows the performance indicators of each SNMP alarm NBI.

Table 8-5 Performance indicators of an SNMP alarm NBI

Item	Indicator
Number of NMS connections received concurrently	10
Alarm forwarding capability	No less than 60 records per second when 3 NMSs are connected
Alarm forwarding delay	Less than 10 s when 3 NMSs are connected
Delay of response to SNMP request	Less than 5 s when CPU usage is lower than 50%

FTP Performance NBI

Table 8-6 shows the performance indicators of each FTP performance NBI.

Table 8-6 Performance indicators of an FTP performance NBI

Item	Indicator
Number of NMS connections received concurrently	3

TL1 Service Provisioning NBI

Table 8-7 shows the performance indicators of each TL1 service provisioning NBI.

Table 8-7 Performance indicators of a TL1 service provisioning NBI

Item	Indicator
Maximum number of TCP connections received concurrently	15
Capability of processing TL1 request command	10 records per second for commands of the configuration type. This item does not depend on the number of TCP connections.
Time of response to TL1 request command	Within 2 minutes (commands of the test type are excluded)

MML Test NBI

Table 8-8 shows the performance indexes of the MML test NBI.

Table 8-8 Performance indexes of the MML test NBI

Item	Index
Maximum number of concurrent EMS connections	64
Connection duration	After a TCP/IP connection is established, if the client does not deliver any test command in one hour, the connection releases automatically.

8.4 Interconnection Planning of the Service Assurance System

This topic describes four schemes of interconnection between the U2000 and the service assurance system: SNNP alarm NBI, CORBA alarm NBI, XML alarm NBI, and FTP performance NBI.

8.4.1 Interconnection Between the XML NBI and the Service Assurance System
Through the XML alarm NBI, the U2000 forwards alarms to the upper-layer NMS or the third-party NMS. In addition, the U2000 provides the functions, such as filtering alarms by equipment type, alarm type, or alarm severity, and subscribing, acknowledging, clearing, or obtaining real-time alarms.

8.4.2 Interconnection Between the SNMP NBI and the Service Assurance System
The SNMP alarm NBI provides the function of reporting alarms in real time. Through this function, the upper layer NMS can set the Trap of real-time alarms, set the filtering criteria of the Trap of real-time alarms, and receive the Trap of real-time alarms through the event receiving port. In this manner, the U2000 monitors alarms in a centralized manner. This topic mainly describes the SNMP standard and security mechanism supported by the U2000 and the interfaces provided by the U2000.

8.4.3 Interconnection Between the CORBA NBI and the Service Assurance System
Through the CORBA alarm NBI, the U2000 forwards alarms to the upper layer NMS or the third-party NMS. In addition, the U2000 provides the functions, such as filtering alarms by equipment type, alarm type, or alarm severity, and subscribing, acknowledging, clearing, or obtaining real-time alarms.

8.4.4 Interconnection Between the FTP Performance NBI and the Service Assurance System
The FTP performance NBI supports the ability to generate a performance data to the specified directory. An upper layer NMS or a third-party NMS can obtain performance data files through FTP for analysis and use.

8.4.1 Interconnection Between the XML NBI and the Service Assurance System

Through the XML alarm NBI, the U2000 forwards alarms to the upper-layer NMS or the third-party NMS. In addition, the U2000 provides the functions, such as filtering alarms by equipment type, alarm type, or alarm severity, and subscribing, acknowledging, clearing, or obtaining real-time alarms.

The U2000 XML alarm NBI complies with the following standards suggested by TeleManagement Forum (TMF) MTOSI V2.0:

- TMF 518 MTOSI Business Agreement
- TMF 612 MTNM Information Agreement
- TMF 864 MTOSI Solution Set

The U2000 XML alarm NBI has the following technical characteristics:

- Supporting HTTP and JMS standard protocols.
- Using standard JMS middleware. Currently, the provided version is implemented through ActiveMQ.
- Migrating smoothly to other JMS middleware. The JMS message middleware, such as OpenJMS, is supported.

The XML alarm NBI supports the following functions:

- Querying current alarms: It supports the ability to query current alarms of all NEs or the specified NE.
- Subscribing alarm events: It supports the ability to subscribe alarms by condition, such as alarm name and alarm level.
- Filtering alarms and events: It supports the ability to customize alarms and events, such as alarm name and alarm level.
- Reporting alarms: It supports the ability to report alarms in real time.
- Confirming alarms: It supports the ability to confirm alarms through the centralized monitoring system at the upper layer.

8.4.2 Interconnection Between the SNMP NBI and the Service Assurance System

The SNMP alarm NBI provides the function of reporting alarms in real time. Through this function, the upper layer NMS can set the Trap of real-time alarms, set the filtering criteria of the Trap of real-time alarms, and receive the Trap of real-time alarms through the event receiving

port. In this manner, the U2000 monitors alarms in a centralized manner. This topic mainly describes the SNMP standard and security mechanism supported by the U2000 and the interfaces provided by the U2000.

The SNMP protocol that is widely accepted and used is an industrial standard of the NMS protocol. It aims to ensure that the management information can be transmitted between any two points. Therefore, it is easy for a network administrator to search information, modify information, and locate faults on any node in the network. In addition, the SNMP protocol can implement fault diagnosis, capacity planning, and report generating. Until now, the SNMP protocol has three main versions: V1, V2c, and V3. Therefore, the SNMP alarm NBI of the U2000 supports the following protocols: SNMPv1, SNMPv2c, and SNMPv3.

The SNMP alarm NBI of the U2000 uses the security mechanism of the SNMP protocol. Any access to the SNMP alarm NBI must pass the authentication controlled by the security mechanism of the SNMP protocol. The SNMPv1 and the SNMPv2c use the security mechanism based on community name. The SNMPv3 uses the security mechanism based on user. During the SNMP interaction, the mechanisms of authentication and encryption are used. This prevents the packets from being intercepted and modified. Compared with the SNMPv1 and SNMPv2c protocols, the SNMPv3 has a higher security level.

For the ease of the upper layer NMS to timely and accurately obtain the information about real-time alarms on the equipment, the SNMP NBI of the U2000 provides the function of reporting real-time fault alarms to the upper layer NMS. In addition, the U2000 supports the heartbeat mechanism between the SNMP NBI and the OSS to ensure the reliability of the connection. Though this interface, the following functions can be implemented:

- Reporting Fault Alarms in Real-Time
- Querying Current Alarms
- Alarm handshaking and Caching

8.4.3 Interconnection Between the CORBA NBI and the Service Assurance System

Through the CORBA alarm NBI, the U2000 forwards alarms to the upper layer NMS or the third-party NMS. In addition, the U2000 provides the functions, such as filtering alarms by equipment type, alarm type, or alarm severity, and subscribing, acknowledging, clearing, or obtaining real-time alarms.

The specific standards that the CORBA alarm NBI of the U2000 complies with and the TeleManagement Forum (TMF) recommends are as follows:

- TMF 513 MTNM Business Agreement
- TMF 608 MTNM Information Agreement
- TMF 814 MTNM CORBA Solution Set
- TMF 814A MTNM Implementation Statement

The CORBA alarm NBI of the U2000 has the following technical features:

- It completely complies with the Object Management Group (OMG) CORBA 2.3 specifications and supports the Internet Inter-ORB Protocol (IIOP)1.1 and IIOP1.2 protocols.
- It uses the standard CORBA Naming Service1.1 and Notification Service1.0. The current version is implemented by using the TAO (The ACE ORB) and thus is highly efficient. TAO is a widely applauded free Object Request Broker (ORB) product. Therefore, the

CORBA alarm NBI has a great advantage in cost. Users can enjoy a high cost performance ratio.

- It can be smoothly migrated to other ORB platforms. It supports interworking between different ORB platforms, currently including the IONA Orbix2000, IONA Orbix 6.1, InterBus, JacORB, Borland VisiBroker, and Borland BES.

The CORBA alarm NBI provides the following functions:

- Querying current alarms: It supports the ability to query current alarms of all NEs or the specified NE.
- Subscribing alarm events: It supports the ability to subscribe alarms by condition, such as alarm name and alarm level.
- Filtering alarms and events: It supports the ability to customize alarms and events, such as alarm name and alarm level.
- Reporting alarms: It supports the ability to report alarms in real time.
- Confirming alarms: It supports the ability to confirm alarms through the centralized monitoring system at the upper layer.

8.4.4 Interconnection Between the FTP Performance NBI and the Service Assurance System

The FTP performance NBI supports the ability to generate a performance data to the specified directory. An upper layer NMS or a third-party NMS can obtain performance data files through FTP for analysis and use.

The FTP performance NBI uses the FTP protocol to transmit performance data files.

The main functions of the FTP performance NBI are as follows:

- Customizing performance data: You can customize performance data concerned by the upper layer NMS or the third-party NMS.
- Exporting NBI files periodically: The system can generate NBI files for collected performance data periodically to the specified directory. The NBI files generated are in the CSV format. You can customize the period of generating NBI files.
- Deleting outdated data files automatically: The system can detect and delete outdated data files according to the setting. This operation deletes the outdated files with the saving time expired and their directories.

8.5 Interconnection Planning of the Service Provisioning System

This topic describes the schemes of interconnection between the U2000 and the service provisioning system, including XML NBI, CORBA NBI, and TL1 NBI.

The U2000 XML NBI provides unified IP service provisioning interfaces to the upper layer NMS or the third-party NMS in the router and Metro domains. The U2000 XML NBI supports the ability to provision and manage services, including ATM emulation services, TDM emulation services, EPL services, EPLn services, and MPLS VPN services.

The U2000 CORBA service provisioning NBI supports the ability to provision and maintain various services, including SDH, WDM, RTN, MSTP, ASON, and PTN services, of transport and Metro domains.

8.5.3 Interconnection Between the TL1 NBI and the Service Provisioning System
The U2000 TL1 NBI supports the ability to provision and maintain various types of services, including xDSL services, video services, GPON services, and VoIP services. The OSS system is developed based on this interface for the second time to automatically handle services.

8.5.1 Interconnection Between the XML NBI and the Service Provisioning System

The U2000 XML NBI provides unified IP service provisioning interfaces to the upper layer NMS or the third-party NMS in the router and Metro domains. The U2000 XML NBI supports the ability to provision and manage services, including ATM emulation services, TDM emulation services, EPL services, EPLn services, and MPLS VPN services.

The U2000 XML NBI complies with the following standards suggested by TeleManagement Forum (TMF) MTOSI V2.0:

- TMF 518 MTOSI Business Agreement
- TMF 612 MTNM Information Agreement
- TMF 864 MTOSI Solution Set

The U2000 XML alarm NBI has the following technical characteristics:

- Supporting HTTP and JMS standard protocols.
- Using standard JMS middleware. Currently, the provided version is implemented through ActiveMQ.
- Migrating smoothly to other JMS middleware. The JMS message middleware, such as OpenJMS, is supported.

The XML service provisioning NBI provides the following functions:

- Provisioning of MPLS tunnels
- Provisioning of IP tunnels
- Provisioning of ATM emulation services
- Provisioning of TDM emulation services
- Provisioning of EPL services
- Provisioning of EPLn services
- Provisioning of MPLS VPN services
- Ed-to-end service provisioning (FTTH GPON)

8.5.2 Interconnection Between the CORBA NBI and the Service Provisioning System

The U2000 CORBA service provisioning NBI supports the ability to provision and maintain various services, including SDH, WDM, RTN, MSTP, ASON, and PTN services, of transport and Metro domains.

The U2000 CORBA service provisioning NBI complies with the following standards suggested by TeleManagement Forum (TMF):

- TMF 513 MTNM Business Agreement
- TMF 608 MTNM Information Agreement
- TMF 814 MTNM CORBA Solution Set

The CORBA service provisioning NBI has the following technical characteristics:

- It completely complies with the Object Management Group (OMG) CORBA 2.3 specifications and supports the Internet Inter-ORB Protocol (IIOP)1.1 and IIOP1.2 protocols.
- It uses the standard CORBA Naming Service1.1 and Notification Service1.0. The current version is implemented by using the TAO (The ACE ORB) and thus is highly efficient. TAO is a widely applauded free Object Request Broker (ORB) product. Therefore, the CORBA alarm NBI has a great advantage in cost. Users can enjoy a high cost performance ratio.
- It can be smoothly migrated to other ORB platforms. It supports interworking between different ORB platforms, currently including the IONA Orbix2000, IONA Orbix 6.1, InterBus, JacORB, Borland VisiBroker, and Borland BES.

The CORBA NBI provides the following service provisioning and management functions:

- Provisioning of SDH end-to-end services
- Provisioning of WDM end-to-end services
- Provisioning of SDH ASON end-to-end services
- Provisioning of WDM ASON end-to-end services
- Provisioning of MSTP end-to-end services (configuration of EPL, EVPL, EPLan, and ELL)
- Provisioning of SDH single-station services (configuration of SDH cross-connection)
- Provisioning of WDM single-station services (configuration of WDM cross-connection)
- Provisioning of MSTP single-station services (configuration of ATM cross-connection, ETH cross-connection, VB, and VLAN)
- Provisioning of PTN single-station services (configuration of MPLS tunnel, IP tunnel, ATM emulation service, TDM emulation service, EPL service, EPLn service, and MPLS VPN service)

8.5.3 Interconnection Between the TL1 NBI and the Service Provisioning System

The U2000 TL1 NBI supports the ability to provision and maintain various types of services, including xDSL services, video services, GPON services, and VoIP services. The OSS system is developed based on this interface for the second time to automatically handle services.

The TL1 NBI complies with the Generic Requirements (GR) 831 standard.

Currently, the TL1 NBI provides the following functions:

- Provisioning of xDSL services, including ADSL, SHDSL, and VDSL2 services
- Provisioning of multicast services
- Provisioning of xPON services
- Ethernet port management
- VLAN management
- Service virtual port/PVC connection management

- Traffic profile management
- ACL&QoS management
- Provisioning of voice services
- Provisioning of BRAS services

8.6 Interconnection Planning of the Inventory Management System

This topic describes the schemes of interconnection between the U2000 and the inventory management system, including XML NBI, CORBA NBI, and TL1 NBI.

8.6.1 Interconnection Between the XML NBI and the Inventory Management System
The U2000 XML NBI supports the functions, including query of physical and logical resources, resource change notification, and resource management and maintenance. This NBI is used for the interconnection with the inventory management system to manage network resources in a centralized manner.

8.6.2 Interconnection Between the CORBA NBI and the Inventory Management System
The U2000 CORBA NBI supports the functions, including query of resources in transport and Metro domains, resource change notification, and resource management and maintenance. This NBI is used for the interconnection with the inventory management system to manage network resources in a centralized manner.

8.6.3 Interconnection Between the TL1 NBI and the Inventory Management System
The U2000 TL1 NBI supports the functions including query of resources in access domain, resource change notification, and resource management and maintenance. This NBI is used for the interconnection with the inventory management system to manage network resources in a centralized manner.

8.6.1 Interconnection Between the XML NBI and the Inventory Management System

The U2000 XML NBI supports the functions, including query of physical and logical resources, resource change notification, and resource management and maintenance. This NBI is used for the interconnection with the inventory management system to manage network resources in a centralized manner.

The U2000 XML NBI complies with the following standards suggested by TeleManagement Forum (TMF) MTOSI V2.0:

- TMF 518 MTOSI Business Agreement
- TMF 612 MTNM Information Agreement
- TMF 864 MTOSI Solution Set

The U2000 XML inventory NBI has the following technical characteristics:

- Supporting HTTP and JMS standard protocols.
- Using standard JMS middleware. Currently, the provided version is implemented through ActiveMQ.
- Migrating smoothly to other JMS middleware. The JMS message middleware, such as OpenJMS, is supported.

The XML NBI supports the following inventory management functions:

- Query of physical resources
  - NEs, subracks, slots, cards, ports, and topology links
- Query of logical resources
  - Logical ports, including serial ports, MP group ports, IMA ports, and LAG ports
  - Tunnels, including MPLS tunnels and IP tunnels
  - Service resources, including ATM emulation services, TDM emulation services, EPL services, EPLn services, and MPLS VPN services
- Resource change notification
  - When resources on the U2000 change, to ensure that the upper layer NMS can take measures to the impact caused by the change, the U2000 XML NBI actively notifies the change to the upper layer NMS. The notification contents include the creation, modification, and deletion of resources.

8.6.2 Interconnection Between the CORBA NBI and the Inventory Management System

The U2000 CORBA NBI supports the functions, including query of resources in transport and Metro domains, resource change notification, and resource management and maintenance. This NBI is used for the interconnection with the inventory management system to manage network resources in a centralized manner.

The U2000 CORBA service provisioning NBI complies with the following standards suggested by TeleManagement Forum (TMF):

- TMF 513 MTNM Business Agreement
- TMF 608 MTNM Information Agreement
- TMF 814 MTNM CORBA Solution Set

The CORBA service provisioning NBI has the following technical characteristics:

- It completely complies with the Object Management Group (OMG) CORBA 2.3 specifications and supports the Internet Inter-ORB Protocol (IIOP)1.1 and IIOP1.2 protocols.
- It uses the standard CORBA Naming Service1.1 and Notification Service1.0. The current version is implemented by using the TAO (The ACE ORB) and thus is highly efficient. TAO is a widely applauded free Object Request Broker (ORB) product. Therefore, the CORBA alarm NBI has a great advantage in cost. Users can enjoy a high cost performance ratio.
- It can be smoothly migrated to other ORB platforms. It supports interworking between different ORB platforms, currently including the IONA Orbix2000, IONA Orbix 6.1, InterBus, JacORB, Borland VisiBroker, and Borland BES.

The CORBA NBI provides the following resource management functions:

- Query of physical resources
  - NEs, subracks, slots, cards, ports, and topology links
- Query of logical resources
  - SDH resources, including SDH CTP, SDH cross-connection, SDH trail, and SDH protection group

  - WDM resources, including WDM CTP, WDM cross-connection, WDM trail, and WDM protection group
  - SDH ASON resources, including SNPPLink, SDH ASON trail, and SDH ASON cross-connection
  - OTN ASON resources, including SNPPLink, OTN ASON trail, and OTN ASON cross-connection
  - MSTP resources, including encapsulation layer link, EPL trail, EVPL trail, EPLan trail, ATM cross-connection, ETH cross-connection, VB, and VLAN
  - Metro resources, including MPLS tunnel, IP tunnel, ATM emulation service, TDM emulation service, EPL service, EPLn service, and MPLS VPN service
- Resource change notification
  - When resources on the U2000 change, to ensure that the upper layer NMS can take measures to the impact caused by the change, the U2000 CORBA NBI actively notifies the change to the upper layer NMS. The notification contents include the creation, modification, and deletion of resources.

8.6.3 Interconnection Between the TL1 NBI and the Inventory Management System

The U2000 TL1 NBI supports the functions including query of resources in access domain, resource change notification, and resource management and maintenance. This NBI is used for the interconnection with the inventory management system to manage network resources in a centralized manner.

Currently, the TL1 NBI provides the following inventory management functions:

- Resource query: The TL1 NBI supports the function of querying various resources, such as devices, xDSL resources (including ADSL, G.SHDSL, and VDSL2 resources), video resources, xPON resources (including GPON and EPON resources), VoIP resources, ACL and QoS Resources.
- Resource change notification: The TL1 NBI supports the ability to enable or disable resource change notification. You can set this function for NEs, shelves, and cards respectively.
- Resource management and maintenance: The TL1 NBI supports the ability to maintain (add, delete, reset, or modify alias for) NEs and cards. You can set IP addresses and synchronization time for NEs, and export resources on the specified NE to a file.

8.7 Interconnection Planning of the Service Diagnosis System

This topic describes the interconnection of the U2000 and the service diagnosis system, especially for XML.

This section describes the interconnection of the MML NBI of the U2000 and the service diagnosis system. For the access devices, the means that is widely used for service diagnosis is the line test.

8.7.1 Interconnection of the MML NBI and the Service Diagnosis System

This section describes the interconnection of the MML NBI of the U2000 and the service diagnosis system. For the access devices, the means that is widely used for service diagnosis is the line test.

Multiple access devices can be managed by an U2000. In addition, the U2000 provides the MML interfaces for interconnecting with the centralized test management system. In this way, the narrowband line test and the ADSL line test can be realized. According to different types of test devices, the U2000 provides the following line test solutions:

- Test board (TSS board)
- External test unit
- Integrated test

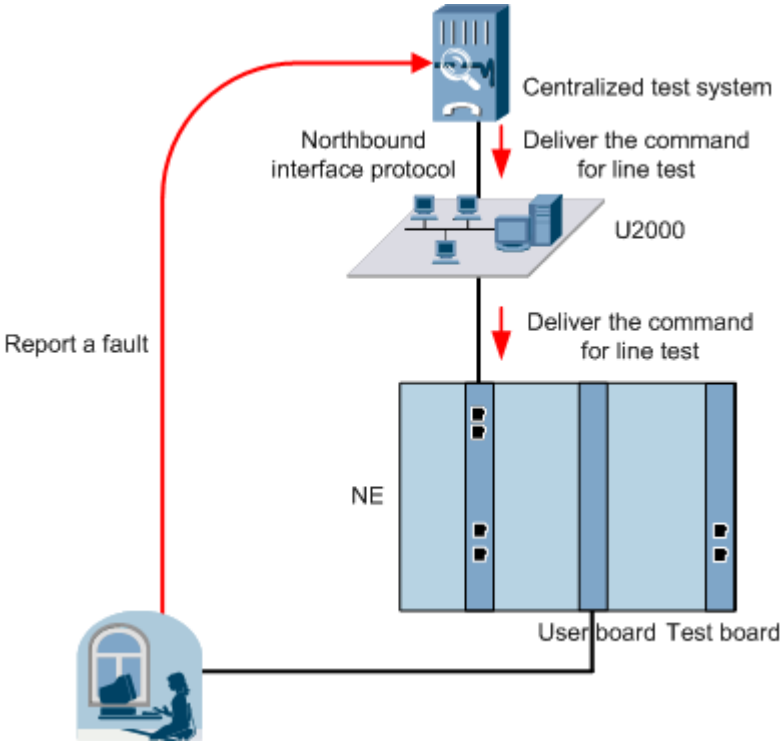
For narrowband line tests, the test board solution is widely used. For DSLAM devices, the solution of the external test unit is widely used.

Test Board

In this solution, the embedded test board (TSS board) of the device is used for the narrowband test tasks. **Figure 8-1** shows the networking of the test board solution. When receiving the fault from a user, the centralized test management system sends test commands to the U2000. Then, the U2000 performs the test through the test board of the device. The features of this networking are as follows:

- The embedded test board is fully utilized. No additional test devices are needed. This reduces the cost.
- The precision and rate of the test can meet the requirements of general users.

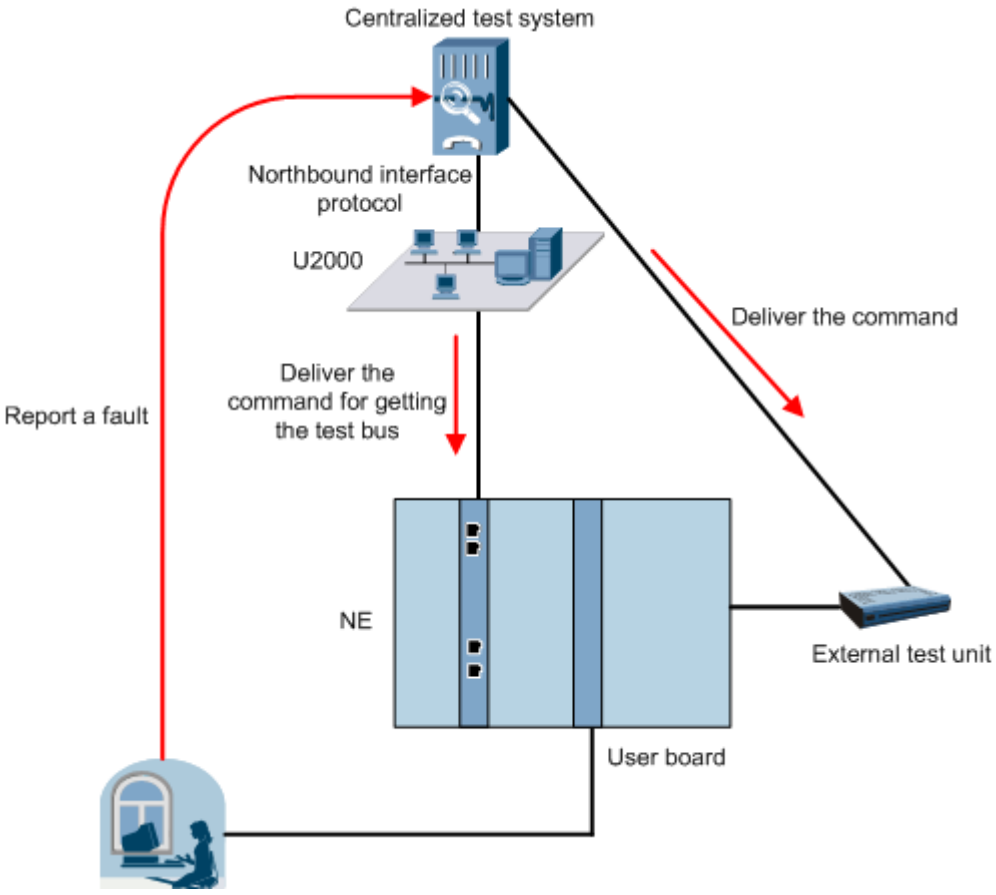
Figure 8-1 Networking of the test board solution



External Test Unit

Figure 8-2 shows the networking of the external test unit solution. The centralized test system connects the specified user loop line to the test bus of a device through the U2000. At the same time, the centralized test system sends test commands to the external test unit to perform the test. The external test unit solution features complete test functions and fast test rate.

Figure 8-2 Networking of the external test unit solution



NOTE

This solution can also be realized through the external line capture module. In this case, the U2000 does not need to provide any port. The line capture module is directly controlled by the centralized test management system.

Integrated Test

In the integrated test solution, both an external test unit and a test board are used for a line test. In this case, the centralized test management system checks whether the test device corresponding to the test user is an external test unit or a test board first, and then the line test is performed accordingly.

9 Security and Reliability Planning

About This Chapter

Security and reliability planning is recommended to ensure the secure running of the U2000.

9.1 System Security Planning
The U2000 ensures that the right person performs the right O&M operations to the telecom network at the right place and at the right time. In addition, the telecom administration signals must be intact and encrypted in transmission, and the system must be immune to malicious attacks to ensure a secure running environment.

9.2 Security Planning of the Database
The database is a key component of the management system to store and calculate data including secret data. The database has its own requirements on security. Using and maintaining the database properly is a key aspect of the security of the U2000. The database security involves the security of database users, and the security of storage and backup of database files.

9.3 Operation Security
The reliability of operation security involves the designs of rights control, ACL control, time control, limit to login times, user monitoring, and operation confirmation.

9.4 Security Planning of U2000 Users
When planning the U2000 users, you need to refer to the principles of the security planning to ensure the security of the U2000 users.

9.5 Security Planning of NE Users
An NE user refers to the one that maintains an NE through the NE management interface. The U2000 provides the NE users management and local command terminal (LCT) users management functions to manage NE users in a centralized manner. When planning the NE users, you need to refer to the principles of the security planning to ensure the security of the NE users.

9.6 Security Planning of Data Transmission
The U2000 data is transmitted in the system (for example, between the system server and clients) or between the U2000 and the external systems (such as the telecommunications equipment and the OSS). The data transmission requires privacy and integrity. Therefore, ensure that the data transmission is not intercepted, and external networks cannot directly access the internal network

of carriers. In addition to the security of the OS, database, and application system, the security during data transmission should also be considered.

9.1 System Security Planning

The U2000 ensures that the right person performs the right O&M operations to the telecom network at the right place and at the right time. In addition, the telecom administration signals must be intact and encrypted in transmission, and the system must be immune to malicious attacks to ensure a secure running environment.

9.1.1 OS Protection Policies

OS security is the basis for the normal running of the U2000. To ensure OS security, it is recommended that you perform the following planning.

9.1.1.1 Firewall Security Policy

Firewall is an important security measure for the U2000. The firewall can provide various security functions, such as package filtering. The firewall monitors the access channel between the reliable network (internal network) and the non-reliable network (external network). This

protects the internal network and data from illegal access (unauthorized and unauthenticated access) and malicious attacks from external networks.

You can deploy U2000 clients in the public network so that different levels of maintenance engineers from carriers can log in to the U2000 conveniently. You can deploy U2000 servers and equipment in the private network. The clients cannot directly access equipment. All the access must go through the U2000 server. The U2000 server and equipment are protected by the firewall. This can effectively prevent illegal network access and attacks.

Using the firewall for isolation is a good solution to the security protection at the network layer.

In the security policy of the firewall, you must filter the traffic according to the IP address and the Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) port number. Disabling unused U2000 ports on the firewall according to **6.6 U2000 Port List** is recommended.

9.1.1.2 System Strengthening

This topic describes the security customization tool SetSolaris that protects the OS.

The SetSolaris is a security customization tool used for a single-server system that runs in the Solaris OS. It can be used to improve the security of the Solaris OS and ensure the normal running of the server computer. The SetSolaris is installed on a protected server, and provides the execution policies and customized scripts that are used to improve the security of the OS. The SetSolaris implements the required customization and system configuration through customized policies. The execution of the policies protects the server computer.

NOTE

The SetSolaris is applicable to Solaris 8 or later versions. Currently, Solaris 7 and earlier versions do not support the policy customization.

9.1.1.3 Antivirus

The Windows OS is vulnerable to virus. Once the Windows OS is attacked by virus, the U2000 does not run properly and even the entire system will break down. Therefore, antivirus planning is recommended to ensure proper running of the U2000.

Antivirus Planning Rules

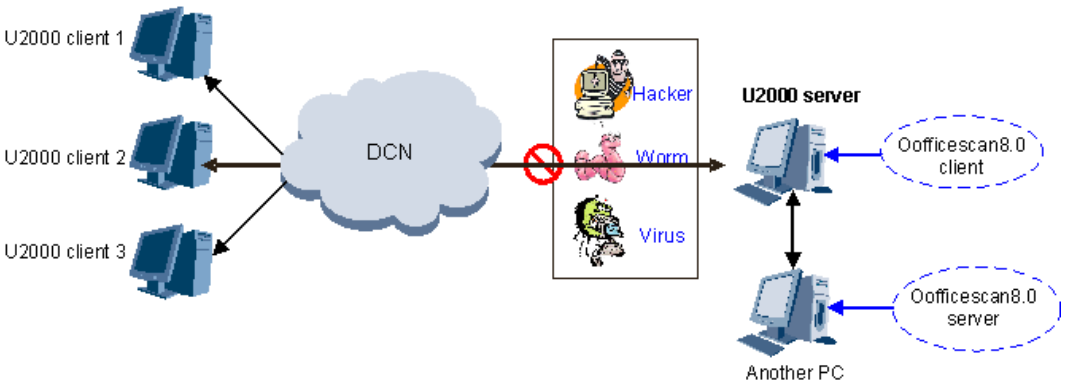
- Designated computer principle: Using a designated computer to install and run the U2000 (including the server and client) is recommended. This computer must be separated from other office computers. Using a U2000 computer to act as an email server or handle emails from a public network is not recommended.
- Minimum installation principle: Installation of mandatory system applications and auxiliary tools only on the computer that runs the U2000 is recommended. Do not install software downloaded from unauthorized Web sites, unofficial software releases, software for testing, or any unnecessary applications of any kind.

Antivirus Software Selection

Multiple types of antivirus software are available for the Windows OS. The Officescan8.0 SP1 is recommended, which is strictly tested and compatible with the U2000.

The Officescan8.0 SP1 uses the C/S structure and supports the installation of the Officescan8.0 server and client on the same computer or different computers. Installing the Officescan8.0 client on the U2000 server and the Officescan8.0 server on an independent computer is recommended.

Figure 9-1 Officescan8.0 deployment example



9.1.2 Security Planning of the OS

The U2000 runs on common OSs. Usually, the default settings of the OSs cannot meet the security requirements of the telecommunications management system. For example, the OSs may run a large number of unnecessary services, or open unnecessary ports that communicate with the external networks. This is the weak point of the whole management system and requires enhanced default security settings.

The security planning of the OS covers the following areas:

- Enhance the security management of the OS users according to the telecommunications O&M requirements. The OS users include those created after the U2000 is installed.
- The file system of the OS requires high secrecy and security to avoid illegal modification and unauthorized reading and copying.
- The services and ports that the OS provides to external networks must be customized to avoid an unstable system or deny of service (DoS) attacks caused by unnecessary or defective services.

9.1.2.1 Solaris OS Security
This topic describes the security policy of the Solaris OS.

9.1.2.2 SUSE Linux OS Security
This topic describes the security policy of the SUSE Linux OS.

9.1.2.3 Windows OS Security
This topic describes the security policy of the Windows OS.

9.1.2.1 Solaris OS Security

This topic describes the security policy of the Solaris OS.

OS User Security

After the Solaris OS, Sybase database and the U2000 are successfully installed on a server, the following OS users are generated:

- **root**: The **root** user is the default administrator of the Solaris OS. With the highest administrative rights, the **root** user can control all resources, create other users, assign rights to these users, and perform all the operations supported by the OS.
- **nmsuser**: During the installation of the U2000, the **nmsuser** user is automatically created by the U2000 as an OS user. The **nmsuser** user can set the environment variables of the U2000 server and start the U2000 client on the server. The **nmsuser** user has all the rights to edit the **/nmsuser** directory. The **.profile** file in this directory records the environment variables of the U2000.
- **sybase**: During the installation of the NMS, the Sybase database is automatically installed and the OS user **sybase** is automatically created. The **sybase** user can set the environment variables of the Sybase database, install the Sybase software, and manage and maintain the Sybase database. The **sybase** user has all rights to edit the Sybase database installation directory (**/opt/sybase**) only. You can use this user account to manage the Sybase database, for example, configuring the running environment variables of the Sybase, and start or stop the Sybase service.

Assign the three accounts to different users based on the actual situation. In addition, follow the security principles of the user name and password, and change the password regularly (such as every three months).

If the U2000 needs to provide the external file transfer protocol (FTP) service, such as file transfer for performance data collection, you must add an FTP user manually on the OS. For security purposes, an independent path of the FTP file system is required for an FTP user to prevent the access of the non-FTP file systems. In addition, set a password for the FTP user, and change the password regularly as required.

OS File Security

By checking and strengthening the read and write rights of the OS files, the system checks the correctness and necessity of the core files, prevents unauthorized access to the key OS files (such as the password file), and prevents the malicious programs from running after the system automatically starts up. The security planning of the OS files must cover the following aspects:

- To avoid the global write attribute of a new file, set the global **umask** values in the **/etc/.profile** and **/etc/.login** files.
- The **.netrc** file may contain the plain password. Therefore, you must set the right of the file to 600.
- By default, the global execution right is disabled for the **rcp/rlogin/rsh** and **tftp** files.
- Check and monitor the content of the **cron** file to avoid the execution of unnecessary scheduled tasks.
- Set strict access rights for key system logs, such as the **/var/log/syslog** file.
- Set strict access rights for the files that contain user information and passwords, such as the **/etc/passwd**, **/etc/shadow**, and **/etc/group** files. Change the owner and group of these files to root:sys or to another value.
- Set the owners of the initiation files that are not in the system user directory and disable the global read and write rights of these files.
- Check and set the access rights of the system execution file, system configuration file, and system equipment file.

Security Planning of OS Services and Ports

The security planning of the Solaris OS services and ports is based on the necessary services provided to the external networks. In addition, the security planning repairs the defective services and system settings to protect the system from malicious attacks from the service request.

The security planning of OS services and ports is as follows:

- Disable the unnecessary network services based on the requirements of the U2000.
- Set the parameters of the TCP/IP protocol stack to avoid malicious attacks. For example, increase the maximum number of SPCs to avoid SYN attacks.
- Disable the route forwarding and broadcast functions of the non-gateways and firewalls to avoid malicious attacks.
- Remind the user to use legal Telnet and FTP services and record the connection information.
- Prevent the system user from login through FTP and prevent the super user from remote login through Telnet.
- Check the NFS and RFS security and prohibit the remote workstation from connecting to the local NFS as the **root** user.
- Check and install the OS patches periodically.

9.1.2.2 SUSE Linux OS Security

This topic describes the security policy of the SUSE Linux OS.

OS User Security

After the SUSE Linux OS, Sybase database and the U2000 are successfully installed on a server, the following OS users are generated:

- **root**: The **root** user is the default administrator of the SUSE Linux OS. With the highest administrative rights, the **root** user can control all resources, create other users, assign rights to these users, and perform all the operations supported by the OS.
- **nmsuser**: During the installation of the U2000, the **nmsuser** user is automatically created by the U2000 as an OS user. The **nmsuser** user can set the environment variables of the U2000 server and start the U2000 client on the server. The **nmsuser** user has all the rights to edit the **/nmsuser** directory. The **.profile** file in this directory records the environment variables of the U2000.
- **oracle**: During the installation of the NMS, the Oracle database is automatically installwed and the OS user **oracle** is automatically created. The **oracle** user has all rights to only the Oracle database installation directory such as **/opt/oracle**. Thus, the **oracle** user can manage the Oracle database such as configuring Oracle to run environment variables and start and stop Oracle services.

Assign the three accounts to different users based on the actual situation. In addition, follow the security principles of the user name and password, and change the password regularly (such as every three months).

If the U2000 needs to provide the external file transfer protocol (FTP) service, such as file transfer for performance data collection, you must add an FTP user manually on the OS. For security purposes, an independent path of the FTP file system is required for an FTP user to prevent the access of the non-FTP file systems. In addition, set a password for the FTP user, and change the password regularly as required.

OS File Security

By checking and strengthening the read and write rights of the OS files, the system checks the correctness and necessity of the core files, prevents unauthorized access to the key OS files (such as the password file), and prevents the malicious programs from running after the system automatically starts up. The security planning of the OS files must cover the following aspects:

- To avoid the global write attribute of a new file, set the global umask values in the **/etc/.profile** and **/etc/.login** files.
- The **.netrc** file may contain the plain password. Therefore, you must set the right of the file to 600.
- By default, the global execution right is disabled for the **rcp/rlogin/rsh** and **tftp** files.
- Check and monitor the content of the **cron** file to avoid the execution of unnecessary scheduled tasks.
- Set strict access rights for key system logs, such as the **/var/log/syslog** file.
- Set strict access rights for the files that contain user information and passwords, such as the **/etc/passwd**, **/etc/shadow**, and **/etc/group** files. Change the owner and group of these files to root:sys or to another value.
- Set the owners of the initiation files that are not in the system user directory and disable the global read and write rights of these files.
- Check and set the access rights of the system execution file, system configuration file, and system equipment file.

Security Planning of OS Services and Ports

The security planning of the SUSE Linux OS services and ports is based on the necessary services provided to the external networks. In addition, the security planning repairs the defective services and system settings to protect the system from malicious attacks from the service request.

The security planning of OS services and ports is as follows:

- Disable the unnecessary network services based on the requirements of the U2000.
- Set the parameters of the TCP/IP protocol stack to avoid malicious attacks. For example, increase the maximum number of SPCs to avoid SYN attacks.
- Disable the route forwarding and broadcast functions of the non-gateways and firewalls to avoid malicious attacks.
- Remind the user to use legal Telnet and FTP services and record the connection information.
- Prevent the system user from login through FTP and prevent the super user from remote login through Telnet.
- Check the NFS and RFS security and prohibit the remote workstation from connecting to the local NFS as the **root** user.
- Check and install the OS patches periodically.

9.1.2.3 Windows OS Security

This topic describes the security policy of the Windows OS.

OS User Security

When the U2000 runs on the Windows OS, the default administrator is needed. With the highest administrative rights of the Windows OS, the administrator account can control all resources,

create other users, assign rights to these users, and perform all the operations supported by the OS.

In addition, follow the security principles of the user name and password, and change the password regularly (such as every three months).

If the U2000 needs to provide the external file transfer protocol (FTP) service, such as file transfer for performance data collection, you must add an FTP user manually on the OS. For security purposes, an independent path of the FTP file system is required for an FTP user to prevent the access of the non-FTP file systems. In addition, set a password for the FTP user, and change the password regularly as required.

OS File Security

The security planning principles of the users, file system, and network services of the OS are as follows:

- Set the rights of the core files and directories of the Windows OS to prevent illegal operations of hackers, such as modifying, moving, overwriting, and deleting the files.
- Set the rights of the registry of the Windows OS to prevent illegal operations of hackers, such as modifying and deleting the registry.
- Set the important key assignments in the registry to prevent the Windows OS from running in the insecure mode. For example, the default value of the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom\Autorun` key in the registry is set to **0** to disable automatic running of a CD-ROM.

Security Planning of OS Services and Ports

The principles for the security planning of the OS services and ports are as follows:

- Do not start the unnecessary services of the OS to avoid security risks. Alternatively, you can analyze how often the service is used and the necessity of the service to the system, and then set in which way the service is started, for example, automatically or manually.
- Shut down the unnecessary private TCP/IP port to prevent attacks from the port. For example, port 25 is used for the Simple Mail Transfer Protocol (SMTP) service.
- Set a sharing directory to prevent hackers from getting sensitive information from the sharing directory.
- Set and strengthen the audit policy of the OS. You can set the OS to audit the operation sessions in the OS, such as the login of a user. Therefore, once the OS is attacked, the system administrator can discover the attack and take measures.
- Set a relatively complex system account rule to prevent the hackers from cracking the user accounts and passwords and logging in to the U2000 for illegal operations.
- Restrict the Internet information service (IIS) that is not required by the OS to protect the U2000 from remote attacks. For example, the anonymous access service of the IIS allows a remote user to log in to the U2000. In this case, the U2000 is subject to remote attacks.
- Set the parameters of the database management system SQL Server to ensure the security of the OS. For example, enable the encryption of the protocols of SQL Server.
- Check and install the OS patches periodically.

9.1.3 Security Planning of the HA System (Veritas)

This topic describes the security planning of the HA system (Veritas), especially the security planning of Veritas cluster server (VCS) users.

The default superuser of the VCS is **admin** and the default password is **password**. You can use this user to monitor and maintain the cluster environment of the HA system (Veritas).

The principles for the user security planning that can be implemented through the U2000 are as follows:

- After the default installation of the U2000 is complete, change the default password of the **admin** user.
- For the users that are created by using the **admin** user, change their passwords at the first login.
- The user password must meet certain requirements on complexity.
- The user password must be changed regularly to ensure the security of the password.

The principles for the security planning that are implemented through the associated management system and specifications are as follows:

- The account is the unique ID for a U2000 user. Therefore, ensure the unique mapping between users and accounts.
- There should be a mechanism to ensure the secrecy of user accounts and passwords.
- If the carrier has an independent software maintenance department or security department, subdivide the rights and designate a person to manage the rights.

9.1.4 Security Planning of System Data

Regular and effective backup of the U2000 applications and data is an important measure to secure the system. Intentional or accidental security threats always exist. If the system security is reduced due to a security accident, you must recover the system by using the system backup data. This is a must to secure the system.

9.1.4.1 Redundancy Backup Deployment During the System Running

According to the operation requirements, and network construction and deployment, carriers can use various system backup schemes. The backup schemes enhance the reliability of managing and maintaining the network. In addition, it enhances the security of system applications and data.

Software Disk Mirroring

The Solaris server uses the disk array, VxVm software, and Volume Manager to implement the disk mirroring. The disk mirroring refers to the mirroring in terms of software. That is, to enhance the system availability and data security by reducing the system performance.

This scheme is applicable to the single NMS that does not require high performance, but requires certain data security and low investment.

RAID

RAID 1 mirrors data from one disk to another. It provides high data redundancy, and ensures the system reliability and recoverability. In addition, the system performance is not affected. RAID 5 distributes verification modules to all data disks. This ensures that any read or write operation on the verification module is equalized to all RAID disks. In this manner, the bottleneck of reading or writing messages to the verification module is solved.

This scheme is applicable to the single NMS or multiple NMSs that require high performance, high data security, and medium investment.

9.1.4.2 Regular Data Backup

Regular data backup refers to backing up the system data to an independent storage device. When the system is abnormal, the latest backup data is restored to the running platform. This repairs the system to a large extent.

Backup of System Database

The U2000 provides an independent database backup tool to back up the data of the system database with multiple policies. The database data can be manually or automatically backed up to disks. In addition, the U2000 supports certain powerful functions, such as the periodic backup.

Other Backup Policies

- Back up data at periodically according to the maintenance and management requirements of carriers. Monthly backup is recommended.
- Back up data after the key configurations change or the system is upgraded.
- Practice the data restoration periodically to ensure the correctness and reliability of the data backup. It is recommended that you practice data restoration half a year.

9.2 Security Planning of the Database

The database is a key component of the management system to store and calculate data including secret data. The database has its own requirements on security. Using and maintaining the database properly is a key aspect of the security of the U2000. The database security involves the security of database users, and the security of storage and backup of database files.

9.2.1 Security Planning of Database Users
This topic describes the security planning of database users.

9.2.2 Security Planning of Database Files
This topic describes the security planning of database files.

9.2.1 Security Planning of Database Users

This topic describes the security planning of database users.

After the installation of the U2000 and the database is complete, the database system generates two database users.

- sa/system: The **sa/system** user is the default system administrator of the database. The **sa/system** user has the highest management rights of the database.

  NOTE

  - If the SQL or Sybase database is installed, the default administrator of the database is **sa**. The password of the **sa** user can be empty. If the password is not empty, it must be 6-30 characters long and consists of letters or digits. Special characters are not allowed..
  - If the Oracle database is installed, the default administrator of the database is **system**. The password of the **system** user can be empty and must be at least six characters long and consist of letters or digits. Special characters are not allowed..

- NMSuser: During the installation of the U2000, the **NMSuser** user is automatically created by the U2000 as a database user. You can use the **NMSuser** user to access the database when the U2000 is running.

For the sake of database security and data consistency, it is recommended that you do not use the **sa/system** or **NMSuser** user to directly maintain or modify the data in the database. Alternatively, you can use or maintain the data in the database through the U2000 and the maintenance tool provided by the database system.

The passwords of the **sa/system** user and the **NMSuser** user must be changed at least every three months to keep the passwords secret.

9.2.2 Security Planning of Database Files

This topic describes the security planning of database files.

To enhance the security of the database, ensure that the data is regularly backed up and the data restoration is regularly verified. For details, see **9.1.4 Security Planning of System Data**.

9.3 Operation Security

The reliability of operation security involves the designs of rights control, ACL control, time control, limit to login times, user monitoring, and operation confirmation.

Rights Control

The U2000 supports the allocation of management rights and operation rights. You can operate only the devices to which you have the management rights, and perform only the authorized operations.

ACL Control

The U2000 supports the ACL control. An authorized user can log in to the U2000 through only the client with a specified IP address, but cannot log in to the U2000 through the clients with IP addresses out of the ACL.

Time Control

The U2000 restricts the login time segment. An authorized user can log in to the U2000 only within a specified time segment, but cannot log in to the U2000 at a time out of the time segment.

Login Attempt Restriction

The U2000 restricts the login attempts. If the consecutive login attempts of a user exceed the maximum attempts within a specified duration, the system locks the user account, records the login failure in the system log, and generates an internal alarm. After a certain period of time (you can set the period of time, which is 30 minutes by default), the system unlocks the user account automatically.

User Monitoring

The U2000 monitors all user operations and generates a maintenance report. User **admin** can force any other user to log out.

Operation Confirmation

The U2000 requires a confirmation for any important operation or the operation that affects the devices in the entire network.

9.4 Security Planning of U2000 Users

When planning the U2000 users, you need to refer to the principles of the security planning to ensure the security of the U2000 users.

9.4.1 Introduction to the Security of U2000 Users

The U2000 security management mainly involves the objects management, password management, access control management, and role-based and domain-based management.

Security Management Objects

User: The user name and the password of a U2000 client user uniquely identifies the U2000 management rights entitled to the user. When a user is added to a user group, the user has all the operation rights of this user group. The U2000 provides a default user: **admin**. It is the super user of the system and has a higher authority than the system administrator group. You can neither modify the rights of the user **admin**, nor add user Administrator to other user groups.

User Group: This is a collection of the U2000 users that have the same management rights. The default user groups include the administrator group, maintenance group, manager group, monitor group, operator group, and SMManager group. The attributes of the user groups include name, description, member and authority.

Object Set: This is a collection of multiple pieces of managed object. Object sets are established to facilitate the user right management. If a user (or user group) is authorized with the operation rights of an object set, the user (or user group) can perform all the authorized operations on all the objects within the object set. This saves you the trouble of setting the management rights for

each NE one by one. Object sets can be created by geographical area, network layer, equipment type and so on.

Operation Set: This is a collection of client-side operations. Operation sets are established to facilitate the user right management. Different client-side operations have different impacts on the system security. Those operations that impose similar impacts on the system security are allocated to the same operation set. In this way, if a user (or user group) is authorized with the rights of an operation set, the user (or user group) can perform all the operations in the operation set. The U2000 has default operation sets. If the default operation sets do not meet the requirements for the right allocation, you can create new operation sets as required.

Password Management

Password Template: The password template defines all the elements required to construct a password. A good password template effectively raises the complexity of the password and prevents the password from being decoded. The password template has the following parts: password composition, password length, and the relation between the password and the user name.

Password Reuse Frequency and Password Reuse Period: For the purpose of password security, when you modify a password, you are not allowed to use a previously used password. The password reuse frequency determines that a new password cannot repeat the one used in the last N times. For example, if the password reuse frequency is set to 8, the new password cannot repeat any one that was used during the last eight times. The password reuse period determines that a password cannot repeat the one used in the past N days. For example, if the password reuse period is set to 8, the new password cannot repeat any one that was used during the past eight days.

The Weakness Password Dictionary: This is a collection of the passwords that are easy to be decoded. If the password being constructed matches an entry in the dictionary, the password is regarded as invalid. In this case you need to reconstruct a new password. The U2000 provides a weakness password dictionary that helps to exclude some common passwords that are easy to be decoded. You can redefine the dictionary as required.

Client Access Control

Remote Maintenance User Management: The U2000 supports the remote maintenance. It allows a remote maintenance terminal to log in to the U2000 server to perform operations on the NEs managed by the U2000. This is a way of maintenance that is commonly used during the remote equipment fault location and the scheduled check. The remote maintenance user is the U2000 user that logs in to the U2000 server through the remote maintenance client. By default, the remote maintenance user is disabled. Before you start the remote maintenance, you need to enable the remote maintenance user, and set related parameters of the user as required.

Client Access Control: To avoid the illegal login, after you create a U2000 user, you can specify an IP address range for the accessible clients. In this case, the U2000 user can only log in to the U2000 server from the clients that are within the IP address range. If you do not specify an IP address range, a U2000 user can log in to the U2000 server from the clients of local server.

SSL Protocol: If the server and the client communicate by the SSL protocol, the data interchanged between the server and the client is encrypted. In this way, the security of the network data is guaranteed.

Single-User Mode: If the U2000 switches from the multiuser mode to the single-user mode, all other users are forced to log out and cannot log in again unless the multiuser mode is enabled.

If no user is logged in under the single-user mode, only the user that has the right of switching user mode can log in to the U2000.

Client Lockout: To ensure the network security, the U2000 locks out a U2000 client if the user does not perform any operations on the client for a long time. This operation only locks out the client, but not affect the normal running of the U2000.

Role-Based and Domain-Based Management

The role-based and domain-based management is based on the allocation of the equipment set and operation set. The role-based management function (operation set) enables you to divide the U2000 rights to different function domains. The domain-based management function (equipment set) enables you to construct different network domains in unit of NE. You can easily control the user rights by entitling the rights of any function domain and network domain portfolio to a U2000 user.

Usually you can use the following two ways to allocate rights to a user or a user group:

- Add a user to a user group. The user added to the user group enjoys all the rights of the user group. This way is always used to allocate basic user rights.
- Adjust user rights. Some operation rights can be added or deleted. This way is always used when the current user or user group does not meet the requirements for the user right. Operation rights of the default user groups cannot be adjusted.

ACL

The ACL is a secure access control mechanism. It restricts a user to log in to the server through only the clients with the specified IP addresses.

ACL can effectively control the client IP address from which the user can log in to the U2000. In this case, even if the user account and the password are obtained by illegal users, these users cannot log in to the U2000, thus the U2000 security is improved. The U2000 provides two ACLs:

- System ACL

  The ACL of the entire U2000. All the users can log in to the U2000 only through specific IP addresses or network segments.

- User ACL

  The ACL of a user. The current user can log in to the U2000 only through specific IP addresses or network segments.

  NOTE

  The IP addresses or the network segments for the user ACL need to be within the range of the IP addresses or the network segments for the system ACL.

Network Management System Maintenance Suite

To ensure the security of the network management system, the password for the network management system maintenance suite should be modified periodically.

9.4.2 Security Planning Principles of U2000 Users

This topic describes the security planning principles of U2000 users.

General Strategy

Only the **admin** user can assign and modify rights to perform security operations, and add users to the user group that has rights to perform security operations. In the case of other operation rights, they are assigned by corresponding **admin** that have rights to make the assignment.

User Security Planning Principles Implemented by the U2000

- After the default installation of the U2000 is complete, modify the default password of the **admin** user.
- In the case of other users that are created by the **admin** user, change their passwords at the first login.
- Set the time validity of an account according to the management requirements. For example, the account is valid only before a certain date, in effective days, or in a specified period every day. Disable the unused accounts temporarily or permanently.
- Set the use policy such as maximum online times of a user and whether to stop using the account temporarily.
- Use the ACL to control the IP address from which the user logs in. After the IP address of a legal client is added to the U2000, the system checks the IP address in the ACL when the client attempts to log in.
- The user password must meet certain complexity requirements. For example, it must be more than 8 digits and be a combination of numbers, letters, and characters.
- Change the user password regularly to ensure the security of the password.

Security Planning Principles Implemented by Management Mechanism and Rules

- Ensure the unique mapping between users and accounts. An account is a unique ID of the user in the U2000.
- There is a mechanism to ensure the secrecy of user accounts and passwords.
- According to the NEs and network management requirements, the U2000 accounts are classified into proper user groups. In this way, the management rights and operation rights of the U2000 accounts are configured properly.
- If the carrier has an independent software maintenance department or security department, subdivide the rights and designate a person to manage the rights.

9.4.3 Rights- and Domain-Based Planning Principles of U2000 Users

This topic describes the rights- and domain-based planning principles of U2000 users.

Division of Rights

- Different rights are assigned to management personnel in the same domain but different positions to manage or operate the objects.
- With the rights-based management, a user account belongs to only one domain. The rights that a user obtains are valid only in the related domain. That is, a user who passes the authentication in a domain can manage only objects in that domain. The rights-based management of different domains is independent of each other.

Division of Domain

- Management personnel of different domains manage different objects. The rights that a user obtain to manage objects are valid only in the related domain.
- In a domain, management personnel can manage the objects in the rights-based mode, but cannot manage equipment, services or data in another domain.

For example: A is from regional maintenance office E and B is from regional maintenance office F. In this case, A can only manage equipment, services, and data of regional maintenance office E, but cannot manage equipment, services, or data of regional maintenance office F. Likewise, B can only manage equipment, services, and data of regional maintenance office F, but cannot manage equipment, services, or data of regional maintenance office E.

Regional Administrator

The regional administrator is created by the central office for the regional maintenance office. Each regional office has only one regional administrator. After the related operation rights and management rights are assigned, the regional administrator can create users in the authorized range, and assign operation rights and management rights to the users in the regional office.

For example, A is the regional administrator created by the central office for regional office E. In regional office E, A can create the operator B, and set B to manage and maintain the UA5000.

9.5 Security Planning of NE Users

An NE user refers to the one that maintains an NE through the NE management interface. The U2000 provides the NE users management and local command terminal (LCT) users management functions to manage NE users in a centralized manner. When planning the NE users, you need to refer to the principles of the security planning to ensure the security of the NE users.

This feature is applicable to access NEs, MSTP NEs, RTN NEs, PTN NEs, WDM NEs, NA WDM NEsand Marine NEs. For the NEs that do not support this feature, you need not plan the NE users.

9.5.1 Introduction to the Security of NE Users
The security management of NEs includes NE access control, NE user management, and NE operation rights management.

9.5.2 Security Planning Principles of NE Users
This topic describes the security planning principles of NE users.

9.5.1 Introduction to the Security of NE Users

The security management of NEs includes NE access control, NE user management, and NE operation rights management.

NE Access Control

The ACL is the access control list that provides the basic data stream filtering function. The NE that is configured with the ACL can determine whether to filter the IP packet that traverses the NE. The ACL can control the incoming and outgoing of a data stream of a network.

Communication port access control: NEs can access the U2000 through the OAM, COM, Ethernet, and serial ports. By enabling the access control of a certain communication port, you

can set the access port of an NE for connecting to the U2000. By default, an NE supports the connection to the U2000 through the Ethernet port

NE User Management

NE user: To ensure the NE data security, a user should use a created NE user account to log in to the NE. In addition, only the authorized operations can be performed by the NE user.

NE user level: According to the authorized operation types, NE users are classified into different operation levels, which are called NE user levels. NE users of different levels are divided into different NE user groups.

NE security parameters: NE can automatically determine whether the password of an NE user is valid according to the NE security settings and thus determine whether to allow the login of the NE user. The U2000 administrator needs to learn the NE security settings and modify the NE user password before it becomes invalid. The NE security parameters include the following: **Allowable Used Times for Outdated Password**, **Password Max. alid Period**, **Password Min. Valid Period**, **Password Uniqueness**, **Lock Testing Time**, **Allowable illegal Access Times** and **Lock Time**.

NE Operation Rights

NE operation rights: There are five levels of NE user operations. In the descending order, these operations include monitor level, operation level, maintenance level, system level, and debug level. Each user of a higher level can have all rights of users of a lower level. For example, the user of operation level can have all rights of users of the monitoring level. The rights of users of the five levels are as follows:

- Monitor Level: all query commands, login and logout, and password change.
- Operation level: all fault and performance settings, some security settings, and some configurations.
- Maintenance level: some security settings, some configurations, communication settings, and log management.
- System level: all security settings and all configurations.
- Debug Level: all security settings, all configurations, and debugging commands.

Rights management: To ensure NE data security, only an NE user is allowed to log in to the NE. The NE user can perform only the authorized operations on the NE. It is recommended that the U2000 administrator finish creating NE users before provisioning services. When a general account for all NEs is created, ensure that the user is set with consistent rights level, so as to prevent rights confusion.

9.5.2 Security Planning Principles of NE Users

This topic describes the security planning principles of NE users.

The principles for the security planning of NE users are as follows:

- An NE adopts the user name + password authentication mode. The security planning principles in terms of user name and password are as follows:
  - The user password must meet certain complexity requirements. For example, it must be more than 8 digits and be a combination of numbers, letters, and characters.
  - Change the user password regularly to ensure the security of the password.

  - Ensure the unique mapping between users and accounts. An account is a unique ID of the user in the U2000.
  - There is a mechanism to ensure the secrecy of user accounts and passwords.
- After an NE is managed by the U2000, the information about the NE users must be promptly synchronized to the U2000.
- Restrict the re-login times of an NE user. If several logins with the same user account occur at the same time, the system needs to trace the security event so as to prevent a potential security risk. The re-entry times of an NE user ranges from 0 to 4. It is recommended that the re-entry times of an NE user be set to **1**. For an NE user account that is not used at present, set the re-entry time to **0**. That is, you cannot use the account to log in to the U2000 temporarily.
- It is important to assign different rights to different NE users for the maintenance of NEs. For example, the rights of the four levels of users are as follows:
  - Super user: A super user can perform all management and maintenance operations on NEs and perform security management of NE users. Usually, a super user is only used to set up the security system and configure the basic information on an NE after the NE is reset. It is not recommended that you use this user account for daily maintenance.
  - Administrator: An administrator equals to a super user basically in terms of management rights. If the **root** user is an administrator for an NE, the highest level of NE users is administrator. Usually, the administrator manages user accounts, operation rights, and management rights.
  - Operator: After authorized by a super user or an administrator, an operator can change or adjust the configurations and services of NEs. For example, the operator can configure the physical data to deploy an NE, configure the data to provision services, and conduct troubleshooting during system operation. If a person needs to perform such operations, the person should be assigned as a user of this level.
  - Common user: A common user mainly queries the running status, alarms, and performance data of an NE, and performs the related basic operations on the NE, such as querying the basic configurations and the version of the NE. A common user cannot change the physical configurations or running status of an NE. If a person needs to perform such operations, the person should be assigned as a user of this level.
- If the carrier has an independent software maintenance department or security department, subdivide the rights and designate a person to manage the rights.

9.6 Security Planning of Data Transmission

The U2000 data is transmitted in the system (for example, between the system server and clients) or between the U2000 and the external systems (such as the telecommunications equipment and the OSS). The data transmission requires privacy and integrity. Therefore, ensure that the data transmission is not intercepted, and external networks cannot directly access the internal network of carriers. In addition to the security of the OS, database, and application system, the security during data transmission should also be considered.

The security of data transmission mainly involves two layers: the communication security at the application layer and the channel security at the network layer.

Based on the security of two layers, the security policies of data transmission include: setting up the out-band DCN, setting up the independent virtual private network (VPN), and isolating through the firewall.

9.6.1 Layers of Data Transmission Security

The security of data transmission mainly involves two layers: the communication security at the application layer and the channel security at the network layer.

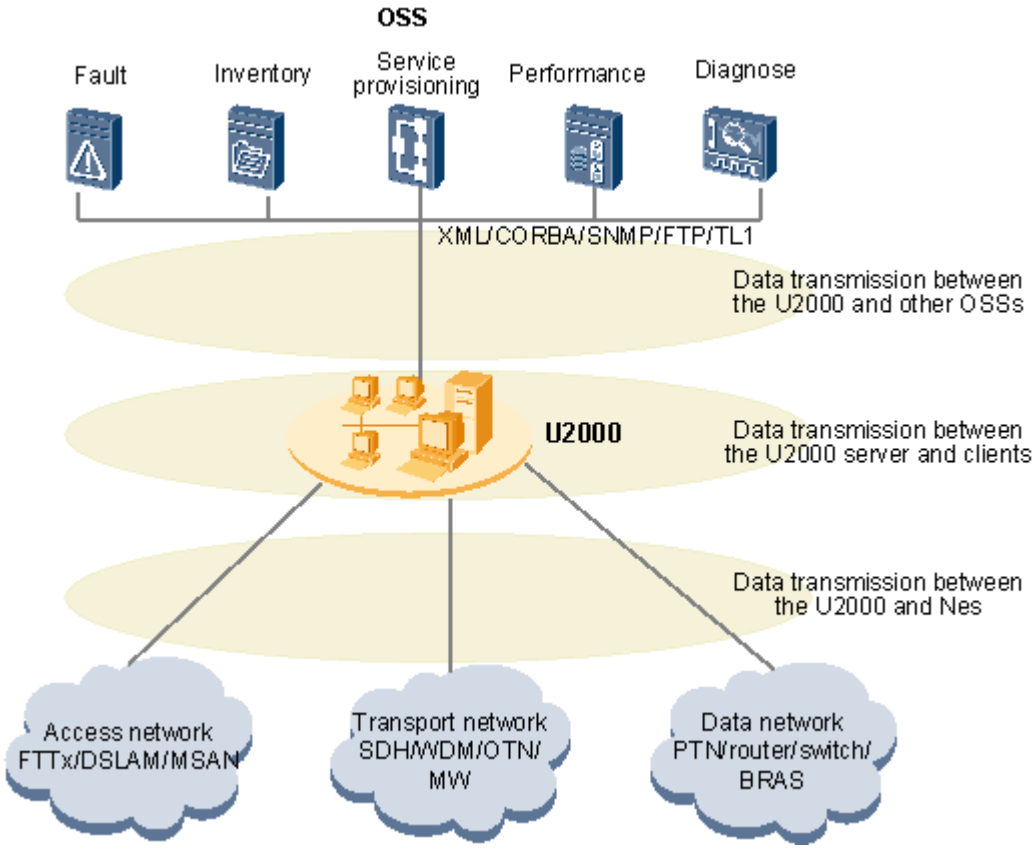
Communication Security at the Application Layer

During the application communication, the communication security is implemented through the following ways: software verification, encryption of user authentication keys, encryption of passwords, and encryption of communication message packages. These are implemented by the application automatically, which is not described in details here.

Channel Security at the Network Layer

The channel security at the network layer refers to the isolation and security of the physical and logical communication links in the network. According to the U2000 networking, the security of communication links covers the following three aspects: data transmission between NEs and the U2000 server, between clients and the U2000 server, and between the U2000 server and other OSSs.

Figure 9-2 Layers of data transmission security



9.6.2 Data Transmission Security Policies

Based on the security of two layers, the security policies of data transmission include: setting up the out-band DCN, setting up the independent virtual private network (VPN), and isolating through the firewall.

Setting Up the Out-Band DCN

The U2000 network needs to be separate from the service network of the managed objects. This type of networking is the out-band NMS. By adopting the independent DCN (DDN, X.25, E1, or FR), the U2000 server and managed objects form a private network through routers and digital trunk units (DTUs) to transmit the U2000 data.

The intranet can serve as the network between the U2000 clients and servers. Alternatively, you can set up an independent network. The IP address can be planned as that for an independent private network.

The out-band NMS can ensure the physical isolation of the U2000 network and the service network. This ensures the network security of the U2000.

Setting Up the Independent VPN

The VPN technology develops fast, including virtual private data network (VPDN) and private VPN. The private VPN, including GRE, IPSec, MPLS, and VLL is widely adopted for the NMS network.

During the VLAN planning of the network, plan an independent global VLAN for the U2000 to transmit the U2000 data in the upstream direction. Usually, the equipment at the access layer does not support the VPN. The VLAN is involved for Layer 2 isolation. At the convergence layer, router or BRASs must support VPN and VLAN. In addition, the equipment must realize the label mapping from the VLAN to the VPN. This ensures that the U2000 data can be transmitted to the VPN gateways connected to the U2000 server through the VPN.

The VPN NMS can ensure the logical isolation of the U2000 network and service network. This ensures the network security of the data transmission of the U2000.

Isolating Through the Firewall

Firewall is an important security measure for the U2000. The firewall can provide various security functions, such as packet filtering. The firewall monitors the access channel between the reliable network (internal network) and the non-reliable network (external network). This protects the internal network and data from illegal access (unauthorized and unauthenticated access) and malicious attacks from external networks.

You can deploy the U2000 clients in the public network so that maintenance engineers of carriers at each level can log in to the U2000 conveniently. You can deploy the U2000 servers and equipment in the private network. The clients cannot directly access equipment. All the access must go through the U2000 servers. The U2000 servers and equipment are protected by the firewall. This can effectively avoid illegal network access and attacks.

Using the firewall for isolation is a good solution to the security protection at the network layer.

Data Encryption

The U2000 must support the following data encryption protocols to ensure data transmission security:

- Data transmission between the U2000 and NEs: SSLv3, SNMPv3, SSHv2, and SFTP
- Data transmission between the U2000 server and U2000 clients: SSLv3
- Data transmission between the U2000 and upper-layer OSS: SSLv3, SNMPv3, SFTP, and HTTPS

10 Manageable Equipment

About This Chapter

This topic provides information about the equipment that the U2000 V100R002C01 can manage.

For information about the equipment of specific types that the U2000 V100R002C01 can manage, see the following topics:

- **Manageable MSTP Series Equipment**
- **Manageable WDM Equipment**
- **Manageable NA WDM Equipment**
- **Manageable Submarine Line Equipment**
- **Manageable RTN Equipment**
- **Manageable PTN Equipment**
- **Manageable FTTx Access Series Devices**
- **Manageable MSAN Series Devices**
- **Manageable DSLAM Series Devices**
- **Manageable Router Series Devices**
- **Manageable Switch Series Devices**
- **Manageable Metro Service Platform Devices**
- **Manageable Broadband Access Series Devices**
- **Manageable VoIP Gateway Devices**
- **Manageable WLAN Series Devices**
- **Manageable Firewall Series Devices**
- **Manageable DPI Equipment**
- **Manageable SVN Series Devices**
- **Manageable OP-Bypass Equipment**

10.1 Manageable MSTP Series Equipment

Manageable MSTP series equipment is listed as follows:

Table 10-1 Manageable MSTP series equipment

Category	Equipment	Description
SDH series	OptiX 155C	OptiX 155C SDH transmission unit for the access network
	OptiX 155S	OptiX 155S simplified STM-1 optical transmission system
	OptiX 1556/622B_I OptiX 1556/622B_II	OptiX 155/622B STM-1/STM-4 compatible optical transmission system (19-inch rack)
	OptiX 2500	OptiX 2500 STM-4/STM-16 compatible optical transmission system
	OptiX 2500 REG	OptiX 2500 REG STM-16 regenerator
MSTP series	OptiX Metro 100	OptiX Metro 100 terminal STM-1 optical transmission system
	OptiX Metro 200	OptiX Metro 200 ultra compact STM-1 optical transmission system
	OptiX Metro 500	OptiX Metro 500 ultra compact STM-1 multi-service transmission system
	OptiX 155/622H (Metro 1000)	OptiX 155/622H*(Metro1000)* STM-1/ STM-4 MSTP
	OptiX Metro 1000	OptiX 155/622H*(Metro1000)* STM-1/ STM-4 MSTP optical transmission system V3 series
	OptiX Metro 1050	OptiX Metro 1050 compact STM-1/ STM-4 multi-service optical transmission system
	OptiX Metro 1100	OptiX Metro 1100 compact container STM-16 multi-service transmission system
	OptiX 155/622 (Metro 2050)	OptiX 155/622*(Metro2050)* STM-1/ STM-4 compatible optical transmission system
	OptiX 2500+ (Metro 3000)	OptiX 2500+*(Metro3000)* STM-16 MADM/MSTP optical transmission system

Category	Equipment	Description
	OptiX Metro 3100	OptiX Metro 3100 STM-16 multi-service transmission system
	OptiX 10G (Metro 5000)	OptiX 10G*(Metro5000)*STM-64 MADM optical transmission system
OSN series	OptiX OSN 500	OptiX OSN 500 STM-1/STM-4 multi-service CPE optical transmission system
	OptiX OSN 1500	OptiX OSN 1500 intelligent optical transmission system
	OptiX OSN 2000	OptiX OSN 2000 enhanced STM-1/ STM-4 multi-service optical transmission system
	OptiX OSN 2500	OptiX OSN 2500 intelligent optical transmission system
	OptiX OSN 2500 REG	OptiX OSN 2500 REG STM-16 regenerator
	OptiX OSN 3500 OptiX OSN 3500 II	OptiX OSN 3500 intelligent optical transmission system
	OptiX OSN 7500	OptiX OSN 7500 intelligent optical switching system
	OptiX OSN 9500	OptiX OSN 9500 intelligent optical switching system

10.2 Manageable WDM Series Equipment

Manageable WDM series equipment is listed as follows:

Table 10-2 Manageable WDM equipment

Category	Equipment	Description
Metro WDM series	OptiX Metro 6020	OptiX Metro 6020 compact container CWDM system V100R001
	OptiX Metro 6040	OptiX Metro 6040 compact container WDM system V100R001
	OptiX Metro 6040 V2	OptiX Metro 6040 compact container DWDM system V200R001 or higher

Category	Equipment	Description
	OptiX Metro 6100	OptiX Metro 6100 DWDM multi-service transmission system V100R002
	OptiX Metro 6100V1	OptiX Metro 6100 DWDM multi-service transmission system V100R003
	OptiX Metro 6100 V1E	OptiX Metro 6100 WDM multi-service transmission system V100R004 or higher
	OptiX OSN 900A	OptiX OSN 900A compact WDM system (A Type)
LH WDM series	OptiX BWS 320G	OptiX BWS 320G backbone DWDM optical transmission system V300R002
	OptiX BWS 320G V3	OptiX BWS 320G backbone DWDM optical transmission system V300R004
	OptiX BWS 1600G, OptiX BWS 1600G OLA	OptiX BWS 1600G backbone DWDM optical transmission system V100R003 or higher
	OptiX BWS 1600S	OptiX BWS 1600S submarine line terminal equipment
	OptiX OTU40000	OptiX OTU 40000 backbone DWDM optical transmission system
NG WDM series	OptiX OSN 1800	OptiX OSN 1800 compact multi-service edge optical transport platform
	OptiX OSN 3800	OptiX OSN 3800 compact intelligent optical transport platform
	OptiX OSN 6800	OptiX OSN 6800 intelligent optical transport platform
	OptiX OSN 8800 T32 OptiX OSN 8800 T64	OptiX OSN 8800 T32 intelligent optical transport platform OptiX OSN 8800 T64 intelligent optical transport platform

NOTE

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 higher versions.

10.3 Manageable NA WDM Series Equipment

Manageable NA WDM series equipment is listed as follows:

Table 10-3 Manageable NA WDM equipment

Category	Equipment	Description
LH WDM series	OptiX BWS 1600A	OptiX BWS 1600A WDM Optical Transmission System
	OptiX BWS 1600G(NA)	OptiX BWS 1600G(NA) Backbone DWDM Optical Transmission System
NG WDM series	OptiX OSN 1800(NA) compact intelligent optical transport platform	OptiX OSN 1800(NA)
	OptiX OSN 3800A compact intelligent optical transport platform	OptiX OSN 3800A
	OptiX OSN 6800A intelligent optical transport platform	OptiX OSN 6800A
	OptiX OSN 8800 I/II(NA) intelligent optical transport platform	OptiX OSN 8800 I/II(NA)

10.4 Manageable Submarine Line Equipment

Manageable submarine line equipment is listed as follows:

Table 10-4 Manageable submarine line equipment

Category	Equipment	Description
Submarine line series	OptiX SLM 1630	OptiX SLM 1630 submarine line monitor
	OptiX PFE 1670	OptiX PFE 1670 Power Feeding Equipment

Category	Equipment	Description
	OptiX BWS 1600S	OptiX BWS 1600S submarine line terminal equipment

10.5 Manageable RTN Series Equipment

Manageable RTN series equipment is listed as follows:

Table 10-5 Manageable RTN equipment

Category	Equipment	Description
RTN series	OptiX RTN 605	OptiX RTN 605 radio transmission system
	OptiX RTN 610	OptiX RTN 610 radio transmission system
	OptiX RTN 620	OptiX RTN 620 radio transmission system
	OptiX RTN 910	OptiX RTN 910 radio transmission system
	OptiX RTN 950	OptiX RTN 950 radio transmission system
	OptiX RTN 5000S	OptiX RTN 5000S radio transmission system

10.6 Manageable PTN Series Equipment

Manageable PTN series equipment is listed as follows:

Table 10-6 Manageable PTN series equipment

Category	Equipment	Description
PTN series	OptiX PTN 1900	OptiX PTN 1900 multi-service packet transmission platform
	OptiX PTN 3900	OptiX PTN 3900 multi-service packet transmission platform

Category	Equipment	Description
	OptiX PTN 3900-8	OptiX PTN 3900-8 multi-service packet transmission platform
	OptiX PTN 912	OptiX PTN 912 multi-service packet transmission platform
	OptiX PTN 910	OptiX PTN 910 multi-service packet transmission platform
	OptiX PTN 950	OptiX PTN 950 multi-service packet transmission platform

10.7 Manageable FTTx Series Equipment

Manageable FTTx series equipment are listed as follows:

Table 10-7 Manageable FTTx series equipment

Category	Equipment	Description
OLT series	MA5600T	SmartAX MA5600T Multi-service Access Module
	MA5603T	SmartAX MA5603T Optical Access Equipment
	MA5680T	SmartAX MA5680T Optical Access Equipment
	MA5683T	SmartAX MA5683T Optical Access Equipment
	MA5606T	SmartAX MA5606T Optical Access Equipment, Only the version of V800R105 support.
	MA5603U	SmartAX MA5603U Multi-service Access Module
MDU series	MA5606T	SmartAX MA5606T Optical Access Equipment
	MA5620	SmartAX MA5620 Multiple Dwelling Unit
	MA5626	SmartAX MA5626 Multiple Dwelling Unit

Category	Equipment	Description
	MA5628	SmartAX MA5628 Multiple Dwelling Unit
	MA5620E	SmartAX MA5620E EPON Multiple Dwelling Unit
	MA5626E	SmartAX MA5626E EPON Multiple Dwelling Unit
	MA5620G	SmartAX MA5620G GPON Multiple Dwelling Unit
	MA5626G	SmartAX MA5626G GPON Multiple Dwelling Unit
	MA5610	SmartAX MA5610 Multi-service Access Module
	MA5612	SmartAX MA5612 Multi-service Access Module
	MA5616	SmartAX MA5616 Multi-service Access Module
	MA5651	SmartAX MA5651 Multiple Dwelling Unit
	MA5651G	SmartAX MA5651G Multiple Dwelling Unit
	MA5652G	SmartAX MA5652G GPON Multiple Dwelling Unit
	MA5635	SmartAX MA5635 Multi-service Access Module
	MA5662	SmartAX MA5662 Multi-Service Access Module
	SRG2220	SRG2220 Service Router Gateway
ONT series	EchoLife:OT550	-
	EchoLife:HG850	-
	EchoLife:HG850a	-
	EchoLife:HG851	-
	EchoLife:HG852	-
	EchoLife:HG853	-
	EchoLife OT925	-
	SmartAX OT928	-

Category	Equipment	Description
	EchoLife:HG810	-
	EchoLife:HG811	-
	EchoLife:HG813	-
	EchoLife:HG860	-
	EchoLife:HG861	-
	EchoLife:HG863	-
	EchoLife:HG865	-
	EchoLife:HG810a	-
	EchoLife:HG866	-
	EchoLife:HG866e	-
	U5KG	-
	810e	-
	813e	-
	850e	-
	925e	-
	U5KE	-
	HG8240	-
	HG8245	-
	HG8247	-

10.8 Manageable MSAN Series Equipment

Manageable MSAN series equipment are listed as follows:

Table 10-8 Manageable MSAN series equipment

Category	Equipment	Description
UA5000 series	UA5000	UA5000 Universal Access Unit
	UA5000(PVU)	UA5000 Universal Access Unit
	UA5000(IPMB)	UA5000 Universal Access Unit
	UA5000(PVMV1)	UA5000 Universal Access Unit

Category	Equipment	Description
MD5500 series	MD5500	MD5500 Multi-service Distribution Module

10.9 Manageable DSLAM Series Equipment

Manageable DSLAM series equipment are listed as follows:

Table 10-9 Manageable DSLAM series equipment

Category	Equipment	Description
MA5100 series	MA5100V2	SmartAX MA5100 Multi-service Access Module
	MA5105	SmartAX MA5105 Multi-service Access Module
MA5300 series	MA5300	SmartAX MA5300 Broadband Access System
MA5600 series	MA5600V3	SmartAX MA5600 Multi-service Access Module
	MA5605	SmartAX MA5605 Multi-service Access Module
	MA5615	SmartAX MA5615 Broadband Access System
MA5600V8 series	MA5600T	SmartAX MA5600T Multi-service Access Module
	MA5603T	SmartAX MA5603T Multi-service Access Module
	MA5606T	SmartAX MA5606T Multi-service Access Module

10.10 Manageable Router Series Equipment

Manageable router series equipment are listed as follows:

Table 10-10 Manageable router series equipment

Category	Device	Description
NE series routers	NE05	Net engine 05 router
	NE08	Net engine 08 router

Category	Device	Description
	NE16	Net engine 16 router
	NE08E	Net engine 08E router
	NE16E	Net engine 16E router
	NE20	Net engine 20 router
	NE20E	Net engine 20E router
	NE40	Net engine 40 universal switching router
	NE80	Net engine 80 universal switching router
	NE40E/NE80E	Net engine 40E/80E core router
	NE5000E	Net engine 5000E core router
R/AR series routers	R series routers	R series routers
	AR18	Advanced router 18 serials router
	AR28	Advanced router 28 serials router
	AR46	Advanced router 46 serials router
	AR19	Advanced router 19 serials router
	AR29	Advanced router 29 serials router
	AR49	Advanced router 49 serials router

10.11 Manageable Switch Series Equipment

Manageable switch series equipment are listed as follows:

Table 10-11 Manageable switch series equipment

Category	Device	Description
S8500 series switches	S8505	Quidway S8505 Series Routing Switches
	S8505E	Quidway S8505E Series Routing Switches
	S8508	Quidway S8508 Series Routing Switches
	S8512	Quidway S8512 Series Routing Switches
S7800 series switches	S7800	Quidway S7800 Series Ethernet Switches

Category	Device	Description
S6500 series switches	S6502	Quidway S6502 Series Ethernet Switches
	S6503	Quidway S6502 Series Ethernet Switches
	S6506R	Quidway S6506R Series Ethernet Switches
	S6506	Quidway S6506 Series Ethernet Switches
S5000 series switches	S50 series switches	Quidway S5000 Series Ethernet Switches
	S55 series switches	Quidway S5500 Series Ethernet Switches
	S56 series switches	Quidway S5600 Series Ethernet Switches
S3000 series switches	S30 series switches	Quidway S3000 Series Ethernet Switches
	S35 series switches	Quidway S3500 Series Ethernet Switches
	S39 series switches	Quidway S3900 Series Ethernet Switches
S2000 series switches	S20 series switches	Quidway S2000 Series Ethernet Switches
	S24 series switches	Quidway S2400 Series Ethernet Switches
box series switches	S2300	Quidway S2300 Series Ethernet Switches
	S2700	Quidway S2700 Series Ethernet Switches
	S3300	Quidway S3300 Series Ethernet Switches
	S3700	Quidway S3700 Series Ethernet Switches
	S5300	Quidway S5300 Series Ethernet Switches
	S5700	Quidway S5700 Series Ethernet Switches
frame series switches	S9300	Quidway S9300 Terabit Routing Switch

10.12 Manageable Metro Service Platform Equipment

Manageable Metro service platform equipment are listed as follows:

Table 10-12 Manageable Metro service platform equipment

Category	Device	Description
CX series devices	CX200	CX200 Metro Services Platform
	CX200C	CX200C Metro Services Platform
	CX200D	CX200D Metro Services Platform
	CX300	CX300 Metro Services Platform
	CX380	CX380 Metro Services Platform
	CX600	CX600 Metro Services Platform

10.13 Manageable Broadband Access Series Equipment

Manageable broadband access series equipment are listed as follows:

Table 10-13 Manageable broadband access series equipment

Category	Device	Description
Multi-service gateways	MA5200E	Multiservice access 5200E service gateway
	MA5200F	Multiservice access 5200F service gateway
	MA5200G	Multiservice access 5200G service gateway
	ME60 series	Multiservice engine 60 serials service gateway

10.14 Manageable VoIP Gateway Equipment

Manageable VoIP gateway equipment are listed as follows:

Table 10-14 Manageable VoIP gateway equipment

Category	Device	Description
VoIP Gateway	VG10	VoIP gateways 10
	VG20	VoIP gateways 20
	VG80	VoIP gateways 80

Category	Device	Description
	XE series	-

10.15 Manageable WLAN Series equipment

Manageable WLAN Series equipment are listed as follows:

Table 10-15 Manageable WLAN series equipment

Category	Device	Description
WLAN	WA10 AP	WLAN 10
	WA12 AP	WLAN 12

10.16 Manageable Firewall Series Equipment

Manageable firewall series equipment are listed as follows:

Table 10-16 Manageable firewall series equipment

Category	Device	Description
Eudemon	E8080E	Eudemon 8000E series Firewall
	E8160E	Eudemon 8000E series Firewall
	NE40E-FW	Eudemon 8000E series Firewall
	NE80E-FW	Eudemon 8000E series Firewall
	E8040	Eudemon 8000 series Firewall
	E8080	Eudemon 8000 series Firewall
	E1000E U2	Eudemon 1000E series Firewall
	E1000E U3	Eudemon 1000E series Firewall
	E1000E U5	Eudemon 1000E series Firewall
	E1000E U6	Eudemon 1000E series Firewall
	Eudemon1000E-D	Eudemon 1000E series Firewall
	Eudemon1000E-I	Eudemon 1000E series Firewall
	E300	Eudemon 300 series Firewall
	E500	Eudemon 500 series Firewall
	E1000	Eudemon 1000 series Firewall

Category	Device	Description
	E200	Eudemon 200 series Firewall
	E100E	Eudemon E100E series Firewall
	E200S	Eudemon E200S series Firewall
USG	USG9310	USG9300 Unified Security Gateway
	USG9320	USG9300 Unified Security Gateway
	USG9210	USG9200 Unified Security Gateway
	USG9220	USG9200 Unified Security Gateway
	USG5320	USG5000 Unified Security Gateway
	USG5330	USG5000 Unified Security Gateway
	USG5350	USG5000 Unified Security Gateway
	USG5360	USG5000 Unified Security Gateway
	USG5310	USG5000 Unified Security Gateway
	USG5300ADD	USG5000 Unified Security Gateway
	USG5300ADI	USG5000 Unified Security Gateway
	USG2130	USG2100 Unified Security Gateway
	USG2130W	USG2100 Unified Security Gateway
	USG2160	USG2100 Unified Security Gateway
	USG2160W	USG2100 Unified Security Gateway
	E200E-B	E200E Unified Security Gateway
	USG2160	USG2100 Unified Security Gateway
	USG2160W	USG2100 Unified Security Gateway
	USG2160BSR	USG2100 Unified Security Gateway
	USG2160BSR-W	USG2100 Unified Security Gateway
	USG2130BSR	USG2100 Unified Security Gateway
	USG2130BSR-W	USG2100 Unified Security Gateway
	USG2120BSR	USG2100 Unified Security Gateway
	USG2160HSR	USG2100 Unified Security Gateway
	USG2160HSR-W	USG2100 Unified Security Gateway
	USG2130HSR	USG2100 Unified Security Gateway
	USG2130HSR-W	USG2100 Unified Security Gateway

Category	Device	Description
	Eudemon200E-B	E200E Unified Security Gateway
	Eudemon200E-BW	E200E Unified Security Gateway
	USG2130HSR-P	USG2100 Unified Security Gateway
	USG2130HSR-WP	USG2100 Unified Security Gateway
	USG2160HSR-P	USG2100 Unified Security Gateway
	USG2160HSR-WP	USG2100 Unified Security Gateway
	USG2110-F	USG2100 Unified Security Gateway
	USG2110-F-W	USG2100 Unified Security Gateway
	USG2110-A-W	USG2100 Unified Security Gateway
	USG2110-A-GW-W	USG2100 Unified Security Gateway
	USG2110-A-GW-C	USG2100 Unified Security Gateway
	USG2110-A-GW-T	USG2100 Unified Security Gateway
	USG50	USG50 Unified Security Gateway
	USG2110	USG2100 Unified Security Gateway
	USG2210	USG2100 Unified Security Gateway
	USG2220	USG2100 Unified Security Gateway
	USG2230	USG2100 Unified Security Gateway
	USG2250	USG2100 Unified Security Gateway
	USG2250-D	USG2100 Unified Security Gateway
	USG2205BSR	USG2200 Unified Security Gateway
	USG2220BSR	USG2200 Unified Security Gateway
	USG2220BSR-D	USG2200 Unified Security Gateway
	E200E_C	E200E Unified Security Gateway
	E200E_F	E200E Unified Security Gateway
	E200E-F-D	E200E Unified Security Gateway
	USG2220BSR	USG2200 Unified Security Gateway
	USG2205BSR	USG2200 Unified Security Gateway
	USG2220HSR	USG2200 Unified Security Gateway
	USG2205HSR	USG2200 Unified Security Gateway
	USG5150	USG5100 Unified Security Gateway

Category	Device	Description
	USG5120	USG5100 Unified Security Gateway
	USG5150BSR	USG5100 Unified Security Gateway
	USG5120BSR	USG5100 Unified Security Gateway
	USG5150HSR	USG5100 Unified Security Gateway
	USG5120HSR	USG5100 Unified Security Gateway
	USG2205HSR	USG2200 Unified Security Gateway
	USG2220HSR-D	USG2200 Unified Security Gateway
	USG2220TSM	USG2200 Unified Security Gateway
	USG2250TSM	USG2200 Unified Security Gateway
	USG5120-D	USG5100 Unified Security Gateway
	USG5120BSR-D	USG5100 Unified Security Gateway
	USG3040	USG3040 Unified Security Gateway
	USG3030	USG3030 Unified Security Gateway
SRG	SRG2220	SRG2200 Secure Routing Gateway
	SRG2220-D	SRG2200 Secure Routing Gateway
	SRG2210	SRG2200 Secure Routing Gateway
	SRG3230	SRG3200 Secure Routing Gateway
	SRG3240	SRG3200 Secure Routing Gateway
	SRG3240-D	SRG3200 Secure Routing Gateway
	SRG3250	SRG3200 Secure Routing Gateway
	SRG3260	SRG3200 Secure Routing Gateway
	SRG20-20	SRG20 Secure Routing Gateway
	SRG20-21	SRG20 Secure Routing Gateway
	SRG20-30	SRG20 Secure Routing Gateway
	SRG20-31	SRG20 Secure Routing Gateway
	SRG20-31-D	SRG20 Secure Routing Gateway
	SRG2220	SRG2200 Secure Routing Gateway
	SRG2220-D	SRG2200 Secure Routing Gateway
	SRG20-10	SRG20 Secure Routing Gateway
	SRG1210	SRG1200 Secure Routing Gateway

Category	Device	Description
	SRG1210W	SRG1200 Secure Routing Gateway
	SRG1220	SRG1200 Secure Routing Gateway
	SRG1220W	SRG1200 Secure Routing Gateway
	SRG1210-S	SRG1200 Secure Routing Gateway
	SRG1210-S	SRG1200 Secure Routing Gateway
	SRG20-11	SRG20 Secure Routing Gateway
	SRG20-12	SRG20 Secure Routing Gateway
	SRG20-15	SRG20 Secure Routing Gateway
	SRG20-15W	SRG20 Secure Routing Gateway
	SRG20-12W	SRG20 Secure Routing Gateway
EGW	EGW2160	EGW2100 series Enterprise Gateway
	EGW2160W	EGW2100 series Enterprise Gateway
	EGW2130	EGW2100 series Enterprise Gateway
	EGW2130W	EGW2100 series Enterprise Gateway
	EGW2220	EGW2200 series Enterprise Gateway
	EGW2220-D	EGW2200 series Enterprise Gateway
	EGW2210	EGW2200 series Enterprise Gateway
	EGW3260	EGW3200 series Enterprise Gateway
	EGW3250	EGW3200 series Enterprise Gateway
	EGW3240	EGW3200 series Enterprise Gateway
	EGW3240-D	EGW3200 series Enterprise Gateway
	EGW3230	EGW3200 series Enterprise Gateway
	EGW2112GW	EGW2100 series Enterprise Gateway

10.17 Manageable DPI Equipment

Manageable DPI equipment are listed as follows:

Table 10-17 Manageable DPI equipment

Category	Device	Description
SIG	SIG9810	SIG9810 DPI Equipment

Category	Device	Description
	SIG9820	SIG9820 DPI Equipment
	NE40E-DPI	NE40E-DPI DPI Equipment
	NE80E-DPI	NE80E-DPI DPI Equipment
	SIG Server	SIG DPI Equipment
	DPI Server	DPI DPI Equipment
	RADIUS Server	RADIUS DPI Equipment
	URL Classify Server	URL Classify DPI Equipment

10.18 Manageable SVN Series Equipment

Manageable SVN series equipment are listed as follows:

Table 10-18 Manageable SVN series equipment

Category	Device	Description
SVN	SVN3000	SVN3000

10.19 Manageable OP-Bypass Equipment

Manageable OP-Bypass equipment are listed as follows:

Table 10-19 Manageable OP-Bypass equipment

Category	Device	Description
OP-Bypass	OP-Bypass	OP-Bypass

A Acronyms and Abbreviations

A

AC	See **Attachment Circuit**
ACE	Adaptive Communication Environment.
ASON	Automatically Switched Optical Network
Asynchronous transfer mode	An electronic digital data transmission technology. In June 1992, ATM is designated by the ITU-T as the transfer and switching mode for B-ISDNs. Because of its high flexibility and support for multimedia services, ATM is considered as the key to implementing broadband communications.
ATM	See **Asynchronous transfer mode**
Attachment Circuit	A circuit that connects a user host to a switch.

B

Bandwidth	In the data communication area, bandwidth specifies the maximum value of the rate when the data passes through some data channel.
BW	See **Bandwidth**
BWS	Backbone WDM System

C

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. See also server.
Cluster	The cluster is an administrative domain composed of a set of switches. It consists of a command switch and multiple member switches. The management over all the switches within the cluster is realized through a public IP address.
CORBA	Common Object Request Broker Architecture.
CPU	Central Processing Unit.

D

Data Communication Channel	Data Communications Channel. The data channel that uses the D1-D12 bytes in the overhead of an STM-N signal to transmit information on operation, management and maintenance between NEs. The DCC channels that are composed of bytes D1-D3 is referred to as the 192 kbit/s DCC-R channel. The other DCC channel that are composed of bytes D4-D12 is referred to as the 576 kbit/s DCC-M channel.
DC	Data Centre. As an independent component of the U2000, the NE software management component implements the backup and uploading of device data.
DCC	See **Data Communication Channel**
DCN	Data Communication Network.
DDN	Digital Data Network.

E

Embedded Control Channel (ECC)	Embedded Control Channel. An ECC provides a logical operations channel between NEs, utilizing a data communications channel (DCC) as its physical layer.
EMS	Element Management System.

F

File Transfer Protocol	A very common method of moving files between two Internet sites. FTP is a special way to log in to another Internet site for the purposes of retrieving or sending files. There are many Internet sites that have established publicly accessible repositories of material that can be obtained using FTP.
FTP	See **File Transfer Protocol**

G

GNE	Gate Network Element

H

HA	High Availability.
HTTP	Hyper-Text Transmission Protocol

I

IDL	Interface Description Language.
IP	Internet Protocol.

L

LAN	Local Area Network.

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

M

MML	Man-Machine Language.
MSP	See **Multiplex section protection**
Multiplex section protection	The nodes online achieve protection switching through the K1 and K2 bytes in the multiplex section,? including linear 1+1 MS protection switching link, linear 1:n MS protection switching link, dedicated MS protection ring and shared MS protection ring.

N

NBI	See **northbound interface**
NE	See **Network Element**
Network Element	It is the network element, including the hardware unit and the software running on it. Usually, one NE has at least SCC (System Control & Communication Unit) board which responsible for the management and monitoring of the NE. The host software runs on the SCC board.
NM	Network Management
NMS	Network Management System.
northbound interface	The interface that connects to the upper-layer device to realize service provisioning, report alarms and performance statistics.
NTP	Network Time Protocol

O

OAM	Operations, Administration, and Maintenance
OEM	An original equipment manufacturer, or OEM is typically a company that uses a component made by a second company in its own product, or sells the product of the second company under its own brand.
OLA	Optical Line Amplifier
ORB	Object Request Broker.
OS	Operating System.
OSI	Open Systems Interconnection.
OSN	Optical Switch Node
OSS	Operation Support System.
OTN	Optical Transmission Network

P

P2P	Point To Point

R

RAID	Redundant Array of Inexpensive Disk.
Route	A route is the path that network traffic takes from its source to its destination. In a TCP/IP network, each IP packet is routed independently. Routes can change dynamically.
RPR	Resilient Packet Ring.
RTN	Radio Transmission Node

S

SDH	Synchronous Digital Hierarchy.
Simple Network Management Protocol	Simple Network Management Protocol (SNMP), is widely accepted and used protocol. It is to guarantee that the management information is transmitted between any two points. It enables the network administrator to query and modify the information about any nodes, search for the faults, perform troubleshoting, plan capability and generate reports. SNMP adopts polling system and proivdes the basic function set. It is suitable for the the scenario with small sized, fast-speed and low priced devices. It is based on UDP and thus is widely supported by various products.
SNMP	See **Simple Network Management Protocol**
SQL	Structured Query Language.
SSL	Secure Socket Layer.
STM-1	Synchronous Transfer Mode at 155 Mbit/s.

T

TCP/IP	Transmission Control Protocol/Internet Protocol
TMF	TeleManagement Forum.

V

Virtual private network	An extension of the private network. A VPN contains shared links or encapsulated, encrypted, and authenticated links on the public network. A VPN can connect users or sites over the Internet.
Voice over IP	A transmission technology that delivers voice communications over the Internet.
VoIP	See **Voice over IP**
VPN	See **Virtual private network**

W

WAN	Wide Area Network.

WDM	Wavelength Division Multiplexing

X

XML	Extensible Mark-up Language.